WORK BY THE FORUM AGAINST DISINFORMATION CAMPAIGNS

2024 INITIATIVES

GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Published by:

GOBIERNO
DE ESPAÑA

MINISTERIO
DE LA PRESIDENCIA, JUSTICIA
Y RELACIONES CON LAS CORTES

NIPO (online edition): 143-25-017-1
Publishing date: July 2025

WORK BY THE FORUM AGAINST DISINFORMATION CAMPAIGNS

2024 INITIATIVES

Experts participate in working groups in a personal capacity, not as representatives of an institution. Therefore, their opinions and recommendations are not representative of nor binding for the institutions to which they belong.

The outcome of this work is the result of a collective reflection. It may not represent the individual opinions of all participants, who may not agree with all of the conclusions or proposals put forward.

INTRODUCTION

In December 2021 the current National Security Strategy was approved. For the first time, a National Strategy included disinformation campaigns as a risk to national security.

Since 2021, not only has the risk that disinformation poses to national security not diminished; its significance and prominence has held firm and could even be said to have increased. In fact, disinformation has become one of the most significant threats democratic systems currently face.

In this regard, the 2024 World Economic Forum report ranks disinformation as the most serious threat globally in the short term (next two years). Moreover, it highlights that artificial intelligence is being used to amplify manipulated and distorted information which may destabilize societies.

In this respect, the 2023 Annual Spanish National Security Report describes how global tensions are leading to an increase in disinformation campaigns that aim to destabilize and polarize society and undermine trust in institutions. It also highlights how, in the context of the war in Ukraine and the conflict in the Gaza Strip, there has been an increase in anti-Western, anti-European and also, at times, anti-Spanish discourse.

Faced with this threat, in 2024 Spain consolidated the Forum against Disinformation Campaigns Affecting National Security, a national public-private collaboration initiative.

This space for collaboration between public institutions and civil society, the private sector and academia, has cemented its position as a trustworthy tool that contributes to generation and sharing of knowledge on the risk disinformation poses to our democracy and the rule of law, as well as encouraging debate on the available mechanisms to address those threats. It brings together representatives from the main sectors in society involved in detecting, understanding and mitigating threats.

On 29 February 2024, the Plenary Session of the Forum decided to undertake a total of **eight initiatives**, whose results are collected in this book. The initiatives, carried out by Forum members or by experts in affected sectors, have aimed to further examine the challenges identified by previous work, generating knowledge on specific aspects of the threat which had not yet been sufficiently explored and continuing to discuss possible available solutions, including new regulatory tools such as the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC), in force since February 2024.

In this second report, on its work in 2024, the Forum has pursued dynamic initiatives that foster debate and the search for common solutions by experts from different sectors involved, seeking greater reach and impact. In this regard, in the context of this year's initiatives, conferences and round tables on the topic were held with highly qualified, experienced experts with excellent communication skills.

This book collects the results of two types of work undertaken by the Forum during 2024: chapter one to four reflect studies of specific subjects by experts; chapters five and six provide a summary and conclusions of two interactive initiatives carried out.

- The **first chapter** lists 125 key terms related to disinformation campaigns, which facilitate understanding and a coherent use of lexicon. This will prevent confusion and provide a common basis for describing concepts, techniques and strategies, given the lack of uniformity in terminology used to date by Spanish society.

- The **second chapter** describes the role **the media and communications departments of public and private institutions** should play to tackle the challenge of disinformation campaigns, which affect all kinds of institutions and bodies. Moreover, it addresses which mechanisms should be used to interact and how, and examines the importance of **communications during crisis management.** It also provides some special considerations on this matter.

- The **third chapter** sets out the tactics, techniques and procedures used by several foreign State actors, including Russia, China and Iran in campaigns to manipulate and interfere with information, focusing on both monetization strategies and economic resources used to fund them.

- The **fourth chapter** outlines an approach that aims to apply all lessons learned in the field of cybersecurity to Foreign Information Manipulation & Interference, using different technologies and procedures to assess how strategies, tactics and operations against specific targets are designed.

- The **fifth chapter** collects the conclusions and recommendations of the **seminar** held in September at the Faculty of Law of Complutense University of Madrid as part of the initiative on **disinformation campaigns and incitement of hate speech**. Speakers and attendees included experts in different fields. The chapter describes how the threats of disinformation and incitement of hate speech often interact, as well as the resulting risks. Moreover, it describes existing mechanisms to combat both threats and lists future challenges in this field.

- The **sixth chapte**r examines whether there is **scepticism in Spanish media and public opinion on the existence of disinformation campaigns linked to foreign interference**. It lists a series of conclusions and recommendations based on two round tables with experts in public opinion and the media.

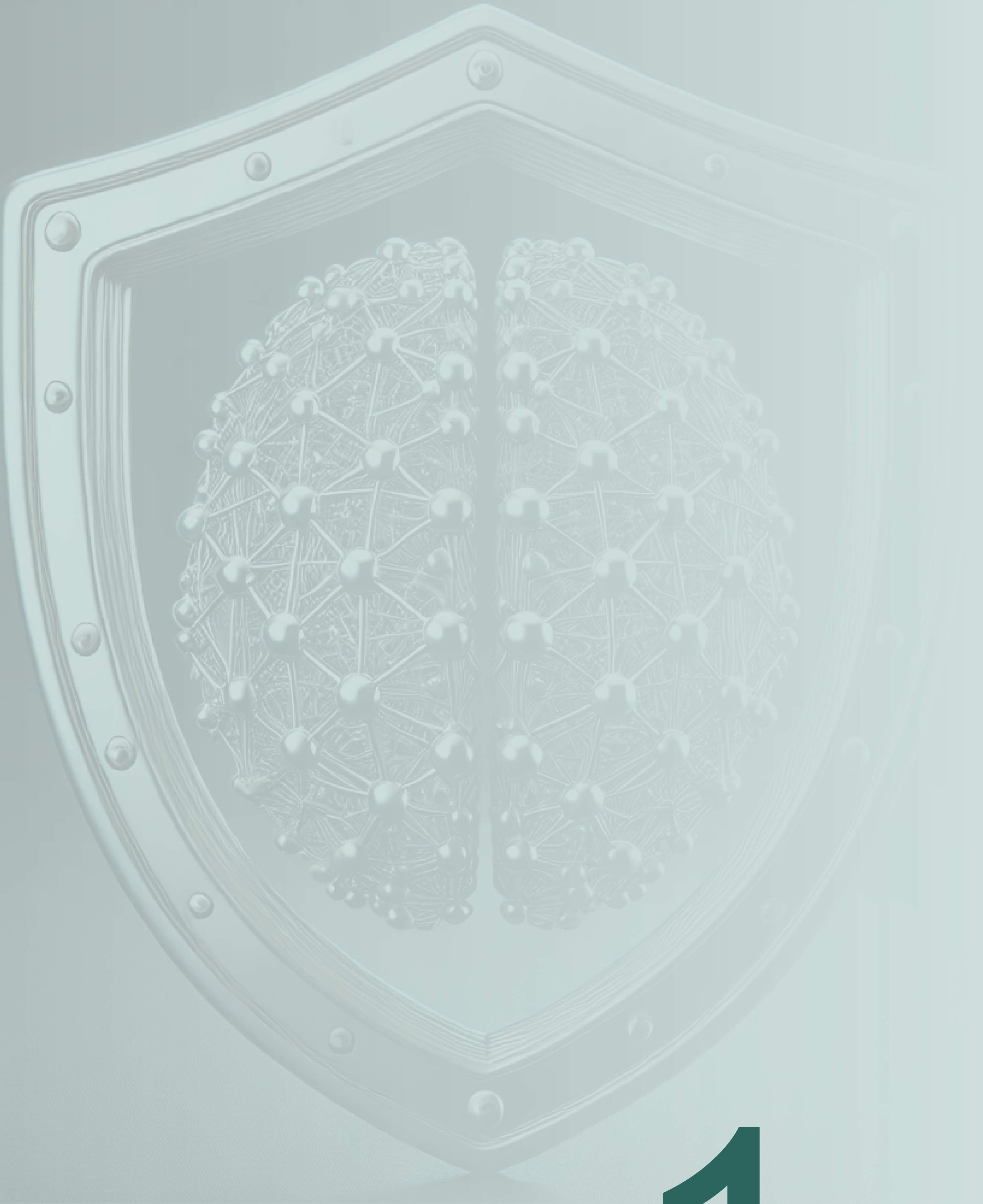
Some initiatives approved by the Forum in 2024 are still underway, which is why their results have not been included in this book. However, once work is complete, the results will be published online or included in the next report on the Forum's work.

We must acknowledge and underline Spanish society's engagement in this initiative—a pioneer in its field at international level—through representatives from civil society, the private sector, think tanks, research centres and academia.

Finally, we would like to highlight the role of Forum members and experts, who participated selflessly in the work carried out in 2024. They have devoted their personal effort, knowledge and experience in their fields to the pursuit of national security, motivated by a shared interest in promoting a more resilient and better-informed society, equipped to face disinformation campaigns and foreign interference in the media.

Dña. Loreto Gutiérrez Hurtado
Director of the Department of National Security and Chair
of the Forum against Disinformation Campaigns Affecting
National Security

INDEX



CHAPTER 1

125 TERMS
ON DISINFORMATION

Coordinators:

Sergio Arce García

Leticia Rodríguez Fernández

Department of National Security

Authors and contributors:

Mª José Establés Heras

David García Marín

Beatriz Marín García

Virginia Martín Jiménez

Concha Pérez Curiel

Elías Said Hung

Ramón Salaverria Aliaga

Astrid Wagner

INTRODUCTION

The proposal for this chapter originated in a working group attached to the Conference of Rectors of Spanish Universities, which aspires to link universities and research centres' activities to the study of and search for solutions to the phenomenon of disinformation.

Previously, the working group carried out an in-depth analysis of the academic literature on this matter published by authors with links to Spanish institutions, described the activity of the main research groups in the field, examined the funding provided by the State Research Agency and other private organizations to projects in this field and examined the role of universities and research centres in national security strategies.

As part of this work, and as the group analysed the different related scientific publications, several debates arose on the concepts and terms used to describe the different techniques and tools that make up a disinformation campaign. Unlike other languages, such as English, where terms such as malinformation, misinformation and disinformation are used to establish different nuances, Spanish uses the catch-all desinformación, which is even wrongly used to describe other situations, such as ignorance of a certain fact. An additional issue in Spanish is the use of terms from other languages, as their translation, framing and interpretation may vary from author to author.

This made clear the need for an easily accessible glossary of clear and standardized descriptions of tactics and strategies used in disinformation campaigns. This chapter therefore lists and defines 125 essential terms to understand these campaigns in the context of national security.

This work was coordinated by Sergio Arce García, senior lecturer at La Rioja International University; Leticia Rodríguez Fernández, tenured lecturer at the University of Cadiz; and a representative from the Department of National Security.

The work was carried out by the following experts: María José Establés Heras, assistant lecturer at the University of Castilla La Mancha; David García Marín, tenured lecturer at Rey Juan Carlos University; Beatriz Marín García, data analyst at the European External Action Service; Virginia Martín Jiménez, tenured lecturer at the University of Valladolid; Concha Pérez Curiel, tenured lecturer at the University of Seville; Elías Said Hung, tenured lecturer at La Rioja International University; Ramón Salaverria Aliaga, professor at the University of Navarra, and Astrid Wagner, tenured research scientist at the Spanish National Research Council's Philosophy Institute in Madrid. In addition, Antonio Díaz, tenured lecturer at the University of Cádiz, acted as representative of the working group of the Conference of Rectors of Spanish Universities at the Forum against Disinformation Campaigns Affecting National Security.

Firstly, the academic literature in this field (articles, book chapters and books) was reviewed in order to compile the terms which were of interest. At first, around 160 terms were compiled. They were assessed and filtered by the working group, based on importance and relevance to the field of security. On average, each author was assigned the definition of twelve terms. These definitions were then revised by all of the group's members, until it reached the final list of 125 definitions found hereunder. Lastly, in order to make reading and understanding this glossary easier, the terms were classified under eight basic criteria: (1) Information manipulation; (2) Impersonation, manipulation and technological resources; (3) Information warfare and foreign interference; (4) Control, suppression and propaganda strategies; (5) Fallacies, conspiracy theories and pseudo-knowledge; (6) Psychological, cognitive and perception tactics; (7) Algorithm and media manipulation; and (8) Cybercrime and online threats.

SCOPE OF THE STUDY

Disinformation in the digital context is a relatively recent phenomenon which is constantly evolving. Therefore, new terms are regularly coined or borrowed from other languages, and they need a precise, rigorous and useful definition for the different actors who take part in communication, identification, detection and solution.

Among them:

- **Communication sector, media and fact-checkers**: journalists both at conventional media outlets and at fact-checking agencies play an essential role in identifying and exposing fake content. Moreover, within the communication ecosystem there are other actors, such as communications departments, communication agencies and advertising agencies, which may be affected indirectly. We want this glossary to be useful to identify disinformation tactics and, in the case of journalists, to become a tool to standardize concepts when informing society.

- **Digital platforms**: tech companies are key actors in the detection of disinformation campaigns. The glossary we propose may be useful for those who curate content or may even be the basis for the development of more effective policies in this field.

- **Cybersecurity:** using this glossary, a future classification of forms of disinformation using IT systems may be undertaken, with an aim to detect disinformation automatically, search for terms efficiently or create early warning systems.

- **Academia:** researchers and academics play a triple role as researchers, educators and disseminators. This glossary contributes to an open debate and establishes standardized terms, facilitating research, education and access to knowledge about disinformation.

- **Society:** broader society is no less important. Nurturing society's knowledge of how disinformation campaigns work and improving their media and digital literacy is, without doubt, an opportunity to continue to enhance its resilience and, by extension, the quality of democracy.

GLOSSARY ON DISINFORMATION

Information manipulation

Alternative facts. Misrepresented or biased version of an event which contradicts empirical evidence and proven facts. This concept was created in political communication, which is where it is most prevalent, and it alludes to information which is not based on reality; rather, it is based on interpretations construed to influence public opinion or defend certain interests.

Cherry picking. Fallacy of incomplete evidence or selective attention, consisting of accepting as true only the data or evidence that confirms one's own idea or position while disregarding information that contradicts it. It also applies to defending an opinion selecting only the evidence and arguments which support it. An example of this fallacy in the field of disinformation is confirmation bias (see definition in this glossary).

Debunking. Act of proving the falsehood or inaccuracy of presumed disinformation using fact-checking strategies and techniques. These strategies are applied professionally by fact-checkers or debunkers in order to tag content as false, misleading, half-true, etc. In these debunking processes, fact-checkers not only publish the final results but also the techniques and evidence used during the fact-checking process.

Disinformation. Action or strategy which consists of deliberately spreading false, misleading, incomplete, decontextualized or partial information with an aim to confuse, persuade and manipulate. While in a general sense, incorrect information may be unintentionally incorrect, disinformation is deliberate and seeks to influence the public's opinions, beliefs and behaviour. Sources of disinformation use polarization, emotional and sensationalist language, hate speech and fear to weaken institutions and reduce trust, especially but not only during election campaigns.

Disinformation superspreader. An individual, organization or automated agent that plays a key role in the spread of fake news or misleading content thanks to their popularity, social influence or relevance. These people or social media accounts have large audiences and often produce or share disinformation among specific populations, increasing the impact. Disinformation superspreaders are characterized by intentional misrepresentation, production or spreading of attractive narratives that confirm pre-existing beliefs among certain groups, and exploitation of the viral potential of content on digital platforms.

Exaggeration. Amplifying the importance of facts, events or data. This highlights relevant aspects for the sender and/or the recipient which may be used to persuade or create intense emotion. It is used to disinform by capturing attention and/or generating false narratives.

Factoid. Popular belief lacking factual basis. False, inaccurate or trivial statement or data which becomes a supposedly indisputable fact after it is repeated by multiple sources.

Fake news. False or misleading information presented and spread deliberately as if it were true in order to influence public opinion and beliefs. It has the appearance of real news, imitating the format, professional style and website of reputable media. Fake news uses viral tactics to share content with millions of social media users. It is based on sensationalism, emotions, the use of made-up quotes and the distortion of facts and of the context of time and place in which events take place. Many experts advise against using this term, as stated in the first document on this matter by the Department of National Security ("Lucha contra las campañas de desinformación en el ámbito de la Seguridad Nacional. Propuestas de la sociedad civil" [Combating Disinformation Campaigns Affecting National Security. Proposals by civil society], only available in Spanish) published in 2022, which recommends using "disinformation" and "misinformation" instead.

Firehose of falsehood. Tactic used to rapidly and repeatedly spread a large amount of false information in order to overwhelm the public, with constant, intense flows of false information. It is akin to water flowing from a firehose, hence its name. This scenario makes it harder for the public to distinguish between true and fake news, which means they cannot check facts, as the amount of false information drowns out truthful information.

Half-truths. Statements which contain elements of truth but are incomplete, biased or presented in such a way as to mislead. They are easier to believe as they incorporate elements of truth and are harder to detect than a complete lie.

Hoax. False or misleading information spread intentionally with the aim of manipulating or deceiving the public. It is a baseless rumour or news item which spreads rapidly, often through social media and traditional media. It is a made-up story or statement, lacking trustworthy evidence to back it up, and has become a type of disinformation used to create confusion and mistrust, and to influence public opinion.

Hybrid strategy. Deliberate and synchronized use of different political, economic, social, diplomatic, military and information acts to take advantage of an opponent's weakness in these different areas—usually, in a target country—to hamper political decision-making and obtain a competitive advantage. Specifically, these strategies may include disinformation campaigns, cyberattacks, espionage, social subversion, sabotage and economic coercion. A hybrid threat may be the real or imaginary perception that said strategy could be carried out.

Inaccuracy. Lack of accuracy in information published about an action, statement or fact. It can either be deliberate, as part of a disinformation campaign, or accidental, when the publisher does not properly check facts. In all cases, inaccuracies in information are especially problematic, as they can lead to false or misleading narratives. They can occur in many ways, including the use of inexact vocabulary, leading to bias in the creation of an information discourse, and a lack of diversity of opinions when dealing with controversial topics.

Information disorder. Situations or phenomena that disrupt the communicative process and flow, and which may be related to disinformation, information overload, manipulation, lies, distortion and misinterpretation of facts and information, as well as limited access thereto and/or censorship. It is produced deliberately and may combine different tactics.

Information manipulation; Foreign Information Manipulation and Interference (FIMI). Information manipulation includes a series of practices to distort and disrupt the communicative process for the purpose of influencing and altering public opinion. FIMI describes a pattern of behaviour, most of it not illegal, whose aim is to threaten or create a negative impact on democratic values and political processes. This activity aims to manipulate and is undertaken intentionally and in a coordinated manner by foreign actors and their proxies inside and outside their territory.

Malinformation. Use of information which is truthful or partially based on the truth with the aim of causing harm to a person, group, organization, institution or country. It includes the political use of sensitive information, the leaking of personal or confidential information, and the publication of compromising information obtained by fraudulent means. Although malinformation is based on true information, the information may be incomplete, out of date or may have been manipulated in order to discredit, harm or undermine the target population or organization.

Misinformation. False, mistaken or inaccurate information supplied with no intent to mislead or manipulate. It may confuse the recipient, although it is often the result of mistakes, negligence or unconscious bias. Unlike disinformation (which does entail supplying false information deliberately), misinformation refers to supplying untruthful information accidentally.

Paltering. Misrepresentation by selecting true statements which, however, are misinterpreted so as to create a misleading narrative. It is based on threading together true statements to create an untruthful narrative, making its general refutation harder. It is often used by the supplier of the information as protection against accusations of dishonesty.

Post-truth. This term refers to an environment in which facts are considered irrelevant or less important than beliefs and personal opinions, and appeals to feeling and disinformation tools are used to influence public opinion and political debate. In these circumstances, the importance of mechanisms to scrutinize, fact-check and justify drops, while the importance of what is felt or perceived to be true rises.

Prebunking. Derived from “debunking”, this term refers to a set of preventive measures aimed at immunizing or forewarning the public against fake content. Based on inoculation theory from the field of sociology, it is mainly used by fact-checking agencies and organizations that promote media literacy.

Rotten herrings. Method or technique used to spread negative or black propaganda, in which a person, group or institution is continuously linked to several scandals or falsehoods. Even if the claims are proven false, the association between the accused and the scandal remains in the public's mind. It is often used on social media or disinformation websites and it can be spread using astroturfing techniques to make its way into the public debate in different sections of society or in the traditional media. It has been used throughout history in numerous occasions, and it is currently one of the most common techniques.

Trial balloon. Communication tactic that consists of leaking information or suggesting potential measures to gauge levels of acceptance or rejection. In political communication it is generally used with the media, to assess the public's reaction to an idea before taking definitive action.

Impersonation, manipulation and technological resources

Bot. Short for robot. It is a software program designed to carry out automated tasks on the internet, without human intervention. It has the capacity to interact with users in real time, handle large volumes of data and adapt to different environments. Bots, when used maliciously, produce disinformation, manipulate public opinion, impersonate people or organizations, launch coordinated attacks against individuals, organizations and groups, overload networks, and manipulate trending search results.

Catfishing. Formula to mislead and defraud which consists of the creation of a false identity on social media or digital platforms. Catfishers create false profiles through chats, emails, phone calls or video calls, using photos, names and details from other people's lives. The most common strategies are emotional manipulation, the use of moving and convincing stories or requests for money to fund financial, health or other emergencies. Its goals are fraudulent financial gain, revenge or mere entertainment.

Cheapfake. Disinformation which consists of simple and crude manipulation of pre-existing media material in any format (text, photo, video or audio). Manipulation can be carried out through editing or by providing a false context. Unlike deepfakes (much more credible and sophisticated, and more difficult to produce), cheapfakes require little effort and technological knowledge, and can be created with simple, accessible tools. Although they are easier to fact-check, they are common in disinformation loops and can have a high impact.

Cyborg. Abbreviation of cybernetic organism. The image of the cyborg corresponds to a being that combines human and technological components. In the context of the disinformation, they can spread fake news in a more effective way than fully automated tools such as bots. They can create consensus or dissent and influence the public's perception of a topic, use algorithms to increase biased content and polarization and erode the public's trust and confidence.

Deepfake. Artificial intelligence technique to manipulate or generate highly realistic fake content such as images, video or audio. This content is created based on deep learning training data, which allow faces to be swapped or even to create a person who does not exist. Deepfakes have been used to create misleading content, such as videos of politicians or celebrities saying or doing things they never actually did.

Generative artificial intelligence. System which enables the generation of large volumes of new data which imitate content created by humans through the use of advanced algorithms.

These systems use deep learning models, such as generative neural networks, to produce text, images, music, video and other types of content. The best known generative models include generative adversarial networks (GAN) and language models such as ChatGPT (Generative Pre-trained Transformer). Misuse of generative AI favours disinformation, document forgery and impersonation through deepfakes with manipulated images, audio and video.

Hack and leak operations. Information manipulation technique which combines cybersecurity with an information operation. These operations start by gaining unauthorized access to systems or data belonging to an organization or individual, followed by a selective leak of the stolen information to manipulate public opinion or harm the reputation of individuals, organizations and governments. Leaked content can be real, fake, manipulated or a combination thereof.

Impersonation. Information manipulation technique which consists of taking on the identity of a real person or of a legitimate organization, such as a media outlet or a public entity, in order to mislead the public and spread fake or misleading information. This technique is used to take advantage of the credibility and trustworthiness associated with the person or organization that is being impersonated, in order to amplify disinformation's scope and impact. The term doppelgänger is used specifically for Russian influence operations which use a network of clones, copying designs and domains of real Western media outlets to spread fake articles, videos and surveys.

Kill chain. Adapting the military and cybersecurity concept to disinformation, the kill chain model breaks down the analysis of an incident into a series of structured phases which describe the life cycle of a disinformation campaign, from conception to execution and assessment through the description of tactics, techniques and procedures (TTPs). The stage-by-stage analysis of an attack allows analysts to predict, recognize, interrupt or prevent an attack in each of the incident's stages.

Leetspeak (also known as 1337 or leet). It is a system of modified spellings using character replacement as a code, rendering it incomprehensible to certain users and unidentifiable to algorithms which detect hate speech, swearwords and insults. By replacing certain letters by other characters, users mock others or avoid certain words being identified as offensive by forum or social media algorithms. In the case of social media account identification, leetspeak is used to hide or create a series of different versions of a user. This may lead to the creation of "number plate" accounts, where a username is followed by a series of numbers and characters.

Phishing. Technique designed to trick people into providing confidential information about themselves or about an institution. It consists of sending messages to gain the target's trust so that they can later be manipulated into carrying out improper activity. Using deceit or flattery, a variety of situations is exploited so that the victim "takes the bait". As a social engineering technique, it focuses on human vulnerability rather than on IT systems, which makes it one of the more simple, dangerous and effective techniques. This is why it is among the most widespread.

Sock puppet account. Fake account used on social media to create false identities or conceal real identities. It can be used as an information manipulation technique to spread disinformation covertly. It can also be used for research purposes in order to protect and hide the true identity of OSINT (Open Source Intelligence) analysts and to obtain access to information on platforms which require an account.

STIX (Structured Threat Information Expression). Standardized language used to codify and exchange cyber threat intelligence. In the field of disinformation, it provides a common syntax to express and structure information on the analysis of threats. STIX provides analysts with a standardized method for sharing information. This language has been adopted as an international standard by several intelligence-sharing communities and it is the common standard adopted by the European Union and the United States to exchange structured information regarding FIMI threats.

TTPs; DISARM. In the context of information manipulation, analysis of tactics, techniques and procedures (TTPs) enables description of a threat actor's patterns of behaviour within a structured framework. As a whole, TTPs describe how threat actors operate stage by stage, from the general planning strategy to specific methods and processes used to manipulate public opinion. Analysis of attack patterns is a crucial tool to plan response and reaction strategies to information manipulation (kill chain). The DISARM Red Framework is a catalogue of open code designed to describe TTPs in the field of disinformation, while the Blue Framework contains suggested answers to said TTPs.

Typosquatting. Information manipulation technique used by threat actors who register internet domains with similar names to real websites. These domains are used to create confusion and to give legitimacy to fake content; to mislead and to obtain personal data; to redirect to malicious websites; or to attract traffic to obtain advertising revenue. Threat actors often register domains similar to legitimate websites to create confusion and redirect users to malicious websites.

Vishing (voice phishing). Technique in which a person, company, organization or public institution is impersonated in a call, a recording or a video. Its aim is to obtain the victim's sensitive personal information, such as a card number or PIN. In cases where public figures such as politicians are impersonated, the aim can be to conduct a disinformation campaign. Vishing can also be used in disinformation campaigns to conduct interviews with public figures and later publish the information obtained and ridicule them. The term is a portmanteau of voice and phishing.

Information warfare and foreign interference

Active measures. This expression was used throughout the 20th century to refer to influence operations such as disinformation and propaganda, aimed at destabilizing, sowing discord and other forms of subversion. These measures, mainly offensive, are used to attack, control, impede or neutralize actions, and include information and physical acts. The term was coined by Soviet leaders in the 1920s, but it became widespread after the Second World War, during the Cold War. The term is now once again commonly used, especially in the context of operations on social media. There have been studies concerning active measures directed at public opinion, politicians, governments, academia, companies and non-governmental organizations.

Cyberwarfare. The use of cyberattacks by nations, States or organizations to harm, interrupt or destruct other countries' or organizations' information systems, networks and critical infrastructure. These attacks may include infiltration to steal information, sabotage critical infrastructure and manipulate the media. It includes techniques such as malware, ransomware, denial-of-service attacks (DoS) or phishing, and it is characterized by its clandestine nature and the difficulty of attributing attacks. It can cause significant harm without resorting to direct physical violence.

Foreign influence; foreign interference. Foreign interference is often part of a wider hybrid strategy and may include efforts to coerce, deceive or mislead in order to disrupt people's free formation and expression of opinions or wishes. It is carried out by a foreign State actor or by its agents. This activity usually pursues political goals and in doing so interferes with, subverts or harms established democratic processes, values and procedures and runs against a State's sovereignty and national interests. In contrast, foreign influence activities are conducted openly and transparently, and are a regular aspect of international relations and diplomacy. They make a positive contribution to public debate.

Hacktivism. Activism in digital environments whose purpose is to draw the attention of public opinion to social or political issues. It uses techniques such as defacement of websites, publication or leaking of confidential information, and overloading web services or websites to stop them working.

Hard power. Unlike soft power, this refers, from an international relations and geopolitics perspective, to national/State power in military and economic terms. This form of political power usually entails coercing or compelling other States with lower military and economic capacity.

Hybrid threats. Coordinated and synchronized action to favour or achieve the goals of State or non-State actors which deliberately seek to undermine, destabilize and harm opponents, as well as to exploit systemic vulnerabilities of States and their democratic institutions They combine a wide range of techniques (from cyberattacks, information manipulation campaigns, covert political manoeuvres and military tactics, among others) and exploit thresholds of detection and attribution, as well as different boundaries (war-peace, national-international, local-State...), and they seek to influence decision-making at a local, State or institutional level in different ways. In addition, they are not clear-cut threats and are difficult to attribute them to a specific actor. The literature occasionally uses the terms hybrid threat and hybrid strategy interchangeably, although the former refers to actions that may occur in the future while the latter, albeit usually including threats as part of a general framework or plan, refers to actions that actually take place in order to achieve a goal. Rapid technological evolution and global interconnectivity have increased the speed, scale and intensity of all these aspects.

Hybrid warfare. Coordinated and synchronized use of a wide range of instruments against an opponent, gauging its intensity and avoiding, insofar as possible, direct military confrontation and even any possible reaction by the opponent. Hybrid warfare combines unconventional and conventional military strategies with hostile intelligence operations, information manipulation and interference campaigns or threats, and political and economic pressure, which are part of psychological warfare. Actions which seek to defeat, or weaken or break the opponent's will. In other words, it is characterized by the spatial and temporary integration of conventional procedures with irregular warfare tactics (propaganda, subversion, lawfare, cyber operations or information warfare), mixed with terrorist acts and connections to organized crime to obtain funding, support and assistance.

Information warfare. Actions based on the misuse of mass psychological campaigns against the population of another State in order to destabilize its society and its government, and force said State to make decisions favourable to its opponent, interfering in its information domain. Information warfare is often initially used to achieve political goals without the need to use military strength and, at later stages, to shape a favourable response from the international community before the use of military strength. Russian military doctrine considers it a conflict between two or more States in the information domain aimed at inflicting harm on information systems, processes and resources, as well as on critical infrastructure, in order to undermine the other State's political, economic and social systems.

Infosphere; noosphere. In a digital context, infosphere refers to the global information environment including all information and communication technologies, data and networks. It includes all of the information created, stored and shared via the internet, databases, social media and other digital media. This is the space where digital interaction and data sharing take place, which, in the digital age, is fundamental for the functioning of society and the economy. The noosphere focuses on the field of knowledge and the collective awareness facilitated by digital technologies. It represents the virtual space where human minds interact and collaborate, transforming information into shared knowledge through digital platforms, social media and online collaboration tools. The digital noosphere encompasses phenomena such as collective intelligence, crowdsourcing and collaboration on projects, increasing human capacity to think, learn and create collectively in the digital realm.

Kompromat. A Russian loan word, referring to compromising material, i.e. damaging or incriminating information compiled to blackmail a person or organization. This information may include real or fabricated evidence on illegal, immoral or shameful activities carried out by the person or organization being blackmailed.

Lawfare. Use of legislation to strengthen the legitimacy of strategic, operative or tactical goals of a threat actor against a specific opponent, or to weaken the legitimacy of the opponents' respective goals. Lawfare is different to the mere adoption of laws that affect an opponent State or the signing of treaties; it depends on how said laws are used, with what purpose and against which opponents to achieve specific goals. Moreover, it can be used in asymmetric warfare to establish the conditions for a conflict or negotiations, and could sometimes be said to be "legal preparation" for a war scenario.

Obstructionism. A tactic which aims to block, delay or impede the fulfilment of certain proposals, actions or agreements around important and sensitive political or social issues. This may include actions to buy time, such as filibusters or blocking the approval of a budget. Its aim may be to prevent the approval of the proposal, to undermine a government, shift the viewpoint on a matter of public debate, create disillusion and frustration in the population, or even erode governance.

Psychological operations (PsyOps). The planned psychological activity component of information operations. These operations use communication methods and other media that target specific audiences to influence perceptions, attitudes and behaviour, hindering the pursuit of political and military goals.

Proxy. Entities, organizations or individuals within a State that act on behalf of a foreign actor. They may act as media, marketing or advertising companies, political organizations, interest groups, civil servants or even public figures and influencers. Although they may be located and operate within their own country, these actors disseminate messages or propaganda that benefit a foreign government or entity, against national interests. Proxies are not always directly affiliated with foreign actors, or may sometimes hide such an affiliation, but they can receive support through funding, information or resources. Proxies are used by foreign actors to hide their identity or evade international law. The term also refers to websites used by threat actors as fronts to whitewash their manipulated information content.

Reflexive control. Techniques used to transmit to an interlocutor or opponent information specially prepared to predispose them to voluntarily make the decision the actor carrying out the action wants. The tactical advantage which the perpetrator seeks is obtained by altering factors that are key to the perception of information by the opponent (which may be a State) and seeks to neutralize its strong points, making it choose harmful action plans which, in turn, are beneficial to the perpetrator's goals. This process is based on detailed understanding of the opponent's mental models and decision-making structures, which allows a perpetrator to shape their target's perception of reality and guide them towards unfavourable strategic choices. This technique plays a role in Russian military doctrine, and are part of the maskirovka (lit. "masking"), alongside active measures and dezinformatsiya, considered an applied art for manipulation in order to influence strategic decisions.

Soft power. In contrast with hard power, this term, popularized by Joseph S. Nye, Jr., refers to a State's ability to influence another State without using economic or military power, instead using the persuasive power of its cultural expressions in all forms, the political values it defends and its model of society. This concept, linked to domination through non-coercion, is currently used to understand power strategies in the digital environment, where attracting and co-opting are more efficient than coercion through rules.

Xuanchuan. A Chinese word meaning propaganda or publicity. Historically, it is used to refer to Chinese military broadcasts, with an educational component and neutral appearance. In recent years, it has been exhibited as official propaganda, but given the negative connotation of the word propaganda in English, the Chinese term has also acquired a pejorative sense.

Zombie NGO (fake NGO; disappeared NGO). Non-governmental organizations (NGOs) which have either lost their original purpose or effectiveness, are using the name of a previous trustworthy NGO which no longer exists, or are fake. Thus, they distort communication and trust around real social issues or causes. They muddy the waters and dilute the impact of genuine communication campaigns carried out by real NGOs. Their activities contribute to hampering real social initiatives, encourage incorrect allocation of funds, fuel competitiveness over collaboration, reduce the organizational focus, perpetuate inefficient cultural narratives and devalue bona fide social change. They usually participate actively on social networks and exercise their influence on those platforms, in order to mobilize support around a given subject.

Control, suppression and propaganda strategies

Agitprop. A portmanteau of “agitation” and “propaganda”. The term was created by the Department of Agitation and Propaganda of the Secretariat of the Central Committee of the Communist Party of the Soviet Union in 1920. In the view of the Marxist theorist Georgy Plekhanov, which was seconded by Vladimir Lenin, the two concepts were completely different. Agitation was aimed at the masses, at the street, whilst propaganda was focused on ideas. Agitprop encompasses cultural forms whose purpose is openly political and persuasive.

Amplifying conspiracies and extreme voices (junk news). Different forms of propaganda, ideologically extreme, as well as hyperpartisan or conspiracy news, information and content whose aim is to saturate the public debate, amplify extreme narratives and displace other **conversations. Their aim is to reduce public trust.**

Astroturfing. A social media communication strategy, whereby a number of users, apparently the same as the rest, act together, capitalizing on their apparent anonymity, to distribute and amplify disinformation, flooding platforms with it. These users generally follow and are followed by few other users, although the number tends to be higher in the case of repurposed accounts, i.e. accounts that change and adapt their narrative focus as they obtain the advantages of having previously gained followers by posting about other topics. The content aims to shape narratives, create trends or trending topics, and steer public debate towards certain topics. The word is a play on the term “grassroots”, which refers to real spontaneous movements born from the public or from communities, whereas astroturfing is a planned movement trying to pass itself off as a grassroots movement.

Deplatforming. Deliberately withdrawing, limiting or refusing access to certain actors (be they individuals, groups or organizations) who breach usage policies of online platforms, service providers or critical services. This measure is related to the content moderation, determining its eligibility for a given website, location or jurisdiction and reducing its spread and impact.

Euphemesia. This term was coined by Ralph Keyes in his 2004 work The Post-Truth Era: Dishonesty and Deception in Contemporary Life, which alludes to the use of euphemisms to avoid lies, and which characterizes the post-truth era: “Ambiguous statements that are not exactly the truth but fall short of a lie”. Euphemisms are used to soften or disguise the real meaning of a concept or fact.

Hahaganda. Propaganda technique which makes use of humour to mask the spread of disinformation content, aimed at manipulating other users on social media. This technique is used to spread a message, humiliate or discredit a person, institution or post. The danger of this technique lies at the cognitive level of receiving users, as it affects the way they think and how they establish social and political relations.

Information laundering. A set of manipulation techniques used to legitimize certain information content using republication by intermediaries that prevents attribution to the original source, thereby concealing the provenance of the information. The information laundering process has three stages: the first stage is the original publication by one or several communication channels; it is later reused by one or more intermediaries, often interrelated, which hide their links to the original source and launder the content; and lastly, the information is integrated into public discourse, amplifying and legitimizing the manipulative content.

Monetization (and demonetization). In the digital sphere, monetization refers to strategies and methods used to generate income through online content, services or products. This includes advertising, subscriptions, direct sales, merchandise and sponsorship that supports campaigns, including disinformation campaigns, generating profits and greater publicity, even offline. Demonetization, in the context of disinformation, is removing monetization opportunities for those who spread false, misleading or manipulated information. Social media platforms have adopted economic measures to fight disinformation. These policies include the removal of adverts and restrictions on payments to those content creators sharing false or harmful information. Its main goal is two-fold: on the one hand, to reduce the financial motivation to create and spread disinformation; on the other, to limit its reach and spread.

Propaganda. Set of communication techniques and strategies used in politics, war or advertising to influence public opinion, attitudes and behaviour by using bias, exaggeration and manipulation of the facts. It uses intentionality, information selection, emotions, message repetition, simplification, and dehumanization and negative images of adversaries as a form of unilateral persuasion, without needing to offer arguments or balanced views of the facts. Its direct consequences are polarization, distrust and manipulation of public opinion, and it includes disinformation among its tools.

Relativism. Philosophical position which claims statements about truth and falsehood, what is right and what is wrong, as well as the reasoning behind them, are the product of different conventions and interpretation and assessment frameworks, and change accordingly. Therefore, their authority is limited to the cultural, scientific, religious or even ideological contexts they stem from. Therefore, in its different branches, relativism rejects the universal and absolute character of knowledge, truth, facts or values.

Strategic communication (StratCom). Planning of an organization's communication in which specific messages are sent depending on the audience, in order to achieve certain goals. Communication is aligned with the organization's overall strategy, and seeks to improve its position and reputation. In the field of security, the abbreviation StratCom is commonly used. It alludes to communication carried out by governments or military organizations with a broader meaning than simply setting an agenda or planning messages. StratCom is a strategic tool which contributes to coordination of communication activities and operational capabilities, including diplomacy, strategic monitoring, international relations and even implementation of public policies. Formulating strategies of this kind is a means of countering information warfare activities carried out by threat actors such as hostile States utilizing hybrid strategies against their targets, since the process can be used to identify the strengths and weaknesses of threats and come up with effective deterrence measures.

Suppression techniques. A set of information manipulation techniques used to control information by eliminating or suppressing certain voices or messages from the public sphere. Suppression techniques used by authoritarian actors may be internal, but they can also be employed abroad, targeting a diaspora. They can affect any critical independent voice. Suppression may be exercised through control of distribution channels, exploitation of content moderation systems, coercion, pressure or ridicule of individuals or by means of cyberoperations to alter content ranking, prioritizing some messages and blocking others.

Washing; false flag marketing. It aims to position certain narratives, for economic or political motives, that promote a misleading and manipulated scenario, whilst also aiming to give the impression that the operations are being carried out by other users or entities. This favours misattribution or the creation of an environment that contributes to false justifications. This can undermine democratic processes and social cohesion, based on the distortion of reality and manipulation of sentiment in public opinion.

Whataboutism, whataboutery. Rhetorical technique in which an accusation or difficult question is answered using a counteraccusation or bringing up a different topic. This technique has thrived on social media platforms, which enable such counter-argumentative actions to spread rapidly, leading to fragmented and polarized debate. As a result, meaningful dialogue is undermined and a volatile and aggressive digital environment is fostered, affecting transparency and democratic values in public opinion. If the counteraccusation is directed at the person (ad hominem), accusing them of hypocrisy and inconsistency, it may also be called "tu quoque" (you too).

Fallacies, conspiracy theories and pseudo-knowledge

Appeal to authority, argument from authority, argumentum ad verecundiam. Mistake in reasoning which bases the validity of a statement only on its attribution to a person or entity, generally holding prestige, without considering the underlying evidence or arguments. Trust is placed in the person's reputation instead of in the solidity of the argument or evidence. It increases susceptibility to disinformation related to false experts. It is commonly used at a political level.

Big lie. Propaganda technique which consists of launching a campaign based on an evidently false claim, but which causes a highly emotional reaction such as disgust, repulsion or terror. This technique exploits the fact that an emotional response usually displaces rational thinking, allowing the lie to persist in the subconscious despite its evident falsehood. Mentioned by Adolf Hitler in 1925, it is often associated with the "rotten herrings" technique, since it consists of repeating a lie over and over until it becomes accepted as true.

Chewbacca defence. This defensive propaganda technique consists of putting forward nonsensical arguments in order to confuse an attacker or accuser. It is based on flooding the discussion with lies or fallacies by mentioning topics, examples and associations that bear no relation to the topic being discussed, in order to divert attention and spread doubt. This technique can be observed when a hoax is identified on social media or on a website and its promoters use this defence to mislead and confuse the public. Its name comes from the animated series South Park.

Conspiracy theory. Belief that claims an event is being maintained secret by ill-meaning groups in power. This theory is based on the mistrust towards official versions and uses hard-to-verify arguments. Spreaders of conspiracies mistrust institutions, governments, the media and experts. They usually flood public debate with different and sometimes contradictory explanations of a fact which lack an underlying empirical relation (causality) to the fact, in order to saturate the debate with data. They refuse to believe any refutation of their theory, despite their efforts to find a correlation which may mislead public opinion. These closed communities offer simple answers to complex issues, are supported by subjective interpretations of facts and ignore any information or refutation that contradicts their theory.

Conspiracy theory amplification. Process by which conspiracy theories are spread and become more influential. It describes an exaggerated tendency to see conspiracies behind events or situations where they are not necessarily involved. It is characterized by a distorted vision of reality where there is constant suspicion of hidden plots, orchestrated by powerful groups with evil intentions, and by the reduction of complex problems to a single, simple pattern based on the idea of a conspiracy.

Coudenhove-Kalergi Conspiracy (anti-Semitic conspiracy). Anti-Semitic conspiracy theory which states that a group of Jewish people and other international elites are conspiring to destroy European racial and cultural identity through mass immigration and racial mixing. This theory is based on a misinterpretation of the writings of Richard von Coudenhove-Kalergi, who proposed a European Union in the 1920s. It is usually promoted by alt-right and far-right groups, characterized by their tendency to spread conspiracy theories and hate speech.

Deep state. Supposed secret network of civil servants and State agents that act independently of legitimate leaders and the official institutions of a country. Its purpose is supposedly to protect hidden agendas and interests, influencing politics and government **decisions without being subject to democratic control.**

Denialism. A stance that consists of systematic denial or obstinate rejection of historic, scientific or social events or facts that are widely accepted and empirically verified. From a psychological point of view, this behaviour is explained as a mechanism to avoid a psychologically uncomfortable truth. The underlying motivation can be political, ideological, religious, emotional or simply financial. This dogmatic rejection should not be confused with the scientific scepticism that is an inherent part of the research process, entailing constant **revision of data, hypotheses, theories and results.**

False equivalence, false equivalency. Suggesting or assuming that two or more points of view are equally valid, when it is empirically/scientifically proven that one or more of them are much closer to the truth or are in fact the only ones which are true. In the context of disinformation, this occurs when the same weight is given to evidence-based arguments as to false, biased or inaccurate statements, which erodes understanding of reality. The problem of false equivalence is linked to action by certain media and digital platforms which sometimes amplify all kinds of narratives to avoid being accused of ideological bias or censorship.

Freedom convoy. Movement by Canadian truckers against government restrictions over the Covid-19 pandemic. The protest coincided with the circulation of a large volume of false or misleading information on social media and digital media that aimed to polarize public opinion. Some of the disinformation items associated with this event included conspiracy theories about the true motivations and funding of the convoy, and fake news about the level of popular support and the alleged illegality of restrictive health measures.

Logical fallacy; false dilemma. An argument which, using polarizing language, simplifies a complex problem and presents it as a choice between two options, disregarding other solutions and nuances. Logical fallacies include the false dilemma (also referred to as false dichotomy or false binary), which is a false conclusion based on a false premise that overly simplifies reality by excluding valid alternatives, or the questionable cause fallacy (also known as a causal fallacy, false cause, or non causa pro causa), whereby a cause is misidentified.

Love jihad; Romeo jihad. An anti-Muslim conspiracy theory which alleges there is a plan within the Muslim community to convert non-Muslim women to Islam through romantic relationships and interfaith marriages. This claim is based on the accusation that Muslim men are deliberately seducing and marrying women from other faiths in order to increase the Muslim population. The "love jihad" is considered a misleading narrative and is perceived as an attempt to demonize and stigmatize the Muslim community, by presenting interfaith relationships as part of an alleged conspiracy, when in fact there is no credible evidence for such statements.

Manosphere. A network of websites, forums and online communities that promote misogynist, antifeminist and male supremacist ideologies linked to far-right movements. Some examples are groups of men who define themselves as incels (involuntary celibates), MGTOW ("Men Going Their Own Way", i.e. rejecting marriage and relationships with women), MRA (Men's Rights Activists) and others who promote ideas of toxic masculinity.

Post-truth thinking. Reasoning in which feelings and personal beliefs have greater influence than objective facts and verifiable evidence. It is characterized by people's indifference to the distinction between truth and lies, reality and fiction, opinion and knowledge. This mentality tends to grant great importance to narratives through which alternative facts are construed.

Pseudoscepticism. It refers to denialists who self-describe as sceptics. It includes all kinds of denialism: historical (subjective and self-serving reinterpretations of history), scientific (rejection of evidence and of scientific consensus), technological (deep mistrust of technological advances) and political (denial of political, demographic or social facts). It must not be confused with the scepticism inherent to science nor with philosophical scepticism.

Pseudoscience. Cognitive field which claims to be scientific but does not meet some of the essential characteristics of science, thereby invariably clashing with accepted scientific theories. The following criteria help differentiate it from science: pseudoscience proposes entities whose existence cannot be proven, defends spiritualist concepts, lacks logic and objective control procedures, does not develop new problems and hypotheses and has little overlap with other disciplines. Its statements are often not refutable, and underlying theories hardly ever evolve through research.

Red pill. Term used by subgroups linked to the manosphere and to the far right, contrasting with the blue pill. It is a reference to men who have supposedly become aware of true reality in a context where they report, according to their misogynistic perceptions, that feminism has imposed an authoritarian and manipulative control on the world and its socio-political dynamics. The term originates from the film The Matrix (1999), where the main character, Neo, must decide between remaining oblivious to the fact he lives in a manipulated reality (by taking the blue pill) or opening his eyes to the truth (by taking the red pill).

Psychological, cognitive and perception tactics

Cognitive dissonance. A theory proposed in 1957 by the psychologist Leon Festinger, which explains the need people have for their beliefs and attitudes to be consistent with each other, and the discomfort that arises when this is not the case. People's tendency to seek internal consistency of internalized beliefs and behaviours can generate stress when they observe some of their own attitudes or, even, other people's ideas when they disturb that internal harmony. This uncomfortable feeling pushes an individual to reduce the discomfort by either attempting to change their behaviour, or by defending their beliefs or attitudes through self-deception.

Cognitive domain. Control over a set of mental skills and processes related to learning, knowledge and understanding. It includes functions such as perception, the sensorimotor system, attention, memory, thought and reasoning, which facilitate decision-making and critical thinking. Disinformation aims to subliminally undermine the autonomy of these cognitive capacities, which it achieves by managing the information its target audience receives.

Cognitive miserliness, cognitive miser. A mental process by which human beings save effort in processing information or in making decisions. Instead of conducting a meticulous analysis of data obtained applying logical reasoning, it refers to the processing of information in a superficial way through emotions or mental shortcuts that lead to a simpler interpretation of reality. This situation is especially prevalent in contexts of information overload such as today's, where it is impossible for people to pay full attention to the multiple stimuli to which they are exposed.

DARVO (deny, attack, reverse victim and offender). A reactive manipulation technique which consists of rejecting evidence and defending through offence, reversing the roles of victim and offender. This behaviour is common among offenders when they are identified as such. First, they deny the harm or abuse took place; then, they attack the victim and attempt to discredit them as a person or as a group; lastly, they claim to be victims instead of offenders. This technique is used to silence people or groups through criticism and to blame victims.

Dog whistle. Public speaking and propaganda technique which consists of using language with double meanings (doublespeak). This technique is based on the fact that certain groups have specific knowledge, or use specific language or meanings which only they understand, while message has a more innocuous meaning for the public at large. Thus, it is possible to communicate ideas to a particular group without receiving the attention of the rest of the population. The explanation for the name is that dog whistles emit sounds at frequencies that only dogs can hear, not humans.

Echo chamber. An environment where aligned beliefs, ideas or data are frequently shared, and therefore amplified and reinforced. The information, whether true or false, circulates and is spread without being questioned by members of the filter bubble (see glossary entry) or contrasted with other views, creating a distorted and polarized view of reality.

Epistemic flooding. A cognitive processing disorder caused by information overload. It occurs in spaces such as social media, where people are regularly exposed to more information and data than they can process carefully. The overload of images, data and text, and the speed at which they are consumed makes it harder to identify reliable information. This increases the influence of unreliable information.

Filter bubble. A term coined in 2011 by Eli Pariser to refer to the biased effect algorithms generate when they select the content a user is exposed to when surfing the internet. This selection mechanism isolates people ideologically in different bubbles, where they are not exposed to content which is not aligned with their point of view, creating an echo chamber which reaffirms their own beliefs and points of view.

Gaslighting. Strategy that seeks to manipulate another person into questioning their own perception of reality. The term indirectly originates from the play Gas Light, by Patrick Hamilton, of which several film adaptations were later made. In the play, a man manipulates his wife by making small changes around the house.

Gish Gallop. Propaganda technique, but also a response technique in debates, which consists of sending out a large number of messages in a short period of time, where the speed and quantity of argument prevails over their veracity. This technique is generally based on half-truths, lies or misrepresentations, preventing the opponent from having sufficient time to verify or refute the numerous messages in such a short period of time. Its name comes from a creationist called Gish, who used this technique against defenders of the theory of evolution.

Influence by persuasion / suggestion. Deliberate process employed by people or groups to influence and change another's attitude, belief or decision through a direct strategy, which uses clear logical arguments, or an indirect strategy, which uses implicit suggestions and emotional manipulation. The main purpose of persuasion is to convince the other party of the validity of an argument, and it requires efficient communication, including creativity, appeals to emotion, ability to listen, clarity and adaptation to the target audience. Misuse of persuasion can take the form of disinformation, political propaganda or false advertising, among other things.

Infodemic / information overload. A portmanteau of information and epidemic. It alludes to the situation where there is excessive information on a topic or a specific scenario where true, correct information is combined with fake data, rumours, and inaccurate, biased and malicious information. This information overload—amplified and spread to a global audience thanks to the use of digital technologies—exceeds an individual's limited processing capacity; this can lead to serious consequences, especially in the context of crises or emergencies.

Just Asking Questions (JAQing off); sealioning. An attack or harassment technique which consists of continuously questioning and requesting proof, maintaining a very polite and calm façade, in order to disorientate the other party. Although it is similar to the Gish Gallop, this technique differs in that those employing it constantly pose questions and make accusations of a lack of proof instead of presenting different arguments. Its purpose is to anger an opponent, and then act as the aggrieved party. It is a technique very commonly used in social media trolling, especially to silence a person or institution. When a sealioner succeeds in silencing the other party, it makes implausible statements seem acceptable.

Media literacy; media / digital / transmedia education. The power to consult and critically assess media content, as well as to create digital content. This skill entails understanding how the media work, recognizing the different kinds of media that exist and their formats, and developing critical skills to interpret the information they publish. It applies to both digital and traditional media.

Misperceptions. Incorrect ideas or beliefs around a fact, related to factors such as biased information, personal prejudice, or lack of knowledge about an event. The misperception is based on inaccuracy, generalization and extrapolation of individual cases to a general context and on confirmation bias, whereby people give greater credence to information that confirms their pre-existing beliefs. Its consequences are poor decision-making and loss of trust in the source.

Rabbit hole effect. The tendency to fall into an interminable cycle of online content. It has an addictive psychological effect in in which a person is trapped in an interminable cascade of related content through online platforms, social media, forums or news websites. The term comes from *Alice's Adventures in Wonderland, by Lewis Carroll*, where Alice falls down a rabbit hole and enters a bewildering fantasy world.

Algorithm and media manipulation

Algorithmic curation. Selection and filtering of information conducted by algorithms depending on user preferences and behaviours. It is fundamentally applied to queries using search engines and social media, and it affects access to information since said curation limits individuals' exposure to other opinions or views.

Bias, prejudice. A generic form of conscious or unconscious prejudice, linked to everyday trial and error, which generally contributes to a person's support for or opposition to a thing, person or organization over others. Bias occurs when the information or content shared is presented in a partially true or manipulated manner to favour certain interests, opinions or perspectives over others. Bias on social media takes various forms, and can influence the different perspectives of individuals, social groups or institutions. An example is how the algorithms that organize content on social media help to adapt what we see based on our behaviour and prior preferences.

Clickbait. This practice, which is used in digital marketing and media, consists of changing the content using ambiguous, misleading or sensationalist formats, especially in headlines, so that people visit pages out of curiosity. Once users have accessed the content, it is usually disappointing or does not meet expectations.

Confirmation bias. A kind of cognitive bias which consists of a person favouring, seeking, interpreting and remembering information that confirms their prior beliefs, assumptions or expectations, and giving less credence to alternative or contradicting evidence. Some of the characteristics of confirmation bias are systematic errors in inductive reasoning, selective gathering or recalling of information, biased interpretations (especially when linked to emotional issues or when beliefs are deeply rooted) and interpretation of ambiguous evidence as supporting pre-existing beliefs. Confirmation bias also explains polarization of attitudes, persistence of false beliefs and perception of illusory correlations.

Creepypasta. A variant of copypasta, from "copy and paste". It is a form of digital content that includes elements of fiction and horror to create an experience of fear or shock in the reader. These stories can also be used to spread disinformation and hoaxes, since they may contain elements of truth, but they are mixed with fictional elements and are spread intentionally to create a feeling of fear of paranoia. As a result, readers may share the story without checking its authenticity, thereby contributing to the spread of disinformation.

Fact-checking. Activity to check the authenticity or validity of data or statements. In the digital sphere, it also encompasses checking sources and the identity of their publishers. It is a crucial tool to combat disinformation. The impact of fact-checking depends on several factors, including the platform used, the kind of content and users' ideological predisposition. Fact-checkers often use a range of channels and social media to share their work and publicly debunk false content.

Micro-targeting. A marketing and communication strategy which consists of identifying specific audiences and personalizing messages based on collected user data. This leads to greater and more effective acceptance of the message. In disinformation strategies, it is used to identify more susceptible audiences and increase the probability that false, manipulated or half-true content will be believed.

Partisanship. A tendency to support a political party, group or ideology unconditionally, without assessing their arguments critically, even if these are based on misleading statements. This unwavering commitment can lead to biased judgement and decision-making, where loyalty to a political group trumps objective analysis of evidence.

Polarization. The increasing division of society into groups with conflicting ideas, opinions and interests. It occurs when individuals' or groups' ideological positions drift to opposite extremes, making a consensus harder to reach and increasing social conflict. A differentiation is usually made between ideological polarization, which refers to political parties' positioning towards the extremes of the political spectrum, and affective polarization, which refers to sympathy or hostility towards parties, their leaders and their voters, which indicates the level of tension in the public sphere. Polarization is also a communication strategy used by interest groups (e.g. political groups) to attract users by exploiting digital platforms, by using narratives which may include hate speech and disinformation content. It implies a combination of socio-political and communicative phenomena in which rhetoric based on hate speech leads to the spread of prejudice and intolerance in contemporary societies.

Pseudo-media. A publication which imitates journalism in structure and format, and is characterized by breaches of journalism's ethical and professional principles and standards. The term is mostly used to refer to digital publications, although it could also apply to media on other platforms. Pseudo-media platforms defining characteristics are their pursuit of polarization, ideological activism, spreading of conspiracy theories and a general tendency to circulate false, unchecked and extremely biased or partisan content.

Psychographic profiling. Psychological, ideological, socio-economic and ethno-demographic categorization of a person through their personal data and their internet searches and browsing, creating patterns not only of their overt, conscious preferences but also of what they are attracted to and what repulses them at a sub-conscious level. Profiling allows the creation of personalized content aimed at certain individuals, thus improving the efficiency of any sort of micro-targeting or personalized campaigns.

Yellow or tabloid journalism. Sensationalist and exaggerated journalism that prioritizes the more lurid, scandalous or spectacular aspects of reality over objectivity and accuracy of information. It is characterized by the use of attention-grabbing headlines, dramatic language, shocking images and misrepresentation or exaggeration of facts, in order to draw the public's attention and produce a greater emotional impact, even at the cost of truthfulness. Specifically, the ethical and professional principles of journalism are sacrificed in favour of commercial interests and the search for sensationalism, contributing to disinformation and the manipulation of public opinion.

Cybercrime and online threats

Bot farm; Troll farm. Mass organization of bots or trolls, coordinated to create and spread huge numbers of false messages on social media, based on disinformation, abusive and violent content targeting a person or group or certain subjects. The farms can be used to generate confusion, manipulate or divide public opinion, defraud or raise the profile of certain brands or users for commercial or social purposes.

Butterfly attack. Similar to astroturfing but with a different approach: rather than supporting issues or groups pretending to be grassroots movements, it is used to infiltrate, divide and neutralize existing communities, campaigns and groups. In this method, groups of moles or trolls infiltrate these groups or campaigns, whether on social media or in real life, in order to cause division using lies and disinformation. Once they have entered a group, they exploit differences and prejudices within it, creating confusion and discrediting the group. The term was coined by Patrick Ryan in 2017 based on the behaviour of butterflies, which change their fluttering pattern to confuse predators.

Cybersecurity. A set of practices, technologies and processes designed to protect IT systems, networks and devices, as well as the data stored on them, against attacks, harm and unauthorized access. It encompasses several areas such as device, network, information and application security. It also includes identity and access management, incident response, and disaster recovery, guaranteeing Business Continuity.

Cybersquatting. A form of cyber-crime where a person buys or registers a domain which is the same or similar to an existing domain, in order to benefit from a well-known registered brand, trademark or personal name. This kind of crime is commonly used to create phishing pages, scams or fake surveys, in order to gather user data and steal or hijack their online digital identity.

Doxing. A propaganda or information spreading technique whereby the private personal data of a person, group or institution are intentionally revealed to the public. This strategy seeks to cause harm by sharing details such as home address, telephone number, family information, personal details, emails and photographs, among others. Their goal is not only to single out and harm the person targeted, but also to scare, threaten or shame them into ceasing the activities they were previously carrying out. This technique has been used against journalists, politicians, military staff, activists, business people and sportspeople, among others.

Harmful content. Content shared through traditional or digital media which, once published, has a harmful, persistent impact for a significant period. It aims to cause harm towards a specific person or social group. This kind of content appears in different forms, inciting hate, using offensive language, intimidation, harassment and exposure to disinformation content.

Hate speech. Any statement or expression which attacks or uses hostile, uncivil, threatening, offensive, discriminatory or explicitly violent language referring to a group or person based on their ethnicity, nationality, race, gender, ancestry, religion, vulnerability or other forms of identity such as political ideology, language, social or economic origin, disability, health condition or sexual orientation, among others. This kind of discourse is of a public nature and seeks to cause harm and incite violent or discriminatory actions, as it reflects a motive of hate or discrimination. The narrative may be capable of or suited to causing a climate of hate.

Offline / online violence. A strategy which seeks to transfer violent action from the online environment to the physical (offline) world. It seeks to multiply the impact of online campaigns, carrying out actions in both environments, and establishing greater interconnections through the physical interaction of like-minded people. It may include organizing a demonstration linked to an online movement, using media such as radio, press or advertising in general to reinforce an ideological message, and the establishment of in-person meeting places for sympathisers to gather.

Surveillance capitalism. An economic and social model characterized by mass gathering and exploitation of user personal data, in order to generate profits by predicting and modifying behaviour. This system is based on capturing detailed information on the activities, preferences and habits of people, using a range of devices and digital platforms. The information is later analysed and monetized by large technology companies, which use them to develop personalized products and services, as well as to influence individuals' decision-making. Surveillance capitalism has been criticized for its impact on people's privacy, autonomy and freedom, converting their data into a valuable good that is traded without their full consent. Moreover, this model could increase social inequalities and consolidate the power of a small number of corporations globally.

Troll. A person with a hidden real identity who posts provocative or harmful messages on social media, websites or messaging platforms with a specific ideological goal: to create disinformation, boycott or hamper the conversation, cause harm... Their actions are known as "trolling". Trolls often act in coordination with others in what is called a troll farm (see definition).

CONCLUSIONS AND PROPOSALS

This chapter contains 125 terms which are essential to understanding the phenomenon of misinformation, with its implications for national security and the digital environment. The aim of this glossary is to provide insight into different aspects of this field which have an impact on society. Its purpose is to gather, share and publicize key techniques and elements used in the field. It is aimed at media outlets, experts, the education sector, academia and, especially, to wider society as a useful tool.

Although it is an initial proposal that aims to bring together different experts' views on the issue, regular revisions and additions are called for, whether it is through the Forum against Disinformation Campaigns Affecting National Security or through other similar publications. As disinformation evolves, some of these concepts may become obsolete, which is why revisions will be necessary, so that this glossary may remain useful and up to date.

Whilst disinformation is global and affects different countries, the translation of this glossary into other languages will allow it to be used in other contexts, broadening the scope on tactics and tools that transcend national borders. Moreover, there is an opportunity to establish common international frameworks, facilitating collaboration and understanding between experts and researchers from different regions. These translations will also be useful in the field of media and digital literacy.

New challenges related to disinformation such as artificial intelligence, global regulatory potential, immersive reality, privacy and cryptography will also need to be analysed in the future. Although this is but a first step, in itself valuable and necessary, the common language this glossary proposes will prove essential to empowering citizens, academics and professionals in the fight against manipulation and disinformation.

BIBLIOGRAPHY

Aguilar, D. (2023), "How to Use Sock Puppet Accounts to Gather Social Media Intelligence", Maltego Technologies GmbH, https://www.maltego.com/blog/how-to-use-sock-puppet-accounts-to-gather-social-media-intelligence, 22 August.

Arce-García, S., E. Said-Hung and D. Mottareale-Calvanese (2023), "Types of Astroturfing campaigns of disinformative and polarised content in times of pandemic in Spain", *Revista ICONO 14: Revista científica De Comunicación Y Tecnologías Emergentes*, 21(1). https://doi.org/10.7195/ri14.v21i1.1890.

Carrasco Rodríguez, B. (2020), *Information Laundering in Germany*, NATO Strategic Communications Centre of Excellence, https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_information_laundering_in_germany_final_web.pdf

C-Informa (Coalición Informativa contra la desinformación en Venezuela) (2022), "¿Fake, Trolls, Astroturfing? Conoce estos y otros conceptos en el Glosario sobre desinformación", Cazadores de Fake News, https://www.cazadoresdefakenews.info/fake-trolls-astroturfing-conoce-estos-y-otros-conceptos-en-el-glosario-sobre-desinformacion, 29 November.

de Goeij, M. W. R. (2023), "Reflexive Control: Influencing Strategic Behavior", *Parameters*, 53(4), https://doi.org/10.55540/0031-1723.3262.

Departamento de Seguridad Nacional (2023), *Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional*: Trabajos 2023, https://www.dsn.gob.es/sites/default/files/documents/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf.

Disarm Foundation (n.d.), "DISARM Red Framework", https://www.disarm.foundation/framework.

EU Disinfo Lab (2024). "What is the Doppelgänger operation? List of resources", https://www.disinfo.eu/doppelganger-operation, 13 August.

European Commission (2020), C*ommunication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0790, 3 December. (2022), "Developing a better understanding of information suppression by state authorities as an example of foreign information manipulation and interference", https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2023-DEMOCRACY-01-02.

European External Action Service East StratCom Task Force, (2021), "Modus Trollerandi Part 5: Provocations", EUvsDisinfo.eu, https://euvsdisinfo.eu/modus-trollerandi-part-5-provocations, 25 August.

Fridman, O. (2024), *"Defining Foreign Influence and Interference", Institute for National Security Studies (INSS)*, https://www.inss.org.il/publication/influence-and-interference, 4 January.

Giles, K., J. Sherr and A. Seaboyer (2018), “Russian Reflexive Control”, Royal Military College of Canada, https://www.researchgate.net/publication/328562833_Russian_Reflexive_Control.

Goldenziel, J. I. (2021), “Law as a Battlefield: The U.S., China, and the Global Escalation of Lawfare”, *Cornell Law Review,* 106(5). https://www.cornelllawreview.org/wp-content/uploads/2021/09/Goldenziel-final11234.pdf

Harper, N. (2020), “No, you’re not ‘just asking questions.’ You’re spreading disinformation”, Minnesota Reformer, https://minnesotareformer.com/2020/12/17/no-youre-not-just-asking-questions-youre-spreading-disinformation, 17 December.

HybridCoE (The European Centre of Excellence for Countering Hybrid Threats) (n.d.), “Hybrid threats as a concept”, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon.

Lupiáñez Lupiáñez, M. (2023), “Cómo hacer frente a un ataque cognitivo: Prototipo de detección de la propaganda y manipulación en operaciones psicológicas dirigidas a civiles durante un conflicto”, *Revista del Instituto Español de Estudios Estratégicos*, 22, 61-93. https://revista.ieee.es/article/view/6058/7348.

Mannan, S. H. (2019), “Book Review: Projecting Power: How States Use Proxies in Cyberspace”, Journal of National Security Law & Policy 10:445, https://jnslp.com/wp-content/uploads/2020/04/Projecting_Power_How_States_Use_Proxies_in_Cyberspace.pdf.

Ministry of Defence of the Russian Federation (2011), *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space* (Trad. NATO Cooperative Cyber Defence Centre of Excellence), NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), https://ccdcoe.org/uploads/2018/10/Russian_Federation_unofficial_translation.pdf.

NATO (North Atlantic Treaty Organization) (2024), “Countering hybrid threats”, https://www.nato.int/cps/en/natohq/topics_156338.htm, 7 May.

OASIS Open (Organization for the Advancement of Structured Information Standards) (2021), *“STIX™ Version 2.1” (Ed. B. Jordan, R. Piazza and T. Darley)*, https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html, 25 January.

Parliament of Australia (2020), *Report on the conduct of the 2019 federal election and matters related thereto*. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2019Federalelection/Report.

Presidency of the Government of the Kingdom of Spain (2017), *Estrategia de Seguridad Nacional 2017: Un proyecto compartido de todos y para todos*, https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidenciadelgobierno/documents/2017-1824_estrategia_de_seguridad_nacional_esn_doble_pag.pdf.

President of the Russian Federation (2000), “Doctrine of Information Security of the Russian Federation”, https://base.garant.ru/182535/, 9 September.

Rid, T. (2020), *Active Measures. The History of Disinformation and Political Warfare*, New York, Farrar, Straus and Giroux.

Rodríguez-Fernández, L. (2021), *Propaganda digital. Comunicación en tiempos de desinformación*, Editorial UOC.

Sessa, M. G. (2023), "Disinformation glossary: 150+ terms to understand the information disorder", *EU Disinfo Lab*, https://www.disinfo.eu/publications/disinformation-glossary-150-terms-to-understand-the-information-disorder, 30 March.

Sharma, S. (2023), "The biggest names pranked by Russian duo Lexus and Vovan, from Prince Harry to Elton John", *The Independent*. https://www.independent.co.uk/news/world/europe/russian-lexus-vovan-leo-varadkar-prank-call-b2467203.html, 20 December.

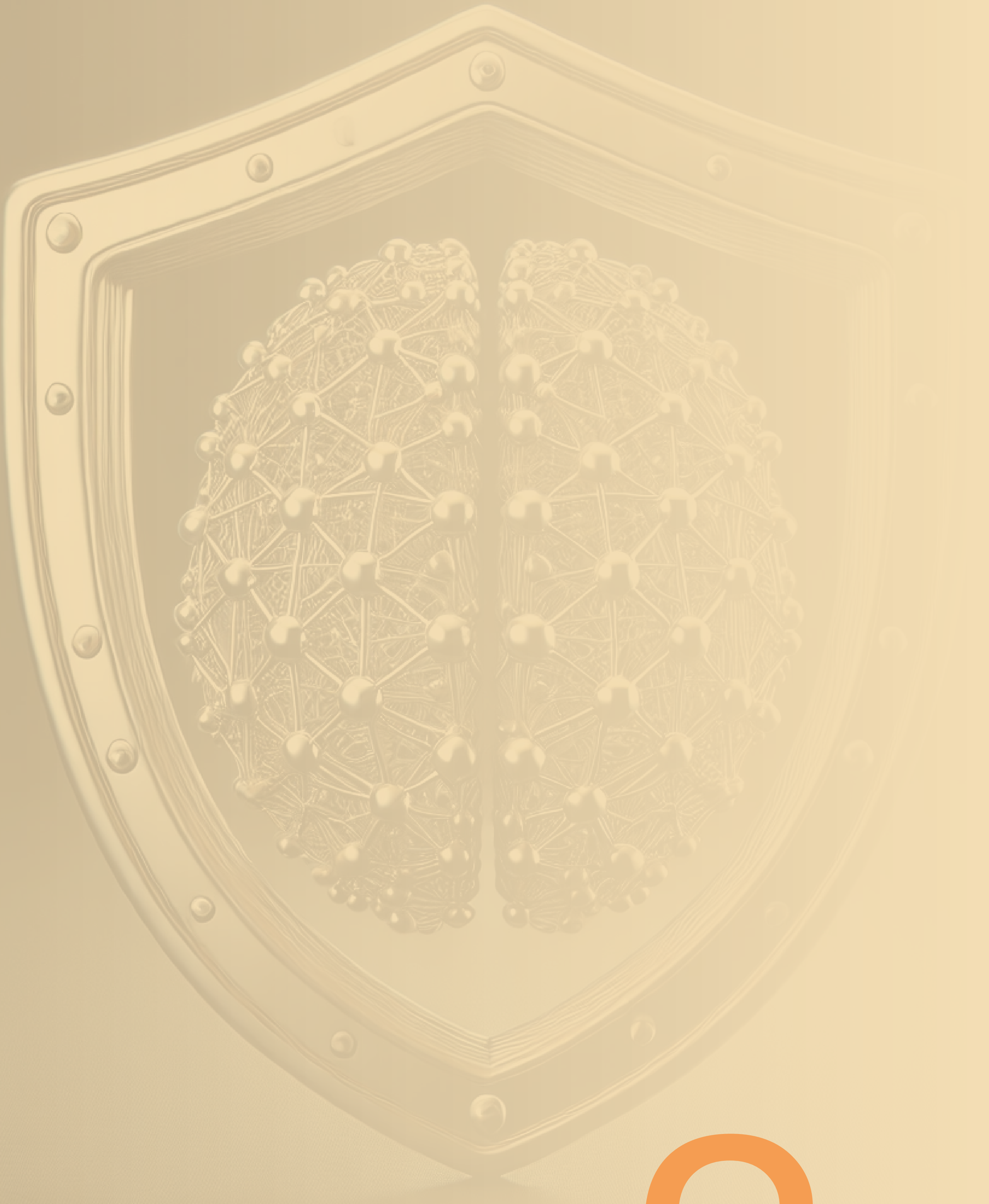
Sitaraman, G. (2023), "Deplatforming", *The Yale Law Journal*, 133(2), 419-668, https://www.yalelawjournal.org/article/deplatforming.

STOA (Scientific Foresight Unit) (2021), *Strategic communications as a key factor in countering hybrid threats*, European Parliament, https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323.

Strategic Communications, Task Forces and Information Analysis (STRAT.2) Data Team (2023), 1st EEAS *Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence, European Union External Action*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

Voyger, M. (2018), "Russian Lawfare – Russia's Weaponisation of International and Domestic Law: Implications for the Region and Policy Recommendations" *Journal on Baltic Security*, 4(2), https://www.researchgate.net/publication/330477790_Russian_Lawfare_-_Russia's_Weaponisation_Of_International_And_Domestic_Law_Implications_For_The_Region_And_Policy_Recommendations.

Zabrisky, Z. (2020). "Big Lies and Rotten Herrings: 17 Kremlin Disinformation Techniques You Need to Know Now", *Byline Times*, https://bylinetimes.com/2020/03/04/big-lies-and-rotten-herrings-17-kremlin-disinformation-techniques-you-need-to-know-now, 4 March.



CHAPTER 2

THE ROLE OF THE MEDIA AND COMMUNICATIONS DEPARTMENTS IN COMBATING DISINFORMATION

Coordinators:

Emilio Lliteras Arañó

Miguel Lopez Quesada

María Penedo

Department of National Security

Authors and contributors:

Emilio Lliteras Arañó

Miguel López-Quesada

María Penedo

Fernando Romero Valderrama

BACKGROUND

Disinformation is an ancient and ever-present concept, and has always been employed to obtain privileged positions in all kinds of societies.

The array of disinformation techniques is vast, but in today's world, the greatest threats relate to the Internet and exploitation of social networks and artificial intelligence. These environments often offer no transparency, social responsibility or legal liability with respect to the person or bodies transmitting such messages, while algorithms increase the visibility of the most extreme content and content that aligns with personal biases, irrespective of the accountability of the source. Given this state of affairs, the fight against disinformation is both vital and high-priority. To combat the narratives of those who are predicting the fall of liberal democracies, it is crucial to immediately and resolutely establish a system to safeguard and protect the predominance of democracies over the various forms of totalitarianism that aim to hide the truth.

The universal right to receive truthful information (Desantes Guanter, 1977), entails recognition of professions that defend freedom of information in the media and in sources.

How can this disinformation crisis be tackled without encroaching on the fundamental rights and freedoms of liberal democracies?

There is a widespread consensus that media literacy must be improved across the board. It is also important to remember that democracies have combated and triumphed over lies and abuses of power—inseparable concepts—thanks to the media, political and social stakeholders and citizens all defending the truth.

Tracking, identifying originators and ensuring that writers are professionally trained and able to bear responsibilities and fact-check and compare information are all vital ingredients of the complex world of public information; they are an essential framework for liberal democracies to be recognized as legitimate defenders of peaceful co-existence.

THE MEDIA AND COMMUNICATIONS DEPARTMENTS, CURBING AND PREVENTING DISINFORMATION

At this time, when defending the truth is a strategic necessity, the media and communications departments of businesses and institutions have a key role to play. They are pillars of a society in which truth, plurality and trust prevail over those who exploit anonymity and a lack of editorial responsibility on social networks to spread lies and stoke polarization and distrust. The visibility of enterprises and their brands, and the reputational, social and legal liability they bear in relation to their information and messages, are a vital counterweight to the impenetrable and secretive world of social networks and algorithms.

The media and such departments comprise qualified professionals who must meet ethical standards and must answer to the society to which they transmit their messages. Even the most sophisticated advances in producing and distributing information are of little value without trustworthy intermediaries whose sole aim is to safeguard the right of citizens and of all of society to receive truthful information.

To effectively combat disinformation, the media, journalists and communications managers must be equipped—as organizations and as professionals—with proper training, experience and proven communication skills, but they must also, especially, be committed to deontological ethics and be fully legally liable.

Many factors have contributed to the rise of deception as a political, economic and military weapon, to radicalize, polarize and undermine democratic values. The focus in this chapter will be on one factor in particular, which greatly affects journalists, the media and communications managers and departments: the end of intermediation by journalism, which just a few years ago was proclaimed by some to be key to making the dream of true democracy a reality. That intermediation, traditionally performed by the media in collaboration with communications departments, was previously demonized, but a decade later is being championed as fundamental. So the question is: Why has there been a shift in the opinion on the value and purpose of traditional media and of public and private communications departments?

The advent of "citizen journalism", as it is sometimes known, which was prophesied to end reliance on the media as indispensable intermediaries when communicating with large audiences, has instead flooded social networks with subterfuge, hoaxes and untruths, spread unchecked by an anonymous army of fabricators of lies, whose intentions are unknown. Even in the best of cases, this "citizen journalism" is barely "amateur journalism"; it is bereft of context and fact-checking, and those who produce it are not bound by the same ethical and vocational responsibilities as professional journalists. In the most extreme cases, this practice has been used as cover by those who spread hate and lies, assisted by bots and fake accounts; they largely go unpunished, as the law does not hold them accountable for the damage caused by the disinformation they propagate.

On the issues of public perception of the media and journalists working therein, and the usefulness of both as reputable and trustworthy sources of information, the following figures are from the First Study on Disinformation (*I Estudio sobre desinformación*) by the Union of Free-to-air Television Broadcasters (Spanish acronym: UTECA) and the University of Navarre, published in June 2022 (UTECA and Universidad de Navarra, 2022). In the survey, 84.6% of respondents said they preferred to obtain information from media outlets rather than social networks, because of the teams of professional journalists who fact-checked, compared and analysed information. In addition, 80.1% answered that the press, radio and television were the best safeguards against the rise of disinformation.

Even so, 88.1% acknowledged that people tend to give greater credence to messages that align with their way of thinking. In terms of the importance attached to the media, when respondents were asked how to combat the spread of disinformation, the most frequent answer (53.4%) was not forwarding or reposting anonymous messages; the second most frequent answer (43.4%) was to obtain information from the television, press or radio to avoid being misled. The results of the survey suggest that the public appreciate having a media and journalists that offer authoritative, truthful, organized information and provide context for it, in accordance with the ethical principles that are followed by responsible, transparent professional organizations.

It is widely known that lies spread more quickly than the truth, as they travel more easily without the burden of scrupulousness. Therefore, to contain the spread of lies, the media and communications managers must act, drawing on rigour, truthfulness, fact-checking and accountability to continuously reaffirm their position as authoritative and paramount sources.

The media, journalists and communications managers must contribute to robust democracies, in which the truth is cherished. It is vital that they perform their work responsibly, to set them apart from those who spread disinformation.

Another means of combating disinformation, with respect to its aim of promoting uniform thinking, is for public and private bodies to foster a plural society through their different areas of work.

The commitment to ethical standards and legal liability of the media and of communications departments is also key to countering disinformation.

In times such as these, it is particularly important for communications professionals to act in accordance with the highest possible ethical standards for their professions: fact-checking information before publishing and always identifying the persons or entities responsible for the information they disseminate under their brand. However, this does not mean that the media, journalists and communications managers never make mistakes in their day-to-day work. When mistakes happen, they have their own protocols to act in a professional, transparent and effective manner, applying codes of ethics for journalism or corporate public relations. Furthermore, natural or legal persons that feel affected by the information published by a media outlet can exercise their right to rectification, pursuant to Organic Law 2/1984 governing the right to rectification. The outlet is thus obliged to publish a rectification; this right does not protect natural or legal persons with regard to information posted on social networks.

To build on this self-imposed accountability, there is a valuable network of professional associations, within which participants constantly examine and share good practices. One reflection of this commitment is the document published in April 2021, entitled "Journalists and communications managers: an ethical commitment for the future"[1] (*Periodistas y directores de comunicación. Un compromiso ético para el futuro*), jointly published by the Spanish Federation of Associations of Journalists (FAPE), the Madrid Press Association (APM), the Association of Economic Information Journalists (APIE) and the Association of Communications Managers (DIRCOM). In addition, numerous media outlets have style guides and codes of ethics that they require their journalists to follow. At the national level, the FAPE code of ethics compiles good practices for members of press associations in Spain.

[1] Available at: https://www.dircom.org/wp-content/uploads/2022/01/Documento_Buenas-Practicas_ES_DBPPD.pdf

ASSETS, TOOLS AND PROCEDURES FOR THE MEDIA IN THE FIGHT AGAINST THE SPREAD OF DISINFORMATION

Media outlets are effective and vital tools in combating the spread of disinformation, not only because they are structured, professional organizations of journalists, but also because they have in-house editorial safeguards, assume responsibility for their content, and are accountable to society. In a world in which many seek to spread distrust and confusion, the media offers context, comparison, analysis and attribution.

Fact-checking using reputable sources is an inextricable part of the profession of journalism. This practice is set out in the codes of ethics of journalism associations, as well as in the style guides, good practices and internal protocols and procedures of public and private sector media outlets.

The assets that most highly valued are the brand of the outlet and the related reputation, which make the media the public's primary source for determining the truthfulness of a current affairs news item received by other means (UTECA & Universidad de Navarra, 2022).

The value of the brand is complemented, boosted and strengthened by the value of the firm itself. In contrast with the hoaxes and other fabrications that circulate freely and anonymously on social networks and instant messaging services, the media champions attribution of the content it disseminates, drawing on the influence of brands and naming of authors. These practices provide the disseminated information with a guarantee of trustworthiness that other channels lack.

As regards organization of work, media outlets are accountable bodies, with internal editorial safeguards for publications, to ensure that the content they distribute—except in the event of occasional mistakes—is truthful and appropriate, and does not promote hate or violence. They also structure information in accordance with professional criteria based on pluralism and multiple viewpoints.

In response to malicious campaigns to portray as disinformation any publicly expressed opinion that goes against a specific way of thinking, it is important for media literacy initiatives to address the difference between opinion and disinformation, the latter being the intentional dissemination of falsehoods to harm a third party. If the opinion is based on a real event or fact, it cannot be dismissed as being disinformation. Being able to disagree with another opinion is part of the freedom of expression; portraying an opinion as disinformation contributes to confusion and distrust of the media. A variety of opinions and approaches to a given event or fact contributes to debate and reflects a plural media and society.

The media face constant challenges and must not give in to temptations. In this new age of artificial intelligence, internal controls must be applied rigorously and reputable and trustworthy sources must be used. In addition, training is required, and technical skills must be constantly updated, to distinguish what is real in a sea of technically faultless fake images.

ASSETS, TOOLS AND PROCEDURES FOR COMMUNICATIONS DEPARTMENTS IN THE PUBLIC AND PRIVATE SECTORS

Communications managers of businesses and institutions, as the public face of communications departments, are now on the front line of the fight against disinformation. They are linked to the social responsibility of the organizations they represent and must put into practice the latter's commitment to accountability to all of society, since their foremost corporate social responsibility is tied specifically to the truthfulness of their messages.

Journalists hold main responsibility for fact-checking. However, when truths relate to public or private organizations, communications managers are also professional disseminators of truthful information (which is vital for the media) from a party or source. The purpose is to act as a counterweight and a safeguard in the complex world of public information, in which the new concept of source-based journalism (Fernández del Moral, 2020) represents a tool that communications managers can employ strategically to ensure that the information published by their departments is truthful.

On account of their capacity to link the media to sources and to produce and transmit information from different agents in society, including high-profile ones such as businesses and institutions, communications managers have a strategic role within organizations. Because of this, they should form part of senior management and decision-making bodies (board of directors or similar).

Businesses' and institutions' communication policies should follow criteria on truthfulness, ease of understanding and clarity with respect to the information provided to the media, customers and society. Communications managers are also bound by ethical commitments in their relations with interest groups and must abstain from promoting, financing or favouring media, networks or profiles that fuel disinformation. Like the media, these managers are responsible for the information they provide as an interested party to the media and journalists, whether off the record or for publication.

THE MEDIA AND COMMUNICATIONS DEPARTMENTS: VITAL INTERACTION

An effective relationship and smooth communication between the media and journalists, on one hand, and communications managers and communications departments, on the other, help to debunk hoaxes and expose lies, benefiting society as a whole, as they make the fight against disinformation more effective.

Media outlets, as disseminators of information, are held in high esteem by companies and bodies, as they are vital intermediaries in communication with society; they are professional organizations of journalists with editorial responsibilities, which compare and check information and have at their disposal mechanisms to make rectifications if incorrect information is published or broadcast.

Likewise, communications departments are used by the media as reliable, responsible and transparent sources of information.

The duty and commitment of the media and journalists to compare and check information before it is disseminated must be duly paralleled by quick and truthful answers from communications managers, always with respect for the independence and the professional criteria of each of the parties.

In their dealings with the media and with journalists, communications managers perform duties relating to “source-based journalism”, acting as accredited suppliers of key, truthful information to halt orchestrated campaigns of disinformation against companies and bodies, which seek to sow distrust, damage reputations and cause financial losses.

For the media, communications departments and communications managers are crucial sources when confirming the truthfulness of viral information, messages and images distributed anonymously online, which often appear to be genuine. In addition, such departments and managers put the media in contact with experts in various areas who are widely recognized as being reputable and credible; authoritative, trustworthy, knowledgeable statements in these areas are crucial to combat disinformation that can affect sensitive subjects such as national security, health, the economy or international relations.

It can be said, therefore, that this interaction is supported by honest and self-analytical professional conduct, contributing to a society that is better informed and thus also better equipped to respond properly to lies and hoaxes that circulate online unchecked.

In short, defending the truth entails close collaboration between media professionals and communications departments of public bodies and businesses, performing an invaluable task in society.

COMMUNICATION AS A DEFENCE AGAINST DISINFORMATION IN CRISIS SITUATIONS

In these times of information overload, crisis situations have become a part of daily life, with multiple ramifications. Disinformation, which in everyday circumstances is already a significant challenge, becomes increasingly challenging in such situations. A crisis, which is characterized by uncertainty and urgency, leads to conditions that call for swift and specific decisions. Messages spread quickly, audiences' expectations become higher and available information is limited.

One of the most important capabilities of communications professionals in such situations is being able to act swiftly and effectively. Communications managers are trained to manage crisis situations in record time, making informed decisions even when information is scarce. This celerity is vital to mitigating the harmful effects of disinformation in crises. Even if one does not have a full picture of a situation, one cannot stop answering questions or break the unspoken agreement with audiences. This gives rise to expectations that should be correctly managed, as should the pressure arising from such situations.

Crises often extend beyond a single business or body, and necessitate collaboration and cooperation with multiple stakeholders. When disinformation prevails and reappears continuously, communications managers must prioritize stronger links with the media, as their first course of action. Mutual trust is essential, to ensure that disseminated information passes quality checks and meets appropriate professional standards.

Collaboration between the public and private sectors is central to effectively managing crises. It is vital to have coordination mechanisms that are almost entirely automated, so that if a crisis is identified, information is shared quickly among the parties involved. They may be public or private entities, which must work together to address threats more effectively. One example of effective collaboration is building a culture within businesses whereby critical events such as cyberattacks are not hidden, and instead immediately reported to the competent authorities. A process of immediate reporting and establishment of early warning systems, such as sensor systems on servers, enables threats to be detected quickly, benefiting the affected organization and improving the entire national security system.

This collaboration also entails businesses relinquishing some of their autonomy, by allowing the authorities to install monitoring tools on their systems. In exchange, these organizations receive early warnings and additional levels of protection. It is not just a case of seeking help when a crisis occurs, but also of building networks for systemic collaboration, which work as structural safety nets. In essence, it is the same as putting together a "reserve force" that—despite not being active all the time—is ready to respond systematically and effectively when required.

Public authorities play a vital role in crisis management. Maintaining stable institutional relations with the public administrations is key to addressing any queries over information that is received or disseminated. This is particularly important for multinationals that must build strong ties with diplomatic missions, including embassies and consulates. It is also vital to foster professional, robust relationships with departments of the Ministry of Foreign Affairs, the intelligence services and other government bodies.

Technology, which is frequently considered a boon when communicating and managing information, can also become counterproductive, especially in relation to disinformation. Institutions, businesses and even NGOs are increasingly losing credibility with civil society (Edelman, 2023) and there are very few effective tools with which to address this challenge.

Therefore, crisis management entails anticipating events through social listening, contextual intelligence and prevention using pre-established systems. These may include simulations, updates to crisis procedures or protocols, ongoing training or continuous monitoring of indicators that may help to identify crises.

One of the keys to effective crisis management is establishing suitable channels for communication and actively engaging with the different audiences concerned. This calls for operational channels for communication. In other words, alternative channels must be ready to operate if the main systems fail. Such planning ensures that communication flows uninterrupted, enabling organizations to act swiftly and retain the trust of the public, even at critical times.

Another crucial aspect of crisis management is understanding the psychology of group behaviour or crowd psychology, and applying sociological knowledge to respond to disinformation practices. Because they are constantly researching consumer behaviour and identifying trends, businesses have a significant advantage. They have successfully identified emerging concerns such as environmentalism, the circular economy, natural fibres and sustainable tourism before many other parties. However, this analysis of trends is not being used to anticipate disinformation or misperceptions that may become embedded in consumers' thinking; and consumers are also voters and citizens. Companies can also be key allies in crisis management and in anticipating potential crises, thanks to their capacity to constantly listen to consumers through opinion polls, market surveys and analysis of consumer trends.

In addition, businesses have multiple channels for communicating with consumers, such as advertising, public relations and communications through influencers. These capabilities can be used to transmit important messages to society, making them valuable allies in the fight against disinformation.

In crisis situations, in addition to conducting traditional polls, it is vital to consider sentiment analysis of social media. Even so, online sentiment does not always reflect reality and is often distorted by orchestrated campaigns using bots or influencers, which are frequently not representative of real public opinion. It is therefore vital to develop and implement mechanisms to distinguish between genuine opinion leaders and more artificial, less spontaneous or less authentic profiles. Communications professionals are constantly assessing the reliability of sources of information; this task is increasingly crucial in a digital environment where many assume what they read online to be true, without questioning it.

It is equally important to recognize that even with sources that are considered reliable, a party may be attempting to manipulate information for their own benefit. In all cases, it is vital to understand that disinformation can come from anywhere. There are no entirely malicious or entirely benevolent actors; disinformation as a tool is used by different entities, irrespective of their geopolitical allegiances. Sometimes, disinformation is structural and forms part of a deliberate strategy. In some settings, an entire society, including communicators, may become actively involved in a disinformation campaign, contributing to creating and perpetuating a false narrative that then becomes part of the community's world-view.

When disinformation becomes structural and is embraced by society, society itself may actively contribute to disseminating it, because it aligns with existing interests or beliefs. In such cases, disinformation is not only a tool for influencing public opinion, but also a malady that transforms perceived reality for large swathes of the population. This is particularly dangerous when disinformation relates to issues of identity, such as race, gender or religion. When an entire society adopts and embraces disinformation, its triumph is sweeping and lasting, with severe repercussions for social and economic progress.

One key element of crisis management is the capacity that a society has to unite around a shared view of a dispute. However, such agreement occurs in only a few areas. On many issues, such as immigration or certain social challenges, societies are divided, and there is no sensation of a shared threat that unites everyone around a single aim. Societies that find themselves in a constant state of crisis also continually perceive themselves to be under threat, giving rise to strong internal unity. In contrast, in more stable and prosperous societies, in which normal conditions persist without meaningful disruption, this feeling of unity and shared focus becomes diluted, potentially weakening shared responses to serious crises.

To support efforts to manage disinformation, not only in crisis situations but also on a day-to-day basis, it is important to give consideration to establishing a national public professional body of communication specialists.

These specialists, who would be trained in state-of-the-art communications techniques and means of combating disinformation, would play a central role in international communications, through diplomatic services and embassies, and also in the public administration at the national and local levels, including ministries, provincial councils and local authorities. Having such a specialized national communications body would enable more effective management of communications content and a swifter and better-coordinated response to threats from disinformation or interference campaigns.

The specialists could be trained through specific qualifications or through the competitive civil service exam system, thus ensuring a capable body of professionals exists with shared knowledge, skills and approaches to management of public communications. Such a distributed structure would facilitate ongoing training of the specialists, thus enabling specific recommendations to be made in crisis situations.

These national communication specialists should be integrated into a wider network, encompassing communications specialists from the private and third sectors, which would be able to effectively counteract hoaxes, manipulation of information and other forms of disinformation. A unified and proactive network would shield society from manipulation of information, and significantly improve stability and trust in public and private entities.

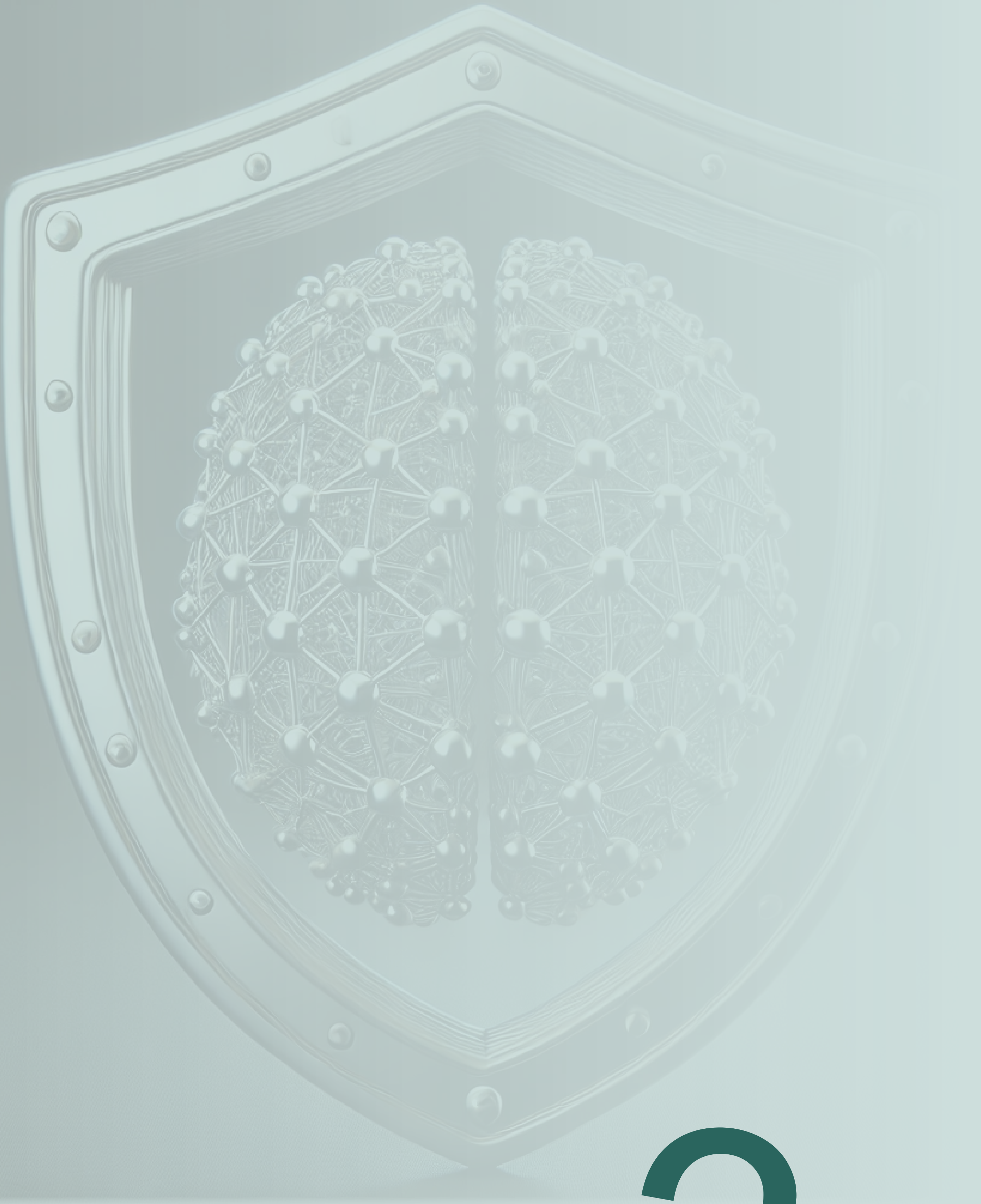
BIBLIOGRAPHY

Desantes Guanter, J. M. (1977), *Fundamentos del Derecho de la información*, Madrid, Confederación Española de Cajas de Ahorro.

Edelman (2023), *Edelman Trust Barometer: Global Report*, https://www.edelman.com/sites/g/files/aatuss191/files/2023-03/2023%20Edelman%20Trust%20Barometer%20Global%20Report%20FINAL.pdf.

Fernández del Moral, J. (2020), "Periodismo de fuente", *Diccionario de la reputación y de los intangibles empresariales*, J. Villafañe and S. Fuetterer (coords.), Madrid, Villafañe & Asociados Consultores, S.L.

Unión de Televisiones Comerciales en Abierto (UTECA) and Universidad de Navarra (2022), *I Estudio sobre la desinformación en España*, https://uteca.tv/wp-content/uploads/2022/06/INFORME-SOBRE-I-ESTUDIO-DESINFORMACION-ESPANA-DE-UTECA-Y-LA-UNIVERSIDAD-DE-NAVARRA-a.pdf.



CHAPTER 3

MONETIZATION OF DISINFORMATION AND THE DISINFORMATION ECONOMY: ANALYSIS OF THE BUSINESS MODEL OF DIGITAL DISINFORMATION OPERATIONS

Coordinators:

Carlos Galán Cordero

Department of National Security

Authors and contributors:

David Arroyo Guardeño

Nicolás de Pedro

Pedro Gómez García

Paula González Nagore

Jesús Manuel Pérez Triana

Nicolás Marchal González

Jania Mier y Teran

Francisco Pérez Bes

Iván Portillo

Jorge Félix Tuñón Navarro

Javier Valencia Martínez de Antoñana

Ministry of Foreign Affairs, European Union and Cooperation

General Commissioner for Information (National Police)

INTRODUCTION

The term disinformation, or foreign information manipulation and interference, refers to those hostile activities that consist in patterns of behaviour in the realm of information displayed by State or non-State foreign actors or their proxies[1], whether domestic or foreign (threat actors). Said patterns of behaviour are coordinated, intentional and manipulative, representing a threat to constitutional values, democratic processes, democratically founded institutions and, therefore, to national security (Department of National Security [DNS], 2021; European External Action Service [EEAS], 2023).

Of particular note among the elements comprising the landscape of orchestrated disinformation campaigns is the amalgam of tactics, techniques and procedures (TTPs) deployed by threat actors, owing to their effectiveness, in pursuit of their strategic goals when engaging in interference in the information space of targeted States. This means that planned actions based on the due selection of the target audience are combined with other measures adopted as and when the opportunity arises, based on tried and tested, but equally effective methodologies.

[1] Entities, organizations or individuals within a State that act on behalf of a foreign actor. They may act as media, marketing or advertising companies, political organizations, interest groups, civil servants or even public figures and influencers. Although they may be located and operate within their own country, these actors disseminate messages or propaganda that benefit a foreign government or entity, against national interests. Proxies are not always directly affiliated with foreign actors, or may sometimes hide such an affiliation, but they can receive support through funding, information or resources. Proxies are used by foreign actors to hide their identity or evade international law. The term also refers to websites used by threat actors as fronts to whitewash their manipulated information content.

One TTP[2] entails the use of purported experts, “guest stars” (National Cryptologic Centre [CCN], 2019) or influencers who enjoy certain credibility among potential audiences. The tactic employed is to have these experts, guest stars or influencers align themselves, directly or indirectly, with the strategic and propaganda interests of the threat actors, for example, by systematically pushing the narratives broadcast by said threat actors’ media outlets, whether these belong to official or covert apparatus. These narratives may sometimes be adapted to the domestic socio-political context, so that messages constituting direct propaganda are not explicit, but rather dressed up as legitimate criticisms that are nonetheless distorted, exploiting the confirmation bias of the target audience. These intermediate actors can therefore be used as subtle but effective weapons of malicious influence with which to weaken support for policies aimed at countering the threat actors’ hostile actions.

This group of actors will typically seek to conceal their links to, or direct interest in, the matters discussed, simulating an apparent spontaneity and neutrality when addressing international and geopolitical topics. However, they may be acting as undercover agents with political, ideological and/or economic agendas and their messages may even form part of a coordinated disinformation strategy of which audiences are unaware.

Financial ties or motives could underlie a number of factors, such as the recurrent use of specific crowdfunding platforms or crypto wallets that facilitate covert financing in the form of donations, some rather opaque, with certain donations standing out because of their recurrent nature or unusually high amount. In such cases, analysts must consider the following two possibilities: 1) the individuals in question regularly push the narrative fostered by the threat actor solely because they have seen that doing so increases their earnings from third-party donations, making them “useful idiots” or “unwitting agents”; or 2) they are aware of the origin of the recurrent payments, irrespective of what efforts the payer may or may not have made to conceal their identity.

Malicious use of content-based recommendation algorithms represents another mechanism for obtaining advertising revenue. This mechanism entails the creation of content for micro-segmented disinformation campaigns necessarily involving a multitude of accounts that can be coordinated to push the narrative more forcefully and can also be used to introduce content into specific communities so as to steer opinion in favour of the threat actors’ interests or, simply, to provoke aggravated and polarizing responses.

Other strategies are more heavily focused on monetizing disinformation campaigns by: placing advertising on ad-hoc websites; using consultancy firms or companies providing strategic services that are supported financially by State actors, private companies or similar organizations to channel funds towards influence and/or cybernetic operations; selling merchandise, books or other products to consolidate the actor’s identity while simultaneously generating revenue; and gathering users’ personal data for subsequent distribution to third parties for profit and to create sophisticated, segmented disinformation campaigns so as to maximize their impact.

Despite efforts to combat disinformation, the presence of websites posting unreliable information has only increased. The owners of these websites also operate other types of websites, including websites focused on entertainment, business or politics; approximately 70% of websites publishing

[2] This document adopts the DISARM framework of reference for describing and analysing the manipulative behaviour of threat actors (DISARM, 2019).

objectively false information advertise business products and services, and almost 40% feature entertainment-related advertising. All of this indicates that these types of websites attract a variety of advertisers who seek to take advantage of the volume of traffic generated on these sites, thus maintaining the flow of revenue towards these disinformation sites.

For example, a little less than half of every 2.16 US dollars spent on news websites in the United States flows to websites that publish disinformation. Despite this, online advertising agencies seek lower-cost advertising spaces, even when they are located on sites posting questionable content, leading to advertising budgets moving from high-quality news websites to controversial low-cost sites (Papadogiannakis et al., 2023).

This situation has arisen because producing manipulated information is extremely cheap and can be highly profitable. The creation and dissemination of these kinds of narratives require very few resources in comparison with legitimate, high-quality reporting. Logically, articles containing objectively false or manipulated information do not need to meet journalistic standards on fact checking and accuracy. Moreover, social media facilitates the rapid and widespread dissemination of this kind of content as the algorithms used by these platforms tend to prioritize the content that generates the most interaction, which often includes distorted or post-truth narratives presented in a sensationalist manner, thus creating a cycle in which this content is circulated both very rapidly and very extensively.

As already mentioned, this kind of content has very low production costs because it does not require professional journalists or rigorous investigation. In addition, the creators of such news pieces can use content generated by third-party users, manipulated or decontextualized images and eye-catching headlines to attract readers' attention, enabling threat actors to maximize their gains with minimal investment (Condliffe, 2017).

Another of the strategies employed is the creation of purported think tanks that focus on geopolitical analysis and make use of known individuals, such as the aforementioned "experts" or "special guests", to offer an apparently greater (but, in fact, baseless) guarantee of the veracity of the narrative broadcast, while at the same time concealing the identity of the entity, organization or agency financing them, or making it difficult to identify them, owing to the excessive complexity of the corporate and/or economic structure supporting them.

In 2020, the University of Oxford (Bradshaw et al., 2020) published a report identifying the cyber troop capacity of numerous countries for conducting disinformation campaigns.

Specifically, the document establishes **Russia** as having a high cyber troop capacity, employing permanent teams operating nationally and internationally and using a wide variety of sophisticated tools and strategies to create and conduct disinformation campaigns, with said campaigns proving particularly effective at amplifying anti-democratic narratives, including for the purpose of interfering in electoral processes in different countries.

China also has a high cyber troop capacity, with permanent, centralized teams of operators. Chinese disinformation campaigns have focused to date on amplifying pro-government narratives and discrediting the government's critics, both at the national and international levels.

Iran too has proven itself to possess a high capacity for information interference, targeting its disinformation campaigns at both national and international audiences using a combination of bots and human-managed accounts to spread pro-government propaganda and attack the opposition.

According to the aforementioned report, **Venezuela** also has significant capacity to conduct disinformation campaigns, using both permanent teams and others operating exclusively in moments of crisis. Disinformation campaigns have been used in Venezuela to support the government and discredit the opposition, with teams organized along military lines to enable the management of large numbers of social media accounts.

All these countries, governed by dictatorial, autocratic or hybrid regimes (Freedom House, 2024; Economist Intelligence Unit, 2023), represent strategic challenges, having the necessary capabilities to deploy information interference actions. For this reason, they were selected as subjects for study and analysis herein.

As a recent example of how such campaigns operate, in September 2024 the United States Department of Justice indicted two employees of a Russian State-controlled media outlet for funding and planning the creation and distribution to US audiences of content with hidden Russian government messaging. This campaign consisted in covertly funding and directing a US-based online content creation company used to publish divisive narratives on various social media channels, including TikTok, Instagram, X and YouTube, most of which were directed to the publicly stated goals of the Russian government (United States Department of Justice, 2024). Fake personas were used to carry out this activity and operations were funded through a network of shell companies to create the impression that the company was financed independently. YouTubers were recruited by offering them vast sums of money and video content was created to achieve a greater impact.

In view of the panorama depicted above, this document seeks, on the one hand, to describe the impact of disinformation campaigns and, on the other, to develop an analysis methodology, based on examination of open-source data, that equips public- and private-sector investigators, journalists and the general public with tools and indicators by which to identify TTPs deployed to monetize disinformation campaigns, with the aim of exposing the economic infrastructure supporting activities undertaken to adulterate the information flows of democratic States.

Although some domestic actors may also make use of these kinds of strategy to obtain financing, this document focuses exclusively on TTPs that can be traced back to foreign State and non-State actors and their proxies, as well as to other parties who, without directly or manifestly engaging in such actions, voluntarily or involuntarily align themselves with the interests of such actors.

We also conducted an analysis, based on both European and Spanish legislation, to determine whether consolidated democracies have the necessary capabilities and legal instruments to address the challenge represented by those threat actors that use disinformation campaigns as a business model for obtaining the financing required to continue funding their own online apparatus, in addition to recruiting potential proxies to spread propaganda and disinformation at a domestic level that is aligned with their interests.

TACTICS, TECHNIQUES AND PROCEDURES USED

As regards the TTPs used by threat actors, an initial analysis procedure was designed. This entailed deciding which tools from the DISARM methodology should be considered.

DISARM is a master framework that seeks to tackle disinformation through data analysis and sharing, drawing on global cybersecurity best practices. DISARM is used to help analysts gain a clear shared understanding of disinformation incidents and to immediately identify defensive and mitigation actions available to them.

To focus on the established objectives of our analysis, we only considered the DISARM TTPs (see list in APPENDIX I) with clear implications for the economic impact of disinformation campaigns and their possible monetization by threat actors.

RUSSIA

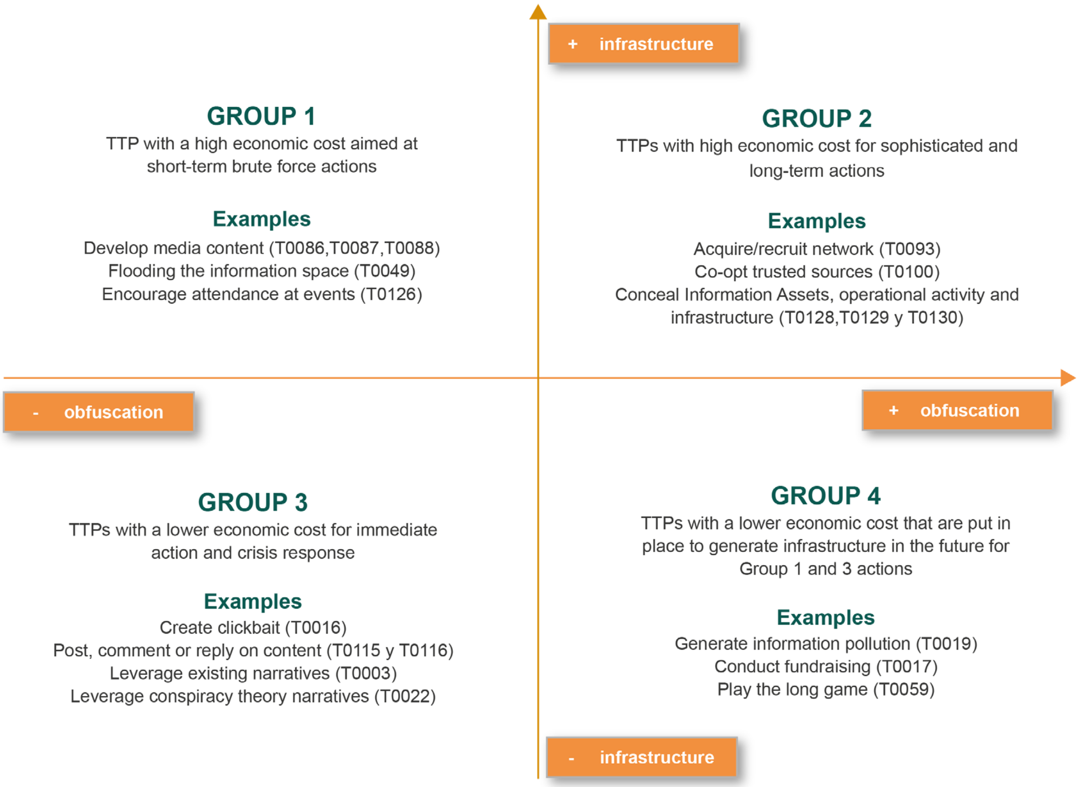
Any analysis of the TTPs comprising the monetization mechanisms used by Russia must necessarily consider a number of different dimensions. Taking the TTPs identified for the framework of this study as our basis, said analysis entails seeking answers to the following questions:

What costs are involved? Is obfuscation necessary? What infrastructure capacity is required?

The financial cost of each of the tactics defined relates to the infrastructure required to carry out the action and includes the expenditure incurred to build, maintain and operate said infrastructure.

The TTPs used by Russia include acquiring or recruiting existing networks (T0093), developing owned media assets (T0095) and co-opting trusted sources (T0100), all of which are actions with high economic and logistical costs. The need for obfuscation may lead to additional costs. Tactics such as that of concealing information assets, operational activity or infrastructure (T0128, T0129 and T0130) are examples of TTPs used to prevent identification of the actor behind a disinformation campaign. Building and funding the infrastructure required to activate a network of social media users (excluding bots and farms) to spread a message in an organic manner requires a highly coordinated system. Moreover, organizing said accounts to avoid any direct links to an autocratic State entails an additional cost—that of the time involved—which is ultimately also an economic factor.

Following this reflection, it is necessary to determine, for each State included in the study, whether it invests more in obfuscation or in infrastructure, thus helping to explain why it might favour certain TTPs over others.



+ infrastructure

GROUP 1

TTP with a high economic cost aimed at short-term brute force actions

Examples

Develop media content (T0086,T0087,T0088)
Flooding the information space (T0049)
Encourage attendance at events (T0126)

GROUP 2

TTPs with high economic cost for sophisticated and long-term actions

Examples

Acquire/recruit network (T0093)
Co-opt trusted sources (T0100)
Conceal Information Assets, operational activity and infrastructure (T0128,T0129 y T0130)

- obfuscation

+ obfuscation

GROUP 3

TTPs with a lower economic cost for immediate action and crisis response

Examples

Create clickbait (T0016)
Post, comment or reply on content (T0115 y T0116)
Leverage existing narratives (T0003)
Leverage conspiracy theory narratives (T0022)

GROUP 4

TTPs with a lower economic cost that are put in place to generate infrastructure in the future for Group 1 and 3 actions

Examples

Generate information pollution (T0019)
Conduct fundraising (T0017)
Play the long game (T0059)

- infrastructure

Figure 1. Categorization of TTPs according to the need for infrastructure and obfuscation. Based on the proposed scheme, we can say that Russia is a versatile actor, utilizing all four categories of TTP depending on the specific situation. There may be occasions when loss of capacity for obfuscation is considered an acceptable price for increased effectiveness and capacity to act, when Russia may employ category 1 and 3 TTPs while utilizing category 2 and 4 TTPs in the background.

Is cost a consideration?

Although certain tactics entail a greater economic cost than others, Russia will typically use any medium or resource at its disposal to engage in disinformation. The influence and disinformation campaigns analysed and attributed to Russia—whether carried out directly or through third parties—include both highly intricate actions aimed at concealing the organization behind them, and other, less intricate, direct actions, such as those carried out by Russia using its own official channels, or with the assistance of spokespersons who push the country's strategic narratives irrespective of how exposed this may leave them.

1. An example of an intricate operation was that analysed and written about by France's Service for Vigilance and Protection against Foreign Digital Interference [VIGINUM], 2024a). This operation, known both as the Pravda network and as Portal Kombat, consisted in the creation and expansion of a pro-Russian propaganda network.

2. Among the operations carried out by Russia through its official channels is that which followed the onset of the war with Ukraine in 2022 and the EU's ban on Russian State media outlets RT and Sputnik. This operation entailed coordination of messages and narratives on the conflict posted on official Western social media accounts belonging to embassies and consulates located in the West and in Latin America.

3. An example of an operation carried out through a strategic spokesperson is that featuring Robert Kennedy Jr., a public figure identified on numerous media platforms as pushing a narrative aligned with Russian interests, posting on geostrategic issues such as Russia's war of aggression against Ukraine, and US policy, in addition to sharing conspiracy theories during the Covid-19 pandemic (Kerr, 2023; Sammarco, 2024; Novelo, 2024).

For all the above reasons, we can conclude that Russia is playing the long game with its action plan to continue its influence operations, which it prepares and carries out with a medium to high level of obfuscation and variable investment in infrastructure, while simultaneously engaging in other immediate operations that require less obfuscation and even make use of pre-established resources, such as influencers, channels of communication, strategic narratives and appropriate media and websites.[3] This requires the necessary economic resources and an understanding of where and when to invest them, without truly ruling out any options. This strategy is clearly in

[3] In October 2024 the Center for Defense Reforms—a Ukrainian not-for-profit think tank—published a report exposing media outlets and actors it believed to have acted or to be acting in the interests of the Kremlin, or to be aligned with its propaganda and disinformation strategy. This report, published under the umbrella of the Ukraine-NATO platform for the early detection and countering of hybrid threats, provides grounds for its findings and was produced following a methodology designed by the Center for Defense Reforms itself. These actors, or "agents of influence", are considered to enjoy an inherent level of trust within society, given that they are seen as experts in security, defence and international relations, enabling them to exert direct and indirect influence in decision-making processes. As regards the media, according to the Center for Defense Reforms report, the website Rebelión, which publishes non-original content, has been using fake profiles under which to publish content (T0009). One such profile is that of "María Mercedes Blanco Reyes", used to post numerous articles on the site (see https://rebelion.org/autor/maria-mercedes-blanco-reyes/) and on other websites based in dictatorial States (see https://www.5septiembre.cu/author/maria/) or on sites seeking to generate social polarization (see https://www.tercerainformacion.es/opinion/27/10/2024/la-co-operacion-ucraniana-con-los-terroristas-africanos-la-verdad-o-desinformacion/). These articles are easy to duplicate on other platforms owing to a licence permitting their distribution free of charge in other sources provided that the author is referenced.

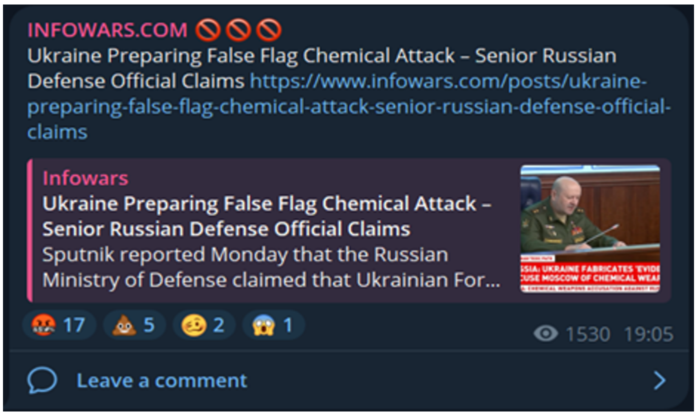
opposition to that of other countries featured in this study, whose situations are very different to that of Russia. Venezuela, for example, has fewer economic resources and therefore has more limited options as regards both infrastructure and obfuscation, whereas Iran and China both have far greater need for obfuscation owing to their operations and strategic goals and endeavour to move in the shadows that help conceal their movements and actual interests..

Does Russia favour direct action or action carried out through third parties?

To answer this question, we looked to previous investigations into actions attributed to the Russian Federation, such as the investigations conducted into online media outlet RNN (VIGINUM, 2023) and into the Matryoshka campaign (VIGINUM, 2024b), as well as the Roller Coaster report published by the Ukrainian media outlet Texty.org.ua. Our examination of the fifty-five TTPs identified for this study led us to pinpoint a specific factor that must be taken into account when analysing the financing mechanisms used: whether or not a particular TTP can be carried out through owned media assets or requires third-party involvement; particular attention should be paid here to those cases in which Russia opts to delegate actions to others even though it could carry them out itself. In this regard, we concluded that almost all the TTPs selected could be carried out by Russia directly, although in some specific cases it prefers to use third parties or avail itself of content created by foreign actors:

- Leveraging conspiracy theory narratives (T0022). For example, an article published in 2023 by the Russian State media outlet Sputnik (Sputnik, 2023).

- Using chat apps (T0043).

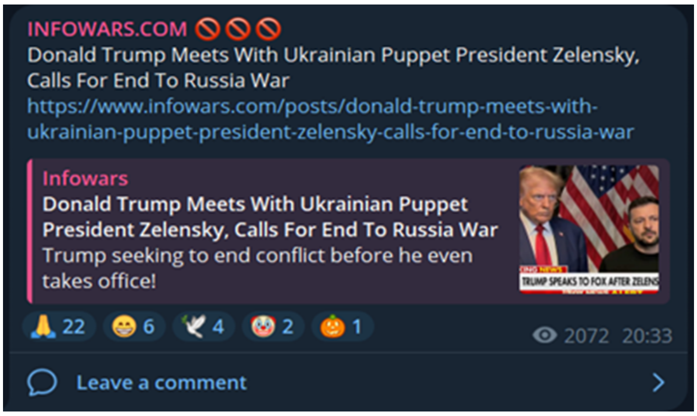


INFOWARS.COM 🚫🚫🚫
Ukraine Preparing False Flag Chemical Attack – Senior Russian Defense Official Claims https://www.infowars.com/posts/ukraine-preparing-false-flag-chemical-attack-senior-russian-defense-official-claims

Infowars
Ukraine Preparing False Flag Chemical Attack – Senior Russian Defense Official Claims
Sputnik reported Monday that the Russian Ministry of Defense claimed that Ukrainian For...

🤬 17 💩 5 🥴 2 😱 1 👁 1530 19:05

Leave a comment

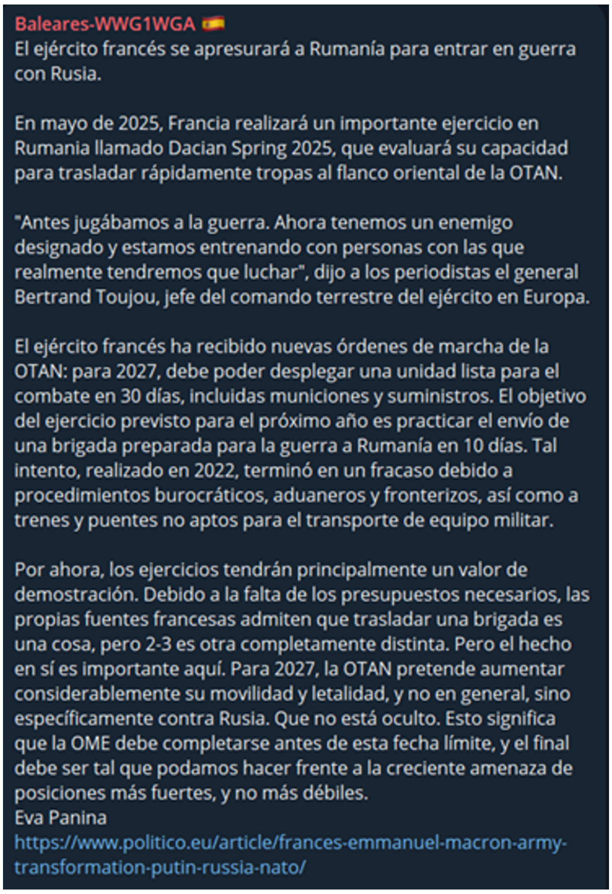


INFOWARS.COM 🚫🚫🚫
Donald Trump Meets With Ukrainian Puppet President Zelensky, Calls For End To Russia War
https://www.infowars.com/posts/donald-trump-meets-with-ukrainian-puppet-president-zelensky-calls-for-end-to-russia-war

Infowars
Donald Trump Meets With Ukrainian Puppet President Zelensky, Calls For End To Russia War
Trump seeking to end conflict before he even takes office!

🙏 22 😁 6 🕊 4 🤡 2 🎃 1 👁 2072 20:33

Leave a comment



Baleares-WWG1WGA 🇪🇸

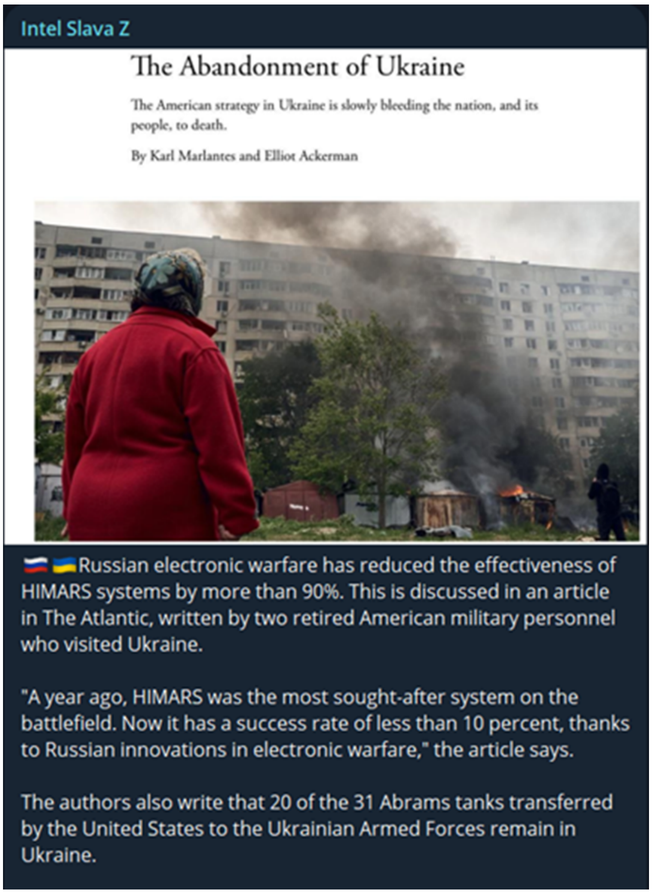
El ejército francés se apresurará a Rumanía para entrar en guerra con Rusia.

En mayo de 2025, Francia realizará un importante ejercicio en Rumania llamado Dacian Spring 2025, que evaluará su capacidad para trasladar rápidamente tropas al flanco oriental de la OTAN.

"Antes jugábamos a la guerra. Ahora tenemos un enemigo designado y estamos entrenando con personas con las que realmente tendremos que luchar", dijo a los periodistas el general Bertrand Toujou, jefe del comando terrestre del ejército en Europa.

El ejército francés ha recibido nuevas órdenes de marcha de la OTAN: para 2027, debe poder desplegar una unidad lista para el combate en 30 días, incluidas municiones y suministros. El objetivo del ejercicio previsto para el próximo año es practicar el envío de una brigada preparada para la guerra a Rumanía en 10 días. Tal intento, realizado en 2022, terminó en un fracaso debido a procedimientos burocráticos, aduaneros y fronterizos, así como a trenes y puentes no aptos para el transporte de equipo militar.

Por ahora, los ejercicios tendrán principalmente un valor de demostración. Debido a la falta de los presupuestos necesarios, las propias fuentes francesas admiten que trasladar una brigada es una cosa, pero 2-3 es otra completamente distinta. Pero el hecho en sí es importante aquí. Para 2027, la OTAN pretende aumentar considerablemente su movilidad y letalidad, y no en general, sino específicamente contra Rusia. Que no está oculto. Esto significa que la OME debe completarse antes de esta fecha límite, y el final debe ser tal que podamos hacer frente a la creciente amenaza de posiciones más fuertes, y no más débiles.
Eva Panina
https://www.politico.eu/article/frances-emmanuel-macron-army-transformation-putin-russia-nato/



Intel Slava Z

The Abandonment of Ukraine

The American strategy in Ukraine is slowly bleeding the nation, and its people, to death.

By Karl Marlantes and Elliot Ackerman

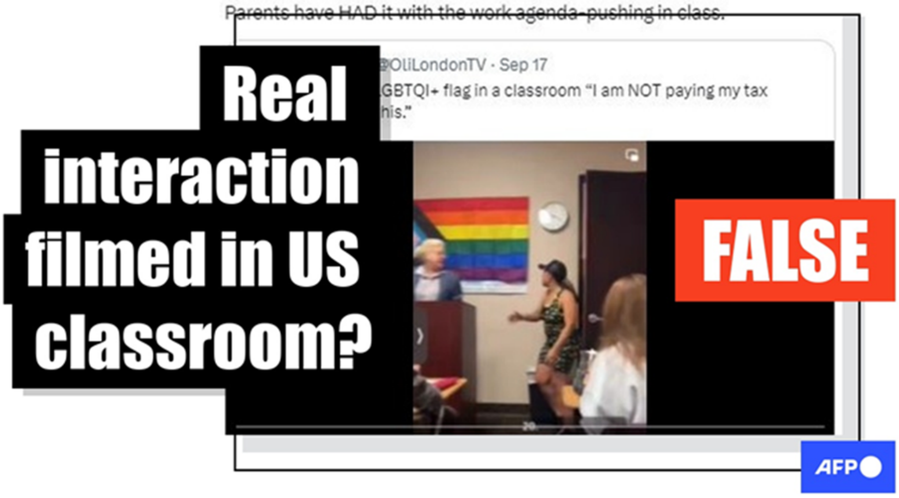
🇷🇺🇺🇦Russian electronic warfare has reduced the effectiveness of HIMARS systems by more than 90%. This is discussed in an article in The Atlantic, written by two retired American military personnel who visited Ukraine.

"A year ago, HIMARS was the most sought-after system on the battlefield. Now it has a success rate of less than 10 percent, thanks to Russian innovations in electronic warfare," the article says.

The authors also write that 20 of the 31 Abrams tanks transferred by the United States to the Ukrainian Armed Forces remain in Ukraine.

Examples of messages published on unofficial Telegram channels of Russia with pro-Russian narratives: (https://t.me/InfowarsChat/188036, https://t.me/infowarslive/39160, https://t.me/BalearesWWG1WGA/39155, https://t.me/intelslava/67942)

- Creating Clickbait (T0016)


Parents have HAD it with the work agenda-pushing in class.

@OliLondonTV · Sep 17

GBTQI+ flag in a classroom "I am NOT paying my tax his."

Video disseminated using a clickbait headline (AFP, 2023) about alleged anti-LGBTI propaganda in the United States. The analysis was conducted after the video was posted on Elon Musk's official Twitter account and by other Twitter users. The same video was mentioned on Hungarian media (Zubor, 2023) after having been disseminated by Russian social media platform VK and by Hungarian groups such as Szent István Légiója (Saint Stephen's Legion), which has been linked (Solymos and Panyi, 2023) to the Russian intelligence services and the disinformation network NewsFront (Global Engagement Center [GEC], 2020a).

The analysis conducted to determine the mechanisms used by Russia to finance its disinformation campaigns shows that both for Russia and for any other actor seeking to undertake disinformation actions or influence campaigns, the first decision to be made is whether the action should be carried out by the actor itself or through third parties.

This decision is crucial because if Russia carries out the actions itself it can control all aspects of the process, thus facilitating the obtainment of financing. By contrast, if the action is carried out through third parties, there is the added complexity of how to ensure the financing reaches the actor that is to carry out the action or take part in the campaign.

It is clear that there are actions that Russia can, if it so chooses, carry out for itself, through assets such as media outlets managed through companies that are ultimately controlled by the government, through its own official channels, etc. By contrast, if the aim is to generate content through other media, influencers or other channels producing digital media impacts, other resources are necessary. The simplest solution to this problem is to use the means made available by digital platforms themselves.

How does Russia finance actions carried out through third parties?

We selected a sample of actors with alleged pro-Russian connections, including social media profiles and websites, based on the findings of the following third-party investigations:

- Roller Coaster (Gadzynska et al., 2024).
- RNN (VIGINUM, 2023).
- Portal Kombat (VIGINUM, 2024a).
- Matriochka (VIGINUM, 2024b).

We then identified the websites and social media platforms used by the sample group to circulate content, as well as the financing systems embedded within said websites and platforms that are made available to third parties to enable them to support their activities. These websites and platforms, ranked from the most to the least used, are:

- **Fundraising and subscription platforms:** This category includes websites such as GoFundMe, Ko-fi, Buy Me a Coffee, GiveSendGo, SendATip, Patreon and Anedot, which are largely used for stand-alone payments but also for subscriptions, as well as SubscribeStar, which is specifically for subscriptions.

- **Social media subscriptions:** Although monitoring donors is very complicated, we were able to determine that several of the actors analysed have streaming channels on Twitch, YouTube or Kick through which they receive monthly subscriptions as well as one-off donations received while streaming. The platform of members of the social network X (formerly Twitter) also falls into this category.

- **Merchandising stores:** These are predominantly websites' own merchandising stores selling promotional products such as caps, shirts, sweatshirts, books and stationary. E-commerce websites such as Shopify, BigCommerce, WooCommerce, Adobe Commerce (formerly Magento), Wix eCommerce, Squarespace, PrestaShop, Shift4Shop, Weebly, Volusion and Ecwid are also used. However, e-commerce websites are used less frequently than merchandising stores, probably owing to maintenance costs.

- **P2P payment platforms and website donation sections:** This category encompasses a wide variety of options, including larger platforms, such as PayPal, which are used by a number of actors, as well as smaller platforms used on a much more residual basis, above all in countries such as the United States, where links to GabPay were also identified. In addition, we found that almost every actor with their own website includes a donation section on it to facilitate project funding.

- **Crypto wallets and crypto exchanges:** These options are used to a similar extent as merchandising stores and website donation sections. We even found references to wallets for the main cryptocurrencies (including Bitcoin, Ethereum, Solana, Cardano, Monero, USDT, Matic and USDC) in website donation sections. By contrast, we did not identify any actors sharing accounts on crypto exchanges such as Binance or Coinbase, probably because such platforms require identification of both the donor and the recipient. APPENDIX IV contains further information on the use of crypto assets as a source of financing.

- **Crowdfunding platforms:** A small number of campaigns were detected on crowdfunding platforms such as Kickstarter. In addition, we identified crowdfunding sections containing direct requests for donations embedded in actors' own websites.

Based on our analysis of these financing models, the questions that must be answered in order to assess the cost or complexity of channelling financing through these media are as follows:

- **Does it cost anything to use the financing medium? There are three possibilities:**

    - The system is free of charge for the recipient; this may be the case with cryptocurrencies, P2P payment platforms, and owned media assets, depending on the payment gateway used.

    - The system entails a cost or fee per transaction, which is the case for some subscription, e-commerce and fundraising platforms.

    - The system also entails some maintenance costs, in the case of some e-commerce and streaming platforms.

- **Does the financing medium require identification of the transaction recipient?** We found that the vast majority of such channels do require the actor receiving the money to identify themselves for tax purposes by means of a national identity document number or corporate identification number. This requirement forms part of the Know Your Customer (KYC) policies of these platforms. The only possible exception in this regard are crypto wallets; however, this depends on the crypto wallet used and whether the aim of the transaction is to convert cryptocurrency into a fiat currency, in which case such identification is required.

- **Does the donor need to identify themselves?** We found that the majority of channels do not require donor identification beyond that pertaining to the payment method employed; however, there are ways to avoid such identification. The only exception in this case are P2P payment platforms and cryptocurrency exchanges, which do require complete identification of users, including both payers and payees.

It is clearly vital for a country such as Russia that its third-party actors use platforms permitting the lowest-cost methods of financing possible, and in which the donor's identity can be concealed. This means that the financing mechanisms most frequently used by Russia to pay third parties to participate in their disinformation and influence campaigns are:

1. Self-managed financing channels, such as online merchandising stores or donation gateways on the actor's own website, with the only cost being that of hosting the website and the payment gateway.

2. Crypto wallets, which are an even safer mechanism for obfuscating transactions, than self-managed financing channels. However, cryptocurrency does ultimately

need to be converted into a fiat currency in order to be used, meaning that crypto wallets represent a different risk.

3. Fundraising platforms, which may even be free of charge for recipients, with the sole cost being a small commission for each payment received.

4. Streaming platforms, through which periodic donations can be easily channelled owing to their lack of transparency regarding lists of subscribers, members, and donations received while content is streaming, despite the greater difficulty of avoiding identification by means of payment method on these platforms than in the other channels featured in this analysis.

Consequently, from a financial perspective it would not, a priori, make sense for Russia to use e-commerce platforms, which are unpopular among disinformation actors owing to the maintenance costs involved, P2P platforms, given the requirement that both payer and payee be identified, or crowdfunding platforms, which are also unpopular among disinformation actors and are usually managed through fundraising platforms..

CHINA

Disinformation: Beijing's key asset in the new Cold War

The Strategic Concept adopted by the North Atlantic Treaty Organization (NATO) at the June 2022 summit held in Madrid could, in a certain manner, be said to officially recognize a new geopolitical world map defined by opposing blocs—almost like a modern-day version of the Cold War. On one side are the NATO countries and their partners, and on the other are China and Russia and their allies. This new scenario had already been perceived in Europe before the summit, especially after Russia's invasion of Ukraine in February of the same year (Hernández, 2022). That event can be said to mark the beginning of an appreciable change in the public image of certain countries, as shown by the Barometer report published by the Elcano Royal Institute just a few days before the high-level NATO summit, which asserted not only that Spaniards' perception of Russia had deteriorated sharply, but that the war in Ukraine was seen as Europe's greatest problem and a threat to the security of the entire continent. The Barometer report also referred to a slight increase in support for Spain's membership of NATO (González Enríquez and Martínez Romera, 2022).

The Madrid summit vested NATO with renewed vigour, even surpassing experts' expectations in some respects. The analysts Arteaga and Simón (2022), for example, compared the outcomes of the summit with forecasts made in December 2021, concluding that the Madrid Strategic Concept had laid the foundations for a much closer relationship between Europe and North America—a relationship already strengthened by Russia's invasion of Ukraine, which had even resulted in "new members, such as the neutral Sweden and Finland" deciding to join the Alliance. Moreover, the Strategic Concept has extended the "regions of strategic interest"—formerly referred to as "flanks"— to include the Middle East, North Africa and the Sahel.

Arteaga and Simón also mention, as signs of increased strength, the commitment made by all NATO members to increasing defence spending by at least 2% of domestic GDP, and to making NATO the leading international organization when it comes to understanding and adapting to the impact of climate change on security. Lastly, they underscore the commitment made to adapting

NATO's stance on conflicts in "all domains (land, sea, air, outer space and cyberspace) and in their conventional and non-conventional forms (hybrid war)", as well as the establishment of a common fund to finance the development of defence technology (Arteaga and Simón, 2022), revitalizing its operations and making them more flexible in responding to new challenges such as terrorism, migration and disinformation (Priego, 2022). Disinformation, perpetrated by Russia, is understood as a clear threat to the security and stability of NATO allies, and the strategic and systemic long-term risk represented by China is also identified (Arteaga and Simón, 2021).

It seems clear that NATO's repositioning (Hao, 2022) with respect to China is the most palpable sign of the entry into a new Cold War, one whose main actors—United States, China, Russia and the European Union—are performing in a complex setting (Aguirre, 2022). In this Cold War, digital technologies play a key role, constituting one of the main resources for devising hybrid threats. According to diverse EU reports (European Parliament, 2021), said technologies facilitate the creation of large volumes of information which is rapidly circulated and can be weaponized, increasing the influence of States through soft power (Repnikova, 2022). Consequently, and as observed in NATO's new Strategic Concept, the combination of soft and hard power in the form of hybrid threats has become a key geostrategic tool, used especially by China to expand its influence (Luna, 2022), through campaigns which habitually blend propaganda (De la Cal, 2022c) with disinformation (Milosevich-Juaristi, 2020).

Chinese narratives and disinformation campaigns

In the case of the Asian giant, the Communist Party of China (CPC) is the organization that has for several decades been managing the political narrative within the country's borders—maintaining an iron grip on both conventional media (Belinchón, 2022) and digital media (T0002)—while simultaneously investing an equal amount of effort in curating the country's image abroad, focusing, for the time being, on Chinese-speaking communities living abroad and on foreign correspondents posted to China.

Despite the image that some may have of China as the epitome of an isolationist country (M. Martín, 2021), over the past decade the CPC has intensified its efforts (International Republican Institute [IRI], 2022) to shape the content and narratives of media from all over the world (Dubow et al., 2022) and media in different languages (Cook, 2020), defending a world order aligned with its interests. The narrative fostered is based on the idea of a new international consensus, in which the People's Republic will be one of the main actors responsible for the governance of a *new multipolar world* (Delage, 2019), an idea implicit in its age-old culture[4], in which the country is represented as the centre of the world and the origin of civilization (Hernández and García, 2021).

[4] The citizens of China call their country Zhongguo, meaning something akin to "State" or "central town", and later "central nation". The origin of this expression may be geographical, although its use has changed as the country has expanded, coming to refer to a central Chinese culture that is both distinct and superior. Another essential concept in Chinese thinking is that of Tianxia, or "everything under the sky", which alludes to the age-old imperial identity of the country as a civilizing culture, and as a culture whose legitimacy was conferred on it—as embodied by its emperor—by the heavens. These principles have survived for centuries in Chinese culture, which has shown itself to be open to peoples of similar cultural resources, who have thus attained a higher level of civilization.

China's diplomats and official media systematically champion this "multipolar world,"[5] a concept with which China seeks to increase its international influence, applying a strategy (Brime, 2021) of "divide and conquer" (T0079/T0077).

Under Xi Jinping's leadership, the CPC has adopted a more aggressive and comprehensive approach in its efforts to extend Chinese influence, frequently employing strategies aimed, according to Cook (2020), at undermining "international norms and fundamental features of democratic governance, including transparency, the rule of law, and fair competition" (T0127/T0066).

China allocates considerable resources to strengthening its soft power, with both the country's State media and its international partnerships playing an essential role in promoting a positive image of the regime, which is especially significant in those territories of the country in which the human rights of certain ethnic minorities are being systematically attacked (De la Cal, 2022b). Thanks to this investment, the tentacles of China's media apparatus have continued to extend their reach across the globe over the past decade. Among the most influential state-owned media outlets in Beijing's communication ecosystem, six are particularly notable (Cook, 2020): the television networks China Global Television Network (CGTN) and China Central Television (CCTV), the newspapers China Daily and People's Daily, the broadcasting company China Radio International (CRI), and the news agencies Xinhua and China News Service (CNS). In addition, the CPC has also increased its sway over media from all over the world through a complex network (Rathbone and Sevastopulo, 2022) of collaborations, partnerships, influence (Corera, 2020; Global Influence Operations Report, 2022; Nimmo, 2022; Reuters, 2022) and acquisitions, with said media having their own communications ecosystem as a base of operations. Beijing disseminates its narrative through this network adopting the editorial lines of the foreign media exploited, making it more difficult for the origin of propagandistic information to be identified, while simultaneously increasing its persuasiveness.

The strategic value of the digital ecosystem for Chinese disinformation campaigns

In recent years, the digital ecosystem has been consolidated as the principal space through which Beijing spreads information, a playing field for promoting the ideas constituting Xi Jinping Thought (Abril, 2022).

In the domestic sphere, the CPC controls the information circulating in Chinese cyberspace through the Golden Shield Project, which was launched at the beginning of the twenty-first century. With this programme, also known as the Great Digital Wall of China and the Great Chinese Firewall, Beijing maintains an iron grip on the information that reaches the population within its borders, ensuring that any post or news piece that criticizes or contradicts the regime is quickly detected

[5] For example: Zhang Meifang [@CGMeifangZhang]. (2022, 28 October). #Latest After Putin's remarks on China-Russia relations on Thursday, Chinese observers said the close interactions between the two countries in the future will drive the world toward a more just, effective and multipolar global order. View: https://pbs.twimg.com/media/FgLNJvNXgAMKDi6?format=jpg&name=small [Image attached] [Post]. X. https://twitter.com/CGMeifangZhang/status/1586055594288422912

and neutralized (T0047), running constant system updates to guarantee its efficacy (Wu and Lam, 2017).

As previously stated, the CPC's power in this realm is absolute; not even slightly dissident narratives escape their attention and control[6]. A recent example (Hernández, 2022) is the censorship placed on any kind of protest (Radio Televisión Española [RTVE], 2022) regarding China's zero-Covid policies (De la Cal, 2022d; Abril and Bonet Bailén, 2022), including protests using blank sheets of paper as a symbol of dissent (Pollard and Goh, 2022). The display of blank canvases as banners has been prohibited and there is no space or tolerance for any kind of intellectual expression that does not exactly reflect the regime's dictates (Araújo, 2022) (T0123).

As regards corporate actors, it should be highlighted that the tech companies operating in China are exclusively national enterprises. Instead of Google, Amazon, WhatsApp and X, the people of China use Baidu, Alibaba, Tencent, Weibo and WeChat (Yam, 2022). These tech giants are working to develop ever-more sophisticated algorithms capable of meeting the regime's censorship and surveillance requirements, as recently indicated in an assessment conducted by the US National Intelligence Council (National Intelligence Council [NIC], 2020). Thus, under CPC guidelines, these organizations are leading the digitalization[7] of national information while at the same time many of them are expanding on the international market (Cook, 2020, p. 17). Given this situation, Chinese citizens critical of Jinping have had to look for other means of escaping censorship, such as using AirDrop (Cheung, 2022) or availing themselves of fake passports when they have been left with no other option than to leave the country (De la Cal, 2022a).

Outside China's borders, however, Beijing makes use of Western platforms (T0059). As is common knowledge, the digital ecosystem is the main source of information for young people, who are usually unfamiliar with print press and, in general, do not watch news programmes on traditional television, but turn to digital platforms on which they select the information they wish to receive, even when the quality of this information is more than questionable.

The rise in the use of social media for the purposes of disinformation is favoured the world over by factors such as the difficulty of identifying the persons or entities responsible for the content posted, and the wide range of channels available for its dissemination (Bartolomé, 2021). For these reasons, Beijing's strategic communication has made the digital sphere one of its pillars, ensuring that the Chinese media apparatus is extended through the numerous accounts that each media outlet has on X, Facebook, YouTube and Instagram abroad. Meanwhile, the Great Digital Wall of China continues to block these platforms (Cook, 2020).

[6] One way in which control is exercised is through the workings of China's institutions. See the long-form piece by Ling explaining how the Party Congress works (2022a, 2022b, 2022c).

[7] For example: Lin, L. [@lizalinwsj]. (6 December 2022). 1/In China, most apps have changed their home page to black and white since Nov 30, the day of Jiang Zemin's death. The only thing remaining in color? Photos of Xi Jinping and the Politburo: https://pbs.twimg.com/media/FjR2wU3acAA1_cu?format=png&name=900x900 [Image attached] [Thread]. X. https://x.com/lizalinwsj/status/1600034448170713088

In recent years, Beijing has made a major shift in its strategic communication and does not hesitate to adopt an aggressive tone[8,9], in the disinformation campaigns orchestrated (Graham, 2022) against its perceived enemies (Cook, 2020). Taiwan (in 2018) and Hong Kong (in 2019)[10] were the targets of China's first disinformation campaigns, but the change in model did not occur until the Covid-19 pandemic (The Associated Press, 2020). China began making regular use of disinformation (Milosevich-Juaristi, 2020) at that juncture, as the CPC was forced to change tack following the damage to its image caused by its management of the health crisis. At that time, it did not avail itself of the traditional strategy of denying access to information[11]; rather it adopted a more aggressive tone (Chan and Thornton, 2022) and, in the Russian style, made use of "official channels to propagate conspiracy theories, subsequently disseminating them in media that depend on State funding and on social media" (Milosevich-Juaristi, 2020) (T0073, T0002).

Financing mechanisms used by China as an autocratic actor in the era of disinformation

China Media Group (CMG) is the main CPC news outlet that broadcasts both video and radio content. Created in 2018, CMG comprises China Central Television (CCTV), China Global Television Network (CGTN), China National Radio (CNR) and China Radio International (CRI). In 2022, CMG received a budget of 2.32 billion RMB (344 million USD), with 96% earmarked for "culture, tourism, sport and media". CMG has financed associations with foreign media and journalists to expand its reach and promote narratives that are favourable to Chinese interests (DFRLab, 2023). Beijing has also worked to co-opt prominent voices in the international information environment (Global Engagement Center [GEC], 2020b), including those of members of foreign political elites and journalists (T0010/T0093).

[8] For example: Air-Moving Device [@AirMovingDevice]. (28 November 2022). Thread: Search for Beijing/Shanghai/other cities in Chinese on Twitter and you'll mostly see ads for escorts/porn/gambling, drowning out legitimate search results. Data analysis in this thread suggests that there has been a *significant* uptick in these spam tweets. https://pbs.twimg.com/media/FinEPCBXEAAc7sZ?format=png&name=large [Image attached] [Thread]. https://twitter.com/AirMovingDevice/status/1597034969293271040

[9] Menn (2022) describes how China was concealing news about protests.

[10] Local elections were held in Taiwan on 24 November 2018. The Democratic Progressive Party (DPP), which governed the island, was defeated by the pro-Chinese party Kuomintang (KMT). During the campaign, local media lent credibility to fake news stories originating in China that attacked the DPP, paying for the creation, also in China, of Facebook networks supporting Han, a KMT candidate. It was later brought to light that the number of fake news items about Han's opponent was increased by contributions from five Chinese provinces and evidence was even uncovered that agents of the Chinese government had intended to purchase pro-Taiwan Facebook pages before the general elections in 2020. Moreover, in 2019, Twitter deleted more than 900 accounts that were used to undermine the credibility of pro-democracy demonstrators in Hong Kong. Facebook and YouTube later took similar actions. The network attacking leaders of the opposition to the CPC, such as Yang Jianli, Guo Wengui, Gui Minhai and Yu Wensheng, had been active since 2017 (Cook, 2020, pp. 10-11).

[11] This was the case at the beginning of the Covid-19 pandemic at least, but there was a change in strategy at the end of 2022. (Europa Press, 2022).

On certain occasions, China has also created fake profiles (T0009), such as that of a Swiss scientist called Wilson Edwards, who criticized the United States over its handling of the Covid-19 pandemic (Davidson, 2021).

Beijing seeks to maximize the reach of biased or fake content presenting the CPC in a positive light and has acquired stock in foreign media through public and non-public media and has sponsored influential people online (T0100). This could form part of its Thousand Talents Plan, a strategy by which the country seeks to recruit Western scientists and researchers (Keown, 2018). China is recruiting Western specialists through social media in the West, especially through the social network LinkedIn (Burgess, 2023). The CPC in Spain is seeking to create and/or raise funds for organizations and think tanks by holding events (T0126/T0057).

IRAN

Investigation methodology used to study Iran's use of disinformation

The methodological approach followed focused on analysing digital narratives aligned with Iran's geopolitical and strategic interests. The investigation encompassed multiple platforms, including Telegram and other digital channels, and sought to identify patterns of communication, State propaganda and diverse manipulation tactics. The aim was to understand how Iran pushes its ideological agenda, mobilizes support, and discredits its adversaries in the global information environment.

As a starting point, the main digital media through which narratives aligned with Iranian interests could be disseminated were identified. We found that Iran's propaganda ecosystem combines multiple layers of traditional and digital media and various languages to maximize its reach. The narrative fostered is amplified and distributed through a set of media outlets and channels that include:

- **State media** such as HispanTV, Press TV and Al-Alam. Our analysis centred primarily on HispanTV, due to its focus on Spanish-speaking audiences. (Press TV and Al-Alam are aimed at Arabic-speaking audiences).

- **Messaging apps and social media** such as Telegram, X, Facebook and YouTube, used to mobilize content and campaigns.

- **Allied media** such as Al-Mayadeen and TeleSUR, which share the same anti-Western agenda and amplify Iranian narratives.

- **Other media** linked to cybercrime groups, which strengthen Iran's strategic messages through cyberespionage campaigns and hacktivism.

The second stage of our investigation was focused on gathering information from digital media previously tagged for monitoring and analysis. The content compiled encompassed different formats, such as news articles, videos, infographics, memes, political or ideological analyses, official narratives and original or republished multimedia content.

Our analysis of Iranian narratives focused on the following:

- **Predominant narratives:** We identified recurrent themes and their respective narrative framing, aligned with Iran's interests, including**:**
    - **Support for Palestinian resistance**, and promotion of the idea that Iran is a key ally in the fight against Israeli occupation.
    - **Delegitimization of Western sanctions**, and presentation of these sanctions as "war crimes" primarily affecting Iran's civilian population.
    - **US hegemony**, with references to the "fall of imperialism" and promotion of a new multipolar world order in alliance with powers such as Russia and China.
- **Ideological and geopolitical alignment**: We determined whether content reflected pro-Iran, pro-Russia, anti-NATO or anti-US positions, or positions in favour of other international actors, such as China and Venezuela..

Lastly, we concluded our investigation by identifying the TTPs used in media promoting pro-Iran narratives, following the DISARM framework.

Disinformation campaigns and propaganda

The narrative disseminated by various digital media reflects a tight network of partnerships between Iran and its main allies, such as Russia, Syria, Palestine, Lebanon and Venezuela, which use these platforms as soft-power tools to push anti-Western messages. Iran has positioned itself as a leader of the resistance against the United States, Israel and Saudi Arabia, fostering condemnation of foreign intervention among its allies and defending a multipolar world.

HispanTV, an Iranian State channel, amplifies Iran's official narrative by praising figures such as Ayatollah Ali Khamenei and Bashar al-Assad and besmirching Iran's adversaries, presenting Western sanctions as unjust acts of aggression. In parallel, the Venezuelan media outlet TeleSUR underpins this narrative by running smear campaigns against political opponents and celebrating Venezuela's partnerships with Cuba and Iran, using video and news content to divide and weaken pro-Western governments in Latin America.

From another front, the Russian State media outlet Sputnik complements these narratives by directly criticizing the United States and NATO, particularly in relation to conflicts such as that involving Russia and Ukraine, with the platform accusing Western forces of being aggressors. Although Sputnik is not directly pro-Iran, it operates under a vision aligned with Iranian interests, promoting an alternative world order in which the emerging powers represent a challenge to Western hegemony. In addition, more niche channels, such as Axis of Resistance and the Spanish-language channel Mundo Multipolar ZOV on Telegram, intensify this message by highlighting the role of global resistance, placing particular emphasis on the ties between Iran, Russia and Palestine.

For its part, the media outlet Al Mayadeen, based in Lebanon, supports the Palestinian cause and armed resistance against Israel, aligning itself with the interests of Iran and Syria and with groups such as Hezbollah, while denouncing US hegemony in the region. In addition, Telegram channels such as Libertad Palestina and Palestina Hoy use images and conspiracy theories to fuel resistance against Israel. In a similar vein, Syrian media such as the Syrian Arab News Agency (SANA) seek to legitimize Bashar al-Assad's regime, presenting him as a defender of sovereignty against terrorism and foreign interference. Lastly, European movements such as the yellow vests movement are pointed to as signs of the collapse of the Western model, underscoring the narrative that a new world order, led by Iran and Russia, is emerging to challenge the current power structure.

Our analysis of the narratives considered, together with the map designed based on the DISARM framework, revealed the use of a number of techniques suggestive of disinformation. One preferred technique is that of facilitating State propaganda (T0002), which is used to amplify official narratives and exclude critical voices. This strategy strengthens the legitimacy of the leaders of allied countries and promotes resistance against the West. Another technique used is that of degrading adversaries (T0066), which entails discrediting actors such as the United States and Israel, presenting their actions as illegitimate aggressions, while at the same time praising allies.

Another key technique is that of harassing opponents (T0048) with the aim of discrediting opposition leaders and delegitimizing the movements headed by them. The technique of responding to breaking news events (T0068) entails aligned actors reacting quickly to crises, shaping narratives to strengthen their agenda. Meanwhile, cross-posting (T0119) maximizes the reach of the message across multiple platforms, as observed in the simultaneous dissemination of pro-Russian and anti-Western content.

Leveraging conspiracy theory narratives (T0022) is another popular option as it introduces narratives accusing Western powers of conspiring to control global politics. This technique is complemented by that of dismay (T0078), where shocking images of civilian victims, particularly in the Palestine-Israeli conflict, are posted to provoke anger towards Israel and its allies. These patterns of information manipulation seek to consolidate the resistance of Iran's allies and weaken the legitimacy of its adversaries.

Additionally, techniques such as creating localized content (T0101) and determining target audiences (T0073) enable messages to be adapted to specific audiences, thereby optimizing their impact. This includes the creation of hashtags and search artefacts (T0015) to make content go viral, used in campaigns supporting the Palestinian cause or criticizing Western interventions in Latin America. These strategies allow aligned actors to disseminate information more widely, strengthening narratives and destabilizing opponents.

Iran has been seeking to exert its influence through diverse means, including by inviting foreign influencers to visit the country, purportedly to promote tourism (News, 2024); by financing the editors of specific websites, such as The Grayzone, through a communication agency owned by the Iranian government (Menn, 2024), to conceal the circulation of propaganda and disinformation; and by nurturing friendly relations with and utilizing journalists, making it easy for them to visit Iran with the approval and coordination of official Iranian bodies, with said visits ultimately serving as pro-regime propaganda campaigns that may include attempts to discredit the West and its media structure (News, 2023). An in-depth analysis would be required to identify and trace the increasingly complex foreign influence and interference operations involving the acquisition or recruitment of non-domestic networks (T0093) or the cultivation of ignorant agents (T0010).

Identifying, through open sources, sufficient elements pointing to the financing sources or hypothetical economic motivations for the procedures used by Iran to monetize strategies based on the aforementioned TTPs would require more complex and lengthier analysis. Our suggestion is for such analysis to be conducted by future working groups of the Forum against Disinformation Campaigns Affecting National Security.

Cyber groups linked to Iran

In the current global context, disinformation campaigns and cyberattacks have emerged as powerful weapons used by State actors and hacktivist groups to influence public perception and destabilize adversaries. Iran, in particular, has been identified as one of the main actors in this sphere, using APT (Advanced Persistent Threat) groups and hacktivists aligned with its ideology to carry out espionage, sabotage and propaganda operations. These efforts are designed not only to protect the interests of the Iranian regime, but also to exert influence at the international level, attacking regional and global rivals, especially the United States, Israel and Saudi Arabia.

As regards APT groups, two in particular are believed to receive Iranian backing and to be linked to the Islamic Revolutionary Guard Corps (IRGC). The first of these two groups, APT42 is an Iranian group that is particularly prominent in espionage and disinformation activities. Its main objective is to carry out campaigns against high-ranking officials from Israel and the United States, including government, political and diplomatic figures, as well as direct critics of Iran, such as activists, journalists and certain think tanks.

APT42 has engaged in a number of recent activities, such as masquerading as a US think tank and using malware against US targets following the October 2023 attacks in Israel. It has also carried out phishing campaigns aimed at media and non-profit organizations in the United States and the Middle East, in addition to targeting individuals linked to the US presidential election during the first half of 2024. These actions demonstrate the sophistication of the group and its capacity to carry out cyberattacks in a complex geopolitical context, using techniques such as determining target audiences (T0073) and creating fake experts (T0009), infiltrating networks and gaining the trust of their victims.

The second of the two aforementioned APT groups, APT33, also known as Elfin, specializes in cyberattacks targeting critical infrastructure, and particularly that of the energy sectors of adversary countries, such as Saudi Arabia. This group promotes a pro-Iran narrative, aligning itself with the regime’s interests against the United States, Israel and Saudi Arabia. APT33 was linked to the distribution of backdoor malware at the end of 2023, in an operation in which the actors passed themselves off as a US company from the space and satellite industry. The techniques used by this group include determining strategic ends (T0074), which enables them to attack high-value targets in critical sectors, and degrading adversaries (T0066) by sabotaging key infrastructure and manipulating sensitive information.

These groups not only engage in espionage and sabotage, but also create narratives favourable to the Iranian regime. Through the combination of cyberespionage and disinformation campaigns, both APT42 and APT33 target strategic sectors in the United States and other Western nations.

APT group activities are complemented by those of hacktivist groups aligned with pro-Iran narratives, such as Cyber Av3ngers (allegedly aligned with IRGC), Al-Toufan Team, ALtahrea Team, Makhlab al-Nasr and Cyber Toufan. These groups seek to weaken their adversaries through cyberattacks, using techniques such as that of degrading adversaries (T0066) by publishing leaks from sensitive documents and exposing vulnerabilities in critical infrastructure. Other techniques used include determining target audiences (T0073)—in this case, pro-Palestinian and pro-Iranian audiences—and flooding the information space (T0049), saturating social media with visual and textual propaganda celebrating their cyberattacks.

A common denominator among these groups is the use of platforms such as X and Telegram to expand their activities and, in some cases, to coordinate them. Groups such as Handala Hack conceal their operating activity (T0129), protecting their identity by using encrypted channels, while others, such as Cyber Court, choose to post content (T0115) about their attacks on a continual basis. Hacktivist groups tend to control the information environment through offensive cyberspace operations (T0123), carrying out attacks that distort their adversaries' information ecosystems. Examples of this include manipulation of stolen documents and exaggeration of the impacts of their attacks on critical Israeli infrastructure, as in the case of the Cyber Flood group.

In total, these groups' actions reflect the scope and complexity of Iran's cybernetic operations, which not only seek to weaken or destroy the infrastructure of its enemies, but also to influence the global narrative. Iran conceals its operational activity (T0129) and plays the long game (T0059), enabling it to exert influence in cyberspace while protecting its geopolitical interests.

VENEZUELA

Venezuela, which was once one of the most consolidated democracies in the whole of Latin America, has experienced a significant deterioration in its democratic institutions under the regime of Hugo Chávez and his successor, Nicolás Maduro. This decline has been accompanied by a rise in digital repression and censorship.

In Venezuela, more than 268 radio stations went off the air between December 2021 and November 2023. This occurred in both rural and urban areas, leaving many regions without access to local news. Television stations have also faced censorship, with the National Commission of Telecommunications (CONATEL) banning certain topics and words from the air. This has led to the disappearance of opinion and interview segments from many channels. Twelve of Venezuela's 23 states do not have local print newspapers. Many newspapers have been closed down due to censorship and economic pressure, including El Nacional, El Universal and Últimas Noticias. More than 52 news websites have been blocked, including Armando.info, Efecto Cocuyo, El Pitazo, La Patilla, Maduradas, Noticiero Digital, NTN24, Vivo Play and VPITV. International media such as Infobae and NTN24 have also been blocked in Venezuela. Various social media platforms, such as X, have also been blocked (Mitchell, 2024).

The government of Nicolás Maduro has made strategic use of social media (T0074) to carry out disinformation campaigns and manipulate public opinion. The group known as Tuiteros de la Patria coordinates its publications to amplify government messages, receiving monetary compensation for achieving publication goals, and using hashtags and language provided by the Ministry of Communication and Information (T0002, T0093). In addition, coordinated social media campaigns during the opposition's presidential primaries (Cocuyo chequea, 2023) (T0015) in 2023 sought to discredit candidates and promote pro-government narratives, using hashtags such as #MariaCorinaEsLeopoldo and #LosLujosDeLeopoldo. Networks of fake profiles and trolls amplifying pro-government messages and harassing the regime's opponents (T0048) were also identified and the Venezuelan government used trends on X to promote its messages and conceal unfavourable information through the coordinated mass publication of tweets with specific hashtags (T0068). Official accounts and troll networks have attacked independent media and journalists publishing information critical of the government, and defamation campaigns and publication of false information have been used to discredit journalists. Moreover, Maduro's government has collaborated with other authoritarian regimes, such as Russia and China, to disseminate narratives favourable to their interests and attack their critics, amplifying messages on State media and social media controlled by said countries[12].

During the most recent elections in Venezuela, the government-controlled National Electoral Council (CNE) proclaimed Maduro the winner without providing a detailed breakdown of the ballot, which led to accusations of fraud by the opposition and questions from the international community. The foreign electoral observers primarily comprised allies of the regime (Pérez Gallardo, 2024) and the Statement issued on 4 August 2024 by the High Representative of the European Union—on behalf of the EU—on post-election developments in Venezuela expresses great concern over recent electoral events in the country, referring to reports from international election observation missions that the presidential elections did not meet international standards of electoral integrity. The High Representative's Statement also mentions the fact that the National Electoral Council of Venezuela (CNE) had yet to publish the official voting records ("actas") of polling stations (Council of the European Union, 2024). The EU, together with 21 other countries, have called for the impartial verification of Venezuela's electoral results (Ministry of Foreign Affairs, European Union and Cooperation, 2024).

ECONOMIC IMPACT OF THE ACTIVITIES ANALYSED

We must distinguish between the economic impacts for the threat actor of deploying their disinformation strategies—considering costs, benefits and efficiency, the increase in influence and reach, as well as their perception of narrative control—and the socio-political impact on society as a whole, including on financial markets.

Owing to technological facilities, manipulation on online platforms, and especially social media, allows the creation of coordinated inauthentic behaviour (CIB) networks, which use a mix of authentic, fake, and duplicated social media accounts and whose success or failure depends on the capacity of said platforms to detect and eliminate them. Despite legislation such as the Digital Services Act, platforms show significant and unequal limitations as regards detecting and removing fake accounts and inauthentic engagement (Bergmanis-Korāts and Haiduchyk, 2024).

Our research identified a rise in the use of fake commercial profiles—usually focused on such topics as cryptocurrency and gaming—to amplify political content, especially during election periods. This represents additional risks of manipulation in democratic processes. One strategy for avoiding detecting is that of dividing mass campaigns into smaller-scale operations to hinder identification by platform classification systems (Bergmanis-Korāts and Haiduchyk, 2024).

[12] Such as, for example: USA en Español [@USAenEspanol] (12 March 2019), Russia uses its State-sponsored disinformation bodies such as Russia Today and Sputnik to divert attention from the humanitarian disaster of Maduro's regime. Russia has spent a large amount of money in Venezuela. More than $17 billion in investments and loans. https://x.com/i/status/1105425709986664448 [video attached] [post] https://x.com/USAenEspanol/status/1105425709986664448

Social media manipulation services are increasingly accessible, and their cost has fallen, making it economically viable for different threat actors to purchase large volumes of fake interactions[13] and amplify their disinformation campaigns. These services include packages of thousands of views or likes at affordable prices, enabling the monetization of these interactions through the promotion of content (Bergmanis-Korāts and Haiduchyk, 2024).

As stated at the outset, the impacts of disinformation campaigns extend beyond the social and political spheres; they also affect the economy.

Indeed, the orchestrated dissemination of fake narratives, rumours and conspiracy theories usually generates uncertainty and volatility in the markets, with consequent impacts on corporate and investment decision-making.

Disinformation campaigns would not have any impact on the economy if it were not because, having successfully reached their target audience (victims), and caused them to doubt other sources of information, they cause harm to the reputation of the organization, institution or system attacked, damaging their name and credibility among clients, users and/or the public as a whole, which finally results in the impact on the economy sought by the attacker.

Indeed, as previously stated, disinformation exacerbates the media business model crisis, as the rapid dissemination of fake content can reduce trust in traditional media, with a negative effect on advertising revenue. This situation is heightened by the dependence of the press on traditional financing models and the growing difficulty of capturing audience attention in a saturated market.

The acceleration of news cycles and the rise of the attention economy, which rewards content that generates rapid, mass reactions, favours the dissemination of fake and polarizing news. This penalizes producers of quality content and threatens the sustainability of media, whose work is difficult and expensive to automate without sacrificing quality (IBERIFIER, 2023). In the United States alone, the main disinformation websites generate more than 235 million US dollars in annual advertising revenue (Global Disinformation Index, 2022).

As previously asserted, manipulated information has an influence on public perception and can alter the economic environment, affecting investment decisions and consumer spending, especially during election periods or times of political crisis (Fake News and its Impact on the Economy, 2020). In addition, incessant flows of false information may lead to the adoption of regulations restricting corporate freedom, requiring organizations to invest in new, additional strategies on communication and crisis management (Christov, 2019).

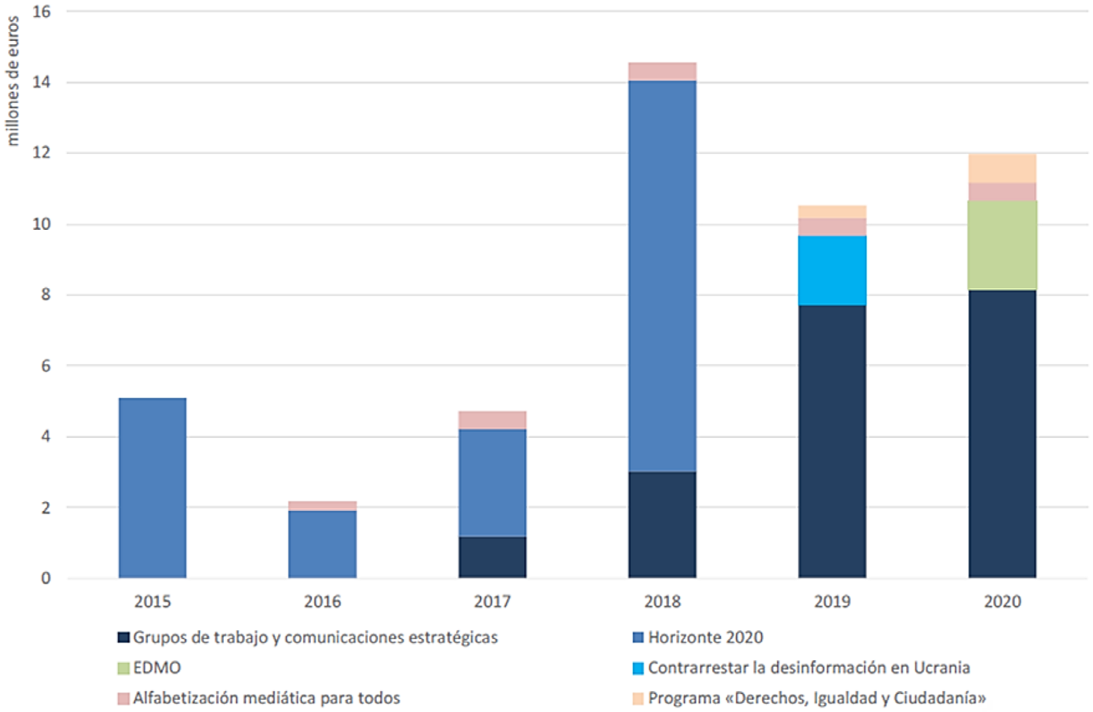
[13] The speed of the manipulation hinders its detection and appropriate blocking by platforms. In 2024, 93% of the fake interactions recorded by the study took place within the first 24 hours (100% on YouTube and TikTok, within the first 12 hours, and 64% on X, within the first 24 hours). The speed of the manipulation affects platforms' effectiveness at addressing the manipulative behaviour quickly enough to mitigate its impact.

ECONOMIC IMPACT OF DISINFORMATION CAMPAIGNS	
Financial market volatility	Disinformation campaigns can destabilize fi-nancial markets. For example, dissemination of false information on the financial health of a company can lead to massive sales of stock, resulting in a sharp decline in their value. Market fluctuations affect not only the compa-nies directly involved, but investors and other market actors too, generating a climate of un-certainty and distrust that can extend to the entire financial system. In the long term, this volatility can discourage foreign investment and reduce economic growth.
Impact on consumer or citi-zen trust	The dissemination of fake news can erode consumer trust in brands and companies, which can lead to a decrease in consumer spending and sales. This may have a negative effect on the economy, especially in sectors such as retail trade and services. For example, during the Covid-19 pandemic, the dissemina-tion of false information about staple food products caused panic and unnecessary scar-city. The impacts are similar when the victims are individuals belonging to a group, region, State or political community. The erosion of trust caused by disinformation campaigns can clearly demotivate citizens from continuing to participate actively in the system, by ceasing to pay taxes, for example.
Mitigation costs	Governments and companies must invest significant resources in detecting and countering disinformation, with such efforts including implementation of advanced technological tools, staff training and campaigns to raise public awareness (Heikkinen, 2021).

ECONOMIC IMPACT OF DISINFORMATION CAMPAIGNS	
Loss of competitiveness	Disinformation can also harm the reputation of companies and countries, affecting their competitiveness on the global market. For example, a country that is seen as an easy target for disinformation campaigns can be perceived as unstable, discouraging foreign investment and tourism. A company that has been the victim of disinformation can suffer long-term harm to its reputation, even after the false information has been debunked. Loss of trust can lead to a fall in sales and in the capacity to attract new clients, negatively affecting the company's market position.
Impact on economic policy	Disinformation can influence political deci-sion-making, leading to the adoption of un-suitable or ill-informed economic policies. For example, during the Brexit campaign, a great deal of misleading information was dissemi-nated about the benefits and economic con-sequences of leaving the European Union, which affected the vote and subsequent politi-cal decision-making (Brändle et al., 2021). Policies based on disinformation can have long-term impacts that are detrimental to eco-nomic growth and financial stability. In addi-tion, the political polarization resulting from disinformation may hinder implementation of necessary economic policies and cooperation between different political actors.

In short, disinformation campaigns represent a significant threat to the economic and financial stability of the countries attacked.

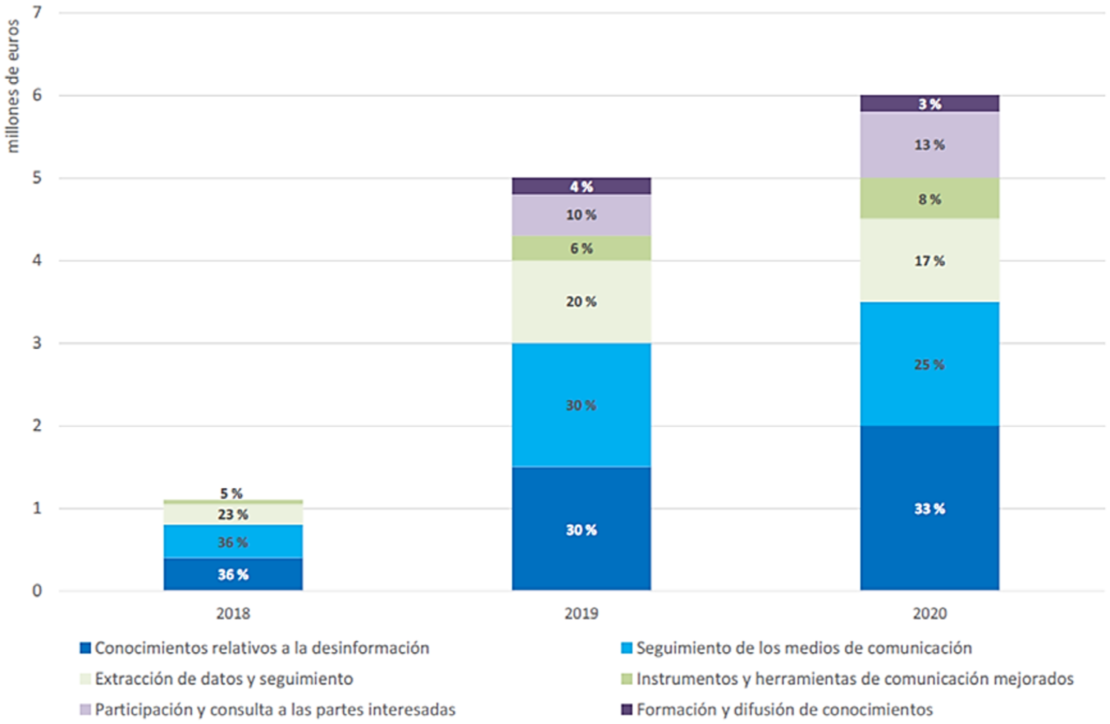
The Special Report of the European Court of Auditors (2021) contains some especially significant data on the economic efforts the European Union has been making to counter disinformation campaigns.



Total financing allocated by the EU to combat disinformation in the 2015-2020 period. (Source: European Court of Auditors, based on information provided by the Commission and EEAS)

EEAS has been especially active in the fight against disinformation, assigning budgetary items to the different Task Forces created in the StratCom[14]. The figure below shows the distribution of these funds during the specified period.

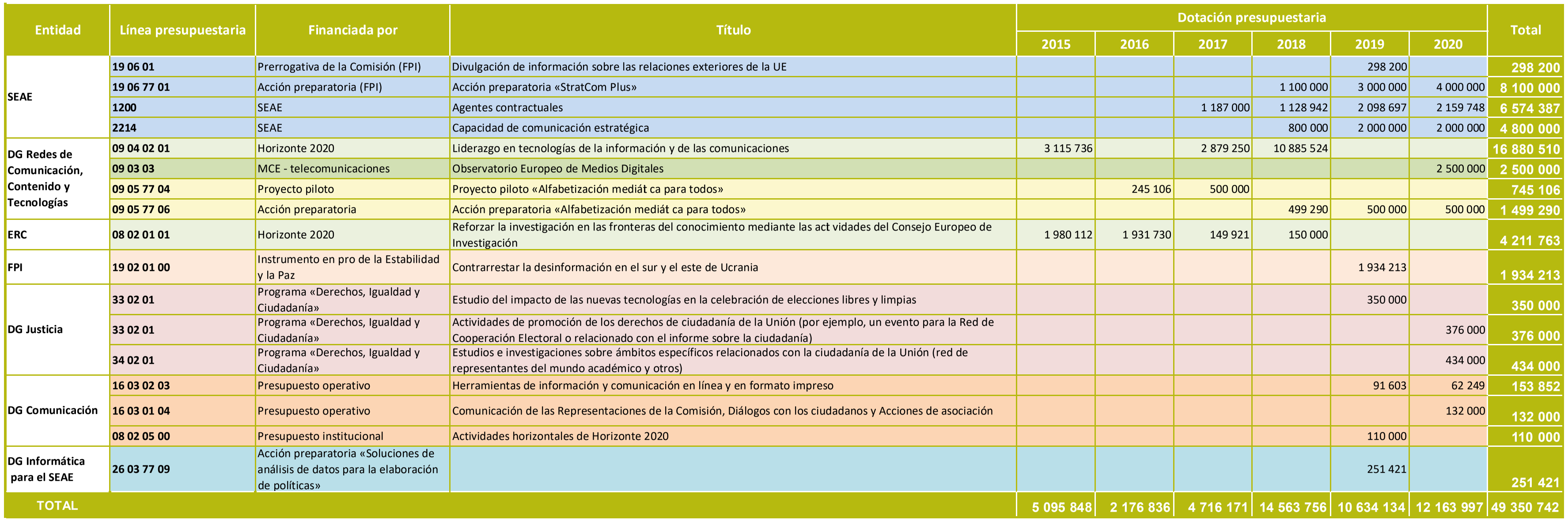
[14] https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en



Funding provided by the Preparatory Action: 'StratCom Plus' for different capabilities of the EEAS StratCom Task Forces (2018-2020). (Source: European Court of Auditors, based on EEAS data.)

Although still clearly insufficient, the EU has in recent years been assigning budget items to combat the risks deriving from disinformation campaigns.

The following table shows the investment made by the EU in actions to combat disinformation during 2015-2020.



Entidad	Línea presupuestaria	Financiada por	Título	Dotación presupuestaria						Total
				2015	2016	2017	2018	2019	2020	
SEAE	19 06 01	Prerrogativa de la Comisión (FPI)	Divulgación de información sobre las relaciones exteriores de la UE					298 200		298 200
	19 06 77 01	Acción preparatoria (FPI)	Acción preparatoria «StratCom Plus»				1 100 000	3 000 000	4 000 000	8 100 000
	1200	SEAE	Agentes contractuales			1 187 000	1 128 942	2 098 697	2 159 748	6 574 387
	2214	SEAE	Capacidad de comunicación estratégica				800 000	2 000 000	2 000 000	4 800 000
DG Redes de Comunicación, Contenido y Tecnologías	09 04 02 01	Horizonte 2020	Liderazgo en tecnologías de la información y de las comunicaciones	3 115 736		2 879 250	10 885 524			16 880 510
	09 03 03	MCE - telecomunicaciones	Observatorio Europeo de Medios Digitales						2 500 000	2 500 000
	09 05 77 04	Proyecto piloto	Proyecto piloto «Alfabetización mediática para todos»		245 106	500 000				745 106
	09 05 77 06	Acción preparatoria	Acción preparatoria «Alfabetización mediática para todos»				499 290	500 000	500 000	1 499 290
ERC	08 02 01 01	Horizonte 2020	Reforzar la investigación en las fronteras del conocimiento mediante las actividades del Consejo Europeo de Investigación	1 980 112	1 931 730	149 921	150 000			4 211 763
FPI	19 02 01 00	Instrumento en pro de la Estabilidad y la Paz	Contrarrestar la desinformación en el sur y el este de Ucrania					1 934 213		1 934 213
DG Justicia	33 02 01	Programa «Derechos, Igualdad y Ciudadanía»	Estudio del impacto de las nuevas tecnologías en la celebración de elecciones libres y limpias					350 000		350 000
	33 02 01	Programa «Derechos, Igualdad y Ciudadanía»	Actividades de promoción de los derechos de ciudadanía de la Unión (por ejemplo, un evento para la Red de Cooperación Electoral o relacionado con el informe sobre la ciudadanía)						376 000	376 000
	34 02 01	Programa «Derechos, Igualdad y Ciudadanía»	Estudios e investigaciones sobre ámbitos específicos relacionados con la ciudadanía de la Unión (red de representantes del mundo académico y otros)						434 000	434 000
DG Comunicación	16 03 02 03	Presupuesto operativo	Herramientas de información y comunicación en línea y en formato impreso					91 603	62 249	153 852
	16 03 01 04	Presupuesto operativo	Comunicación de las Representaciones de la Comisión, Diálogos con los ciudadanos y Acciones de asociación						132 000	132 000
	08 02 05 00	Presupuesto institucional	Actividades horizontales de Horizonte 2020					110 000		110 000
DG Informática para el SEAE	26 03 77 09	Acción preparatoria «Soluciones de análisis de datos para la elaboración de políticas»						251 421		251 421
TOTAL				5 095 848	2 176 836	4 716 171	14 563 756	10 634 134	12 163 997	49 350 742

EU spending on actions to combat disinformation (in euros).(Source: European Court of Auditors, EEAS).

Finally, the table below shows the assessment of projects against disinformation (Pilot Projects, Preparatory Actions, Horizon 2020).

Número de proyecto	Tipo de proyecto	Países	Duración del proyecto (real)	Estado	Vínculo directo con otros proyectos	Importe de la subvención (en euros)	¿Resultó adecuado el seguimiento de la Comisión?	Criterio 1 Pertinencia relat va a la desinformación	Criterio 2 Resultados tangibles y sostenibles	Criterio 3 Escala y alcance suficientes
1	Horizonte 2020	Reino Unido (objetivos: Alemania, Francia, Polonia, Suecia, Reino Unido / Brasil, Canadá, China, México, Rusia, Ucrania, Estados Unidos, Taiwán)	Enero de 2016 - diciembre de 2020	En curso	Sí	1 980 112	Existe una presentación de informes continua e independiente en forma de auditoría y un informe científico.	🟩	🟩	El proyecto produjo, principalmente, documentos de investigación. La mayoría de las presentaciones de estos documentos se han producido fuera de la UE. Tras la salida del Reino Unido de la UE, se desconoce de qué modo podrá esta investigación seguir beneficiando a la Unión.
2	Horizonte 2020	Reino Unido	Julio de 2017 - enero de 2019	Finalizado	Sí	149 921	Existe una presentación de informes continua e independiente en forma de auditoría.	🟩	🟩	No existe ningún tipo de indicio de que el proyecto vaya a ir más allá de una prueba de concepto y, si así sucede, se desconoce si el público se beneficiará tanto como el sector privado en el caso de que el producto final acabe comercializándose.
3	Horizonte 2020	Grecia	Enero de 2016 - diciembre de 2018	Finalizado	Sí	3 115 737	Existe un dictamen experto e independiente e informes de evaluación.	🟩	🟩	La herramienta producida por el proyecto estaba enfocada, principalmente, a los expertos y no resultó lo suficientemente intuitiva para el público general (se requirieron dos proyectos posteriores para precisar los resultados y para mejorar la escala y el alcance del proyecto).
4	Horizonte 2020	Italia	Enero de 2018 - diciembre de 2020	En curso	No	2 879 250	El proyecto sigue en curso en la actualidad. Existe una presentación de informes continua acompañada de una primera evaluación.	🟩	Se ha observado un punto débil, ya que uno de los componentes del soporte lógico está obsoleto, por lo que el proyecto no está empleando métodos de última generación en este ámbito.	🟩
5	Horizonte 2020	Irlanda, Grecia, Italia, Chipre, Austria, Portugal, Rumanía, Reino Unido	Enero de 2018 - noviembre de 2021	En curso	Sí	2 454 800	Se realizó una revisión independiente a distancia en julio de 2020, facilitada por la DG Redes de Comunicación, Contenido y Tecnologías.	🟩	Un proyecto bien gestionado que precisa de algunas medidas correctoras para situar el foco en determinados componentes clave, y una elaboración más detallada de su difusión y explotación.	Puntos débiles en la ejecución de la difusión y en las estrategias de explotación empresarial.
6	Horizonte 2020	Chequia, Irlanda, España, Austria	Diciembre de 2018 - noviembre de 2021	En curso	Sí	2 753 059	Se están llevando a cabo revisiones independientes a distancia (fecha de inicio: agosto de 2020).	🟩	🟩	Existe incertidumbre acerca de cómo interactuarán las plataformas en línea centralizadas con la herramienta.
7	Horizonte 2020	Francia, Italia, Polonia, Rumanía, Reino Unido	Diciembre de 2018 - noviembre de 2021	En curso	Sí	2 505 027	Se realizaron tres evaluaciones individuales en diciembre de 2019 y una evaluación general en febrero de 2020. Además, entre enero y abril de 2020, se llevó a cabo una revisión del proyecto.	🟩	🟩	🟩
8	Horizonte 2020	Dinamarca, Grecia, Italia	Noviembre de 2018 - abril de 2021	En curso	Sí	987 438	El proyecto fue revisado por tres controladores independientes y evaluado por el jefe de proyecto.	🟩	El proyecto sigue en curso en paralelo a un proyecto similar en ese ámbito.	🟩
9	Horizonte 2020	Bélgica, Bulgaria (C), Alemania, Grecia, Francia, Reino Unido	Diciembre de 2018 - noviembre de 2021	En curso	Sí	2 499 450	Ausencia de contribución y de esfuerzos coordinados por parte de la Comisión al inicio del proyecto.	🟩	Se están comprobando los resultados en la fase de prototipo. Esto puede conllevar determinados riesgos. Ausencia de directrices por parte de la Comisión; además, las ideas sobre cómo pueden ser sostenibles los resultados se limitan a iniciativas asociadas vinculadas a sus propios contactos, socios o clientes.	🟩
10	Horizonte 2020	Suiza/Reino Unido	Septiembre de 2018 - noviembre de 2019 (en un principio, febrero de 2020)	Finalizado	Sí	150 000	A petición del Tribunal, el jefe de proyecto se preocupó de recopilar la información necesaria para establecer cómo se aprovecharon los resultados.	🟩	🟩	Los resultados fueron explotados, principalmente, por una empresa estadounidense.
11	Proyecto piloto	Bélgica, Rumanía, Francia, Croacia, Polonia, Finlandia, Estados Unidos	Enero de 2018 - enero de 2019	Finalizado	No	125 000	El seguimiento del proyecto se llevó a cabo mediante diversos indicadores cualitativos y cuantitativos.	🟩	🟩	🟩
12	Proyecto piloto	España, Italia, Malta, Portugal, Reino Unido	2016	Finalizado	Sí	171 057	El seguimiento por parte de la Comisión no fue evidente.	🟩	Tan solo se desarrollaron cursos de formación sostenibles en uno de los cinco países.	Los resultados del proyecto tuvieron un alcance limitado.
13	Proyecto piloto	Bélgica, Grecia, España, Italia, Letonia, Lituania, Hungría, Malta, Austria, Polonia, Portugal, Rumanía, Eslovaquia	2017	Finalizado	No	118 445	Presentación de informes continua y producción de un informe técnico y de una evaluación final independiente.	🟩	🟩	Problemas de sostenibilidad. En su autoevaluación final, el proyecto destacó la ausencia de una estrategia de alfabetización mediática general.

Número de proyecto	Tipo de proyecto	Países	Duración del proyecto (real)	Estado	Vínculo directo con otros proyectos	Importe de la subvención (en euros)	¿Resultó adecuado el seguimiento de la Comisión?	Criterio 1 Pertinencia relat va a la desinformación	Criterio 2 Resultados tangibles y sostenibles	Criterio 3 Escala y alcance suficientes
14	Proyecto piloto	Polonia	Julio de 2018 – junio de 2019	Finalizado	No	127 590	🟥 **Tan solo existe una evaluación de una página que no analiza los resultados.**	🟨 **El proyecto mezcla la verificación de datos con los derechos de las mujeres y el sexismo, por lo que su pertinencia en lo que respecta a la desinformación es escasa.**	🟨 **La página web creada por el proyecto ya no está operativa.**	🟩
15	Proyecto piloto	Bélgica, Austria, Portugal	2017	Finalizado	No	122 815	▨	🟩	🟥 **Se llevó a cabo una tormenta de ideas y se elaboraron libros blancos, pero no existen herramientas específicas.**	▨ **El proyecto se suspendió debido a la insolvencia del coordinador.**
16	Proyecto piloto	Dinamarca, Irlanda, Grecia, Chipre, Portugal	Julio de 2018 – junio de 2019	Finalizado	No	131 150	🟥 **No existe ningún indicio de que se esté llevando a cabo un seguimiento continuo. La evaluación final es de 133 palabras y no contiene ninguna recomendación.**	🟨 **El proyecto se centra en el pensamiento creativo en general.**	🟥 **Los productos o resultados no son cuantificables.**	🟨 **El proyecto fue un ejercicio aislado y no puede reproducirse o prolongarse con facilidad**
17	Acción preparatoria	Bélgica, Bulgaria, Alemania, España, Croacia, Rumanía, Italia, Letonia	Julio de 2019 - agosto de 2020 (prórroga sometida a debate)	En curso	No	124 546,72	🟩 **Se produjo un informe de ejecución técnica provisional.**	🟩	🟩	🟩
18	Acción preparatoria	Dinamarca, Alemania, España, Francia, Italia, Países Bajos, Polonia, Finlandia	2018	En curso	Sí	214 556	🟩 **El proyecto realizó un seguimiento estrecho de las acciones con indicadores claramente definidos.**	🟩	🟩	🟩
19	Acción preparatoria	España, Francia, Rumanía, Suecia	2018	En curso	Sí	159 380	🟩 **El proyecto sigue en curso en la actualidad y la calidad del informe técnico es buena. También se elaborará un informe independiente.**	🟩	🟩	🟩
20	Acción preparatoria	Grecia, España, Lituania, Finlandia	Agosto de 2019 - agosto de 2020 (prórroga sometida a debate)	En curso	No	86 630	🟨 **La presentación de informes tan solo exigió un informe de evaluación intermedia tras un período de siete meses. Algunos documentos no se encontraban disponibles inmediatamente y tuvieron que remitirse por correo.**	🟩	🟩	🟨 **El proyecto está encontrando dificultades de financiación.**

🟥	No completado
🟨	Completado parcialmente
🟩	Completado
▨	S. O.

Assessment of projects against disinformation (Pilot Projects, Preparatory Actions, Horizon 2020) (Source: European Court of Auditors)

APPENDIX II contains a classification of the TTPs considered in the analysis of information manipulation actions based on their cost and impact.

The information presented was taken from rigorous data analysis carried out by VIGINUM, the French body entrusted with the surveillance and monitoring of information manipulation[15].

This study was complemented by EEAS investigations into Foreign Information Manipulation and Interference (FIMI) (EEAS, 2023, 2024) in the EU.

This analysis was conducted in coordination with early warning systems, the methodology for the development of which is set out in Chapter 6 of the first set of studies published by the Forum against Disinformation Campaigns Affecting National Security (2023), and was extended by EEAS itself, with the aim of identifying and preventing FIMI incidents. The table does not quantify data, but instead offers a qualitative overview of the tactics based on the incidents reviewed.

The assessment of each TTP comprises a summary of empirical observations and recent experiences regarding the cost of the actions and their impact on audiences.

The values allocated reflect:

- Cost: the estimated investment in resources and efforts necessary to carry out each TTP, assessed on the basis of prior incidents.

- Impact: a qualitative measurement of the observed reach and influence of each TTP on the audience or targets of manipulation, based on the impact assessments carried out for specific incidents.

This type of analysis proves especially useful to understand the relative effectiveness of each TTP and to determine which countermeasures and counterstrategies to prioritize.

On identifying which TTPs are particularly effective or economical for threat actors, institutions can optimize their alert and response systems, minimizing the vulnerability of audiences to foreign information manipulation.

[15] The information used in this analysis is available in its public repository at GitHub of VIGINUM (see https://github.com/VIGINUM-FR)

ANALYSIS OF LEGISLATION ADDRESSING THE THREAT

Since 2018, EU and Spanish institutions have been publishing documents—both of a legal and of an informational nature—on hybrid threats and, more specifically, on possible mechanisms for combating one of their most disturbing and harmful elements: disinformation campaigns.

As the aim of this work is to examine the economic implications of disinformation campaigns, both as regards the possible benefit for the attackers and the harm caused to their victims—in terms of the expenditure required to implement mechanisms for prevention, deterrence, detection and recovery—we conducted an analysis of the most relevant legislative texts issued by the European Union and by Spain. The EU legislation analysed included the first EU Code of Practice on Disinformation, published in 2018; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act); Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act); and Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Our analysis also encompassed pertinent Spanish regulations, including Royal Decree 444/2024 of 30 April, regulating the requirements to be considered a special interest user of video-sharing platform services, implementing Article 94 of Act 13/2022 of 7 July (the General Audiovisual Communication Act).

In all cases, our aim was to undertake as comprehensive a study as possible (see APPENDIX III), and not to omit from our analysis any (national or European) contribution that might serve our purpose.

CONCLUSIONS AND PROPOSALS

The fight against disinformation requires a coordinated global effort on the part of governments, tech companies, academia, media, journalists and civil society to identify the economic motivation of disinformation campaigns. Measures must be implemented to strengthen societies' resilience to information manipulation and to foster a more transparent and trustworthy digital environment.

Disinformation campaigns, in addition to their social and political impacts, represent a serious threat to the economic stability of countries. However, disinformation strategies also entail economic impacts for the State actors that deploy them, including their costs, benefits and efficiency, the increase in influence and reach, and their perception of narrative control. Impacts on target audiences are intensified during election periods and crises, which are seen as situations in which democracies and institutions are more vulnerable to erosion, and public opinion more susceptible to influence.

The media has been particularly affected by disinformation, given that the rapid propagation of false content erodes trust in traditional sources of information, leading audiences to change their patterns of consumption of information, turning to alternative websites that use disinformation as a business model, motivated by the increased advertising revenues generated by higher volumes of traffic.

Governments must allocate considerable resources to combating disinformation by implementing measures and protocols for prevention and detection and carrying out awareness-raising campaigns. In this regard, while the European Union has increased funding to combat disinformation, the resources allocated are still considered insufficient.

It is crucial to understand that disinformation not only entails a cost for the governments and companies that seek to combat it, but also benefits the actors that engage in it. These actors, often with political or ideological motivations, seek to obtain economic returns through destabilization, market manipulation and even extortion.

To this end, it is proposed that the DISARM model methodology be used as a tool for analysing the tactics, techniques and procedures (TTPs) employed in disinformation campaigns to identify their economic component. The literature reveals the existence of low-cost, high-impact methods, making these campaigns highly profitable for their perpetrators.

The countries included in this study were analysed individually in greater detail, considering the possible economic motives for—and economic benefits of—using the TTPs identified:

- Russia: This actor uses a wide range of TTPs (including website funding, and use of crowdfunding platforms and crypto wallets), from sophisticated and costly operations to more direct, low-cost tactics. This variability, in addition to the concealment of transactions, hampers monitoring of monetary flows, identification of end beneficiaries and assessment of the return on investment in disinformation.

- China: This actor uses its economic clout to expand its influence through disinformation, investing in State media and digital platforms to spread propaganda and control the narrative. Its disinformation strategy has become more aggressive since the Covid-19 pandemic and it supports the creation of a multipolar world in opposition to the West, strengthening its influence by co-opting voices on social media to improve its image abroad. Owing to the opacity and complexity of its networks of influence, identifying the economic component of China's disinformation actions is very difficult.

- Iran: This country focuses on disseminating anti-Western propaganda and mobilizing support for its geopolitical agenda. Through cybercriminal and hacktivist groups, it engages in disinformation campaigns targeting, among others, the United States and Israel, and uses both State media and digital platforms (such as Telegram and X) to maximize the reach of its narratives and discredit its adversaries. Using open sources to identify the economic impact of Iran's disinformation actions is particularly difficult as they do not contain sufficient information about the financing or monetization mechanisms related to the TTPs used in Iran's campaigns.

- Venezuela: This country's government has tightened its grip on the media and uses social media to discredit the opposition and promote pro-government narratives. The use of networks of fake profiles and trolls and the financing of groups that amplify its narrative are TTPs with a clear economic motivation.

In the case of all the countries analysed, it is extremely difficult to determine, from open sources, whether State actors pay direct or indirect compensation to specific social media users whose posts appear to be in alignment with their propaganda. Regardless, the promotion of such social media profiles by the official media and channels of certain State actors helps them to become widely recognized, to be identified as voices of authority and, consequently, to succeed in widening the audience at which content is targeted.

To tackle the challenge represented by foreign State actors and their proxies, which use disinformation campaigns as a business model to obtain financing with which to continue to pay for their digital apparatus or to recruit influencers beyond their borders, using specific TTPs, it is first necessary to determine whether Spain has any legislation less onerous and prejudicial than the Criminal Code for disarming the threat posed by disinformation. It is then necessary for broad consensus to be reached among renowned experts from different fields on how to respond comprehensively to the disinformation campaigns orchestrated and to examine the solutions proposed by democratic allied countries.

This comprehensive response must address the need for our laws to recognize and penalize new types of offences, to impose sanctions on entities involved in foreign funding and logistical support for disinformation campaigns, to hold domestic proxies and influence agents accountable, to strengthen international cooperation, and to reinforce cyber intelligence and co-regulatory mechanisms, including measures entailing loss of property, goods, media or instruments linked to disinformation campaigns.

APPENDIXES

APPENDIX I: IDENTIFICATION AND DESCRIPTION OF TTPs

TTP	DESCRIPTION
T0002: Facilitate State propaganda	Dissemination by diverse non-official profiles or media from the countries mentioned in this report (including influencers) of their governments' official narrative.
T0003: Leverage existing narratives	Use of narratives existing within a territory that are capable of creating significant social polarization.
T0009: Create fake experts	Invention of profiles to facilitate the dissemination of content.
T0010: Cultivate ignorant agents	Promotion of profiles that act as spokespersons for the interests of the dictatorial country (appearing in their media, writing for their publications, etc.).
T0011: Compromise legitimate accounts	Appropriation of legitimate or existing accounts.
T0013: Create inauthentic websites	Creation of fake Western media webpages to deceive citizens. This method is similar to phishing. A recent example is the Rus-sian Doppelgänger campaign.
T0015: Create hashtags and search artefacts	Creation of artificial hashtags with a view to creating trending topic content.
T0016: Create clickbait	Use of attention-grabbing headlines that draw readers into viewing the content of the news item.
T0017: Conduct fundraising	Use of alternative payment platforms to raise funds (Youtube, X, Tipee, Patreon, GoFundMe, etc.)
T0018: Purchase targeted adver-tisements	Targeting of advertising towards specific audiences.
T0019: Generate information pollu-tion	Generation of media noise about a topic, artificially creating a non-existent debate.
T0022: Leverage conspiracy theory narratives	Exploitation of conspiracy theory narratives already circulating within a territory.

TTP	DESCRIPTION
T0029: Online polls	Manipulation of fake social media polls. Tendentious polls are also included under this TTP.
T0043: Chat apps	Direct messaging via chat apps is an increasing method of de-livery. These messages are often automated and new delivery and storage methods make them anonymous, viral and ephem-eral. This is a difficult space to monitor, but also a difficult space to build acclaim or notoriety.
T0045: Use fake experts	Recruitment of individuals willing to present themselves as ex-perts in a particular field and to peddle official narratives.
T0046: Use search engine optimi-zation	Manipulation of content engagement metrics (X, Meta, Tele-gram)
T0047: Censor social media as a political force	Use of censorship to remove unwanted content.
T0048: Harass	Discrediting of national and foreign opponents, including both actual opponents and social media profiles.
T0049: Flooding the information space	Saturation of social media with content about a specific topic.
T0057: Organize events	Organization of events. The rental of spaces or rooms in which to hold events is included under this TTP.
T0059: Play the long game	Campaign planning, allowing messages to grow organically without amplifying them artificially.
T0066: Degrade adversary	Planning of actions to degrade an adversary's image or ability to act.
T0068: Respond to breaking news event or active crisis	Responding to or commenting on a breaking news story, using unclear facts and incomplete information to increase specula-tion, rumours and conspiracy theories, which are all vulnerable to manipulation.
T0072: Segment audiences	Segmentation of the target audience of a disinformation cam-paign. Russia's efforts to foster the Black Legend of Spanish co-lonialism in Latin America are an example of this tactic.

TTP	DESCRIPTION
T0073: Determine target audiences	Targeting of an action at specific profiles. This tactic is used in Operation Overload, a pro-Kremlin disinformation campaign that floods fact-checkers from different countries with requests to investigate irrelevant issues to prevent them from focussing on truly important matters.
T0074: Determine strategic ends	Undermining of trust in institutions and harm to the reputations and economies of adversary countries.
T0075: Dismiss	Responding to criticisms by dismissing critics. This might consist in an actor arguing that their critics use a different standard for them than for other actors or for themselves, or in arguing that their criticism is biased.
T0076: Distort	Alteration of the framing around information or images to twist the narrative.
T0077: Distract	Diversion of attention towards a different narrative or actor. For instance, an actor may accuse their critics of the same activity of which they have been accused (e.g. police brutality).
T0078: Dismay	Issue of threats to journalists that publish or report on a specific news story.
T0079: Divide	Creation of conflicts between subgroups, to widen divisions in a community.
T0080: Map target audience in-formation environment	Analysis of the information space itself, including social media analytics, web traffic and media surveys.
T0081: Identify social and technical vulnerabilities	Identification of social and technical vulnerabilities determines weaknesses within the target audience information environment for later exploitation. Vulnerabilities include decisive political issues, weak cybersecurity infrastructure, search engine data voids and other technical and non-technical weaknesses in the target audience information environment. Identification of so-cial and technical vulnerabilities facilitates the later exploitation of the identified weaknesses to advance operation objectives.

TTP	DESCRIPTION
T0086: Develop image-based con-tent	Creation and editing of false or misleading visual artefacts, of-ten aligned with one or more specific narratives, for use in a disinformation campaign. This may include photographing staged real-life situations, repurposing existing digital images, or using image creation and editing technologies. This technique includes development of AI-generated images (deepfakes).
T0087: Develop video-based con-tent	Creation and editing of false or misleading video artefacts, of-ten aligned with one or more specific narratives, for use in a disinformation campaign.
T0088: Develop audio-based con-tent	Creation and editing of false or misleading audio artefacts, of-ten aligned with one or more specific narratives, for use in a disinformation campaign. This may include creating completely new audio content, repurposing existing audio artefacts (includ-ing cheap fakes), or using AI-generated audio creation and edit-ing technologies (including deepfakes). It may also include film-ing video footage of staged real-life situations, repurposing ex-isting videos, or using AI-generated video creation and editing technologies (including deepfakes). This technique includes cre-ating videos in which the visual content is accurate but the audio content has been manipulated by amplifying or deleting con-tent.
T0089: Obtain private documents	Procurement of documents that are not publicly available, by whatever means, whether legal or illegal, highly resourced or less so. These documents can include authentic non-public doc-uments, authentic non-public documents that have been altered, or inauthentic documents intended to appear as if they are au-thentic non-public documents. All of these types of documents can be leaked during later stages in the operation (hack-and-leak operations).
T0093: Acquire/recruit network	Acquisition by an operator of an existing network by paying, recruiting, or exerting control over the leaders of the existing network.
T0095: Develop owned media as-sets	An owned media asset refers to an agency or organization through which an influence operation may create, develop and host content and narratives. Owned media assets include web-sites, blogs, social media pages, forums and other platforms that facilitate the creation and organization of content.

TTP	DESCRIPTION
T0096: Leverage content farms	Use of the services of large-scale content providers to create and amplify campaign artefacts at scale. This technique can only be used by countries with significant economic resources.
T0100: Co-opt trusted sources	Co-opting of trusted sources to carry out a disinformation cam-paign
T0101: Create localized content	Creation of content that appeals to a specific community of in-dividuals, often in defined geographical areas. An operation may create localized content using local language and dialects to resonate with its target audience and blend in with other lo-cal news and social media. Localized content may help an oper-ation increase legitimacy, avoid detection, and complicate ex-ternal attribution. Local newspapers are particularly relevant in this regard.
T0114: Deliver ads	Delivery of content via any form of paid media or advertising.
T0115: Post content	Delivery of content by posting via owned media (assets that the operator controls).
T0116: Comment or reply on con-tent	Delivery of content by replying or commenting via owned media (assets that the operator controls).
T0119: Cross-posting	Posting of the same message to multiple internet discussions, social media platforms or accounts, or news groups at one time.
T0123: Control information envi-ronment through offensive cyber-space operations	Controlling the information environment through offensive cy-berspace operations uses cyber tools and techniques to alter the trajectory of content in the information space to either prioritize operation messaging or block opposition messaging.
T0126: Encourage attendance at events	Encouragement to attend or participate in certain events pro-moted by official bodies, think tanks, universities, etc.
T0127: Physical violence	Use of force to injure, abuse, damage or destroy. An influence operation may conduct or encourage physical violence to dis-courage opponents from promoting conflictive content or draw attention to operation narratives using shock value.

TTP	DESCRIPTION
T0128: Conceal Information Assets	Concealment of the identity or provenance of a campaign ac-count and people assets to avoid takedown and attribution. This may include deleting accounts or changing the names they are held in once the message has been disseminated.
T0129: Conceal operational activity	Concealment of the campaign's operational activity to avoid takedown and attribution.
T0130: Conceal infrastructure	Concealment of the campaign's infrastructure to avoid takedown and attribution. This may include deleting Reddit or Telegram groups.
T0131: Exploit TOS/ content mod-eration	Exploitation of weaknesses in platforms' terms of service and content moderation policies to avoid takedowns and platform actions.
T0132: Measure performance	Carry out periodic evaluations of the success of a disinformation campaign.
T0133: Measure effectiveness	A metric used to measure a current system state. The aim is to assess whether the method used will facilitate achievement of the goal pursued.

APPENDIX II: COST-IMPACT RATIO BY TTP

TTP	Cost	Impact
T0002: Facilitate State Propaganda	3	3
T0003: Leverage Existing Narratives	1	2
T0009: Create Fake Experts	2	3
T0010: Cultivate Ignorant Agents	2	2
T0011: Compromise Legitimate Accounts	2	3
T0013: Create Inauthentic Websites	2	3
T0015: Create Hashtags and Search Artifacts	1	2
T0016: Create Clickbait	1	1
T0017: Conduct Fundraising	1	2
T0018: Purchase Targeted Advertisements	3	3
T0019: Generate Information Pollution	1	2
T0022: Leverage Conspiracy Theory Narratives	1	2
T0029: Online Polls	2	2
T0043: Use Chat Apps	1	2
T0045: Use Fake Experts	2	3
T0046: Use Search Engine Optimization	2	3
T0047: Censor Social Media as a Political Force	3	3

T0048: Harass Opponents	2	3
T0049: Flooding the Information Space	2	3
T0057: Organize Events	2	3
T0059: Play the Long Game	2	3
T0066: Degrade Adversary	3	3
T0068: Respond to Breaking News Event or Active Crisis	2	3
T0072: Segment Audiences	1	2
T0073: Determine Target Audiences	1	2
T0074: Determine Strategic Ends	2	3
T0075: Dismiss	1	2
T0076: Distort	1	2
T0077: Distract	1	2
T0078: Dismay	1	2
T0079: Divide	1	3
T0080: Map Target Audience Information Environment	2	3
T0081: Identify Social and Technical Vulnerabilities	2	3
T0086: Develop Image-based Content	2	2
T0087: Develop Video-based Content	2	2
T0088: Develop Audio-based Content	2	2

T0089: Obtain Private Documents	2	3
T0093: Acquire/Recruit Network	3	3
T0095: Develop Owned Media Assets	3	3
T0096: Leverage Content Farms	3	3
T0100: Co-opt Trusted Sources	3	3
T0101: Create Localized Content	2	3
T0114: Deliver Ads	2	3
T0115: Post Content	1	2
T0116: Comment or Reply on Content	1	2
T0119: Cross-Posting	2	3
T0123: Control Information Environment through Offensive Cyberspace Operations	3	3
T0126: Encourage Attendance at Events	2	3
T0127: Physical Violence	3	3
T0128: Conceal People	3	3
T0129: Conceal Operational Activity	3	3
T0130: Conceal Infrastructure	3	3
T0131: Exploit TOS/Content Moderation	2	3
T0132: Measure Performance	2	2
T0133: Measure Effectiveness	2	3

APPENDIX III: LEVEL OF ESTIMATED ALIGNMENT/ EFFECTIVENESS OF NATIONAL AND EUROPEAN LEGISLATION ADDRESSING THE THREAT

LEGEND

Estimated level of alignment and effectiveness of the related documents in response to the TTPs:

🟩 **SIGNIFICANT effect**

🟨 **MODERATE effect**

🟥 **LOW effect**

	Ley 13/2022, de 7 de julio, **General de Comunicación Audiovisual.**	Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE **(Reglamento de Servicios Digitales).**	Real Decreto 1138/2023, de 19 de diciembre, por el que se regulan el **Registro estatal de prestadores del servicio de comunicación audiovisual, de prestadores del servicio de intercambio de vídeos a través de plataforma y de prestadores del servicio de agregación de servicios de comunicación audiovisual y el procedimiento de comunicación previa de inicio de actividad.**	Reglamento (UE) 2024/900 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, sobre **transparencia y segmentación en la publicidad política**.	Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE **(Reglamento Europeo sobre la Libertad de los Medios de Comunicación).**
TTP	**Artículos aplicables**				
T0002: Facilitate State Propaganda	art. 42		art. 12	arts. 1 y 8	art. 6
T0003: Leverage Existing Narratives	art. 78				
T0009: Create Fake Experts			art. 12	arts. 11 y 12	
T0010: Cultivate Ignorant Agents	art. 79	art. 22			art. 18
T0011: Compromise Legitimate Accounts	arts. 14 y 15		art. 36		
T0013: Create Inauthentic Websites	art. 9	arts. 9,10	art. 27	art. 11	
T0015: Create Hashtags and Search Artifacts					
T0016: Create Clickbait	art. 78		art. 12	arts. 11 y 12	
T0017: Conduct Fundraising	arts. 14 y 15	art. 67	art. 13		
T0018: Purchase Targeted Advertisements	arts. 14 y 15	art. 44		art. 18	
T0019: Generate Information Pollution	art. 78			art. 13	
T0022: Leverage Conspiracy Theory Narratives					
T0029: Online Polls	arts. 14 y 15	art. 25			

T0043: Use Chat Apps					
T0045: Use Fake Experts			art. 12		
T0046: Use Search Engine Optimization	arts. 14 y 15				
T0047: Censor Social Media as a Political Force	arts. 14 y 15				arts. 3,17
T0048: Harass Opponents		arts.9,34	art. 32	art. 15	
T0049: Flooding the Information Space	arts. 14 y 15	arts. 34, 35	art. 20	arts. 11 y 12	
T0057: Organize Events	art. 78				
T0059: Play the Long Game	arts. 14 y 15				
T0066: Degrade Adversary	art. 78	arts. 9,10			
T0068: Respond to Breaking News Event or Active Crisis	arts. 14 y 15				
T0072: Segment Audiences	art. 78	art. 44		art. 18	
T0073: Determine Target Audiences	DA5[a]	art. 44		art. 18	art. 20
T0074: Determine Strategic Ends	art. 78	arts. 34,35			
T0075: Dismiss		arts. 9,10			
T0076: Distort					
T0077: Distract					
T0078: Dismay	art. 78				
T0079: Divide	arts. 14 y 15				
T0080: Map Target Audience Information Environment	art. 78	art. 34			art. 6
T0081: Identify Social and Technical Vulnerabilities					
T0086: Develop Image-based Content	art. 98	art. 100			
T0087: Develop Video-based Content	art. 98	art. 100			
T0088: Develop Audio-based Content	arts. 14 y 15				
T0089: Obtain Private Documents					

T0093: Acquire/Recruit Network			art. 12		
T0095: Develop Owned Media Assets	art. 78		art. 12		
T0096: Leverage Content Farms	art. 78	arts. 34,35			
T0100: Co-opt Trusted Sources	art. 42	art. 22			art. 6
T0101: Create Localized Content	arts. 14 y 15				
T0114: Deliver Ads	arts. 14 y 15	arts. 9,10	art. 13	art. 18	
T0115: Post Content		arts. 9,10			
T0116: Comment or Reply on Content	arts. 14 y 15	arts. 9,10			
T0119: Cross-Posting	arts. 14 y 15	art. 35			
T0123: Control Information Environment through Offensive Cyberspace Operations		arts. 34,35			
T0126: Encourage Attendance at Events					
T0127: Physical Violence	art. 78	art. 67			
T0128: Conceal People	arts. 14 y 15	art. 30			art. 6
T0129: Conceal Operational Activity		art. 30			
T0130: Conceal Infrastructure		art. 67			
T0131: Exploit TOS/Content Moderation	arts. 14 y 15	art. 34			
T0132: Measure Performance	art. 78				
T0133: Measure Effectiveness	arts. 14 y 15				

	The Strengthened Code of Practice on disinformation 2022	**Plan de Acción contra la desinformación.**	**Directrices** de la Comisión para los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño para la **reducción de los riesgos sistémicos en los procesos electorales de conformidad con el artículo 35, apartado 3, del Reglamento (UE) 2022/2065**	Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 **(Reglamento de Inteligencia Artificial).**
TTP	**Artículos aplicables**			
T0002: Facilitate State Propaganda	Comp. 4 al 13	Pilar 1 / Acción 1	secciones 3.2.1(c)(iv) / 3.2.27	
T0003: Leverage Existing Narratives	Comp. 18	Pilar 4 / Accs 7, 9		
T0009: Create Fake Experts	Comp. 14	Pilar 3 / Acción 6	secciones 3.2.1 (c)(iii) / 3.2.1 (c)(iv) / 3.2.1 (c)(v)	art. 52
T0010: Cultivate Ignorant Agents				
T0011: Compromise Legitimate Accounts			sección 3.2.1(h)	
T0013: Create Inauthentic Websites	Comp. 1	Pilar 1 / Acción 1	secciones 3.2.1 (h) / 3.2.1 (i)	art. 50
T0015: Create Hashtags and Search Artifacts	Comp. 14 / Med. 14.1	Pilar 1 / Acción 1		
T0016: Create Clickbait			sección 3.2.1 (c)(ii)	
T0017: Conduct Fundraising	Comp. 1 / Med. 1.1	Pilar 3 / Acción 6	sección 3.2.1€	
T0018: Purchase Targeted Advertisements	Comp. 2 /Meds. 2.1, 2.2	Pilar 3 / Acción 6		arts. 50 y 52
T0019: Generate Information Pollution				

T0022: Leverage Conspiracy Theory Narratives	Comp. 18	Pilar 4 / Accs 7, 9		
T0029: Online Polls				
T0043: Use Chat Apps	Comp. 25 / Med. 25.2	Pilar 3 / Acción 6		
T0045: Use Fake Experts	Comp. 14	Pilar 3 / Acción 6	secciones 3.2.1 (c)(iii) / 3.2.1 (c)(iv) / 3.2.1 (c)(v)	art. 52
T0046: Use Search Engine Optimization	Med. 14.1	Pilar 1 / Acción 1		art. 5
T0047: Censor Social Media as a Political Force	Cons. (c)	Introducción		
T0048: Harass Opponents	Comp. 48	Pilar 3 / Acción 6	sección 3.2.1(h) / 3.2.1(i)	
T0049: Flooding the Information Space			sección 3.2.1(d)	art. 110
T0057: Organize Events				
T0059: Play the Long Game				
T0066: Degrade Adversary			sección 3.2.1 (b)	
T0068: Respond to Breaking News Event or Active Crisis				
T0072: Segment Audiences			sección 3.112	
T0073: Determine Target Audiences			sección 3.112	
T0074: Determine Strategic Ends				
T0075: Dismiss				
T0076: Distort				
T0077: Distract	Comp. 21	Pilar 4 / Acción 9		
T0078: Dismay				
T0079: Divide				

T0080: Map Target Audience Information Environment			sección 3.112	
T0081: Identify Social and Technical Vulnerabilities				
T0086: Develop Image-based Content				art. 52
T0087: Develop Video-based Content				art. 52
T0088: Develop Audio-based Content				
T0089: Obtain Private Documents				
T0093: Acquire/Recruit Network			sección 3.2.1(i)	
T0095: Develop Owned Media Assets			sección 3.2.1(c)	
T0096: Leverage Content Farms				
T0100: Co-opt Trusted Sources				
T0101: Create Localized Content	Comp. 30	Pilar 4 / Acción 8		
T0114: Deliver Ads				arts. 50 y 52

T0115: Post Content				
T0116: Comment or Reply on Content				
T0119: Cross-Posting				
T0123: Control Information Environment through Offensive Cyberspace Operations				
T0126: Encourage Attendance at Events				
T0127: Physical Violence				
T0128: Conceal People				
T0129: Conceal Operational Activity				
T0130: Conceal Infrastructure				
T0131: Exploit TOS/Content Moderation				arts. 117 y 118
T0132: Measure Performance	Comps. 34, 38 al 44	Pilar 1 / Acción 1		
T0133: Measure Effectiveness				

APPENDIX IV: CRYPTOCURRENCY AS A FINANCING METHOD

In recent years, cryptocurrencies have emerged as a method of financing that facilitates disinformation campaigns and interference operations at the global level. State and non-State actors take advantage of the apparent anonymity and transnational nature of cryptocurrency to finance, organize and maintain networks that seek to destabilize democracies and sow distrust in institutions. Payments in cryptocurrency enable these actors to acquire digital infrastructure, such as online servers and hosting services, which are essential to creating and managing false news websites, bot networks and social media profiles that amplify their influence campaigns.

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury has identified numerous cryptocurrency addresses linked to individuals and organizations that participate in disinformation campaigns and has placed sanctions on those who finance and support these activities.

Donations of cryptocurrencies such as Bitcoin and USDT have been used to finance military operations and propaganda. For example, the Russian disinformation outlet SouthFront asks for cryptocurrency donations on its website, giving instructions to its followers to transfer funds from their personal wallets in order to avoid intermediaries. Another case in point is that of the paramilitary group Task Force Rusich, which is linked to the war in Ukraine; evidence has been found that this group makes use of cryptocurrency to finance the purchase of military equipment and spread propaganda supporting the aims of the Russian government.

Furthermore, these groups purchase stolen accounts and use hosting services on anonymous servers, which also accept payments in cryptocurrencies. On the darknet, there are platforms that sell compromised social media accounts, making it easier for disinformation actors to pass themselves off as actual users and reach large audiences on a massive scale. These services, often in languages such as Russian, enable the large-scale acquisition of accounts, offering threat actors the capacity to scale up their campaigns without being detected. At the same time, providers of offshore infrastructure, such as the Shinjiru web hosting service, offer anonymity to propaganda sites, allowing disinformation campaigns to remain active without risk of regulatory oversight.

The impact of cryptocurrency-backed campaigns is especially evident when they are deployed in combination with troll and bot networks that amplify the messaging.

Pro-Russian paramilitary groups and actors use messaging platforms such as Telegram to ask for cryptocurrency donations which are then used to fund disinformation operations and military activities. Investigations show that some of these actors have received millions of dollars in cryptocurrencies, funds that then flow to exchange accounts where cryptocurrencies are converted into fiduciary currency to finance diverse illicit activities.

Blockchain analysis enables investigators to trace transactions and connect the actors and organizations that finance these disinformation networks.

Tracing cryptocurrencies has become an indispensable tool for security agencies seeking to dismantle global influence networks and identify the actors and financers behind them. Given that cryptocurrencies are frequently used by disinformation actors, blockchain activity contains indicators and evidence that can help government agencies, and investigators in general, to identify, analyse and, in the case of the former, detain threat actors, if evidence of criminal activity is uncovered. Over time, blockchain analysis companies have collaborated with public agencies to trace cryptocurrency transactions linked to diverse illicit activities; analysts and investigators can use cryptocurrency tracing techniques both to increase their understanding of criminal networks and to effectively put an end to their activities.

BIBLIOGRAPHY

Abril, G. (2022), “Xi Jinping, according to the propaganda”, *El País* https://english.elpais.com/international/2022-10-23/xi-jinping-according-to-the-propaganda.html, 22 October.

Abril, G. and Bonet, I. (2022), “Protests spread across China as anger builds over Xi Jinping’s zero-Covid policy”, *El País* https://english.elpais.com/international/2022-11-27/protests-spread-across-china-as-anger-builds-over-xi-jinpings-zero-covid-policy.html, 27 November.

AFP (2023), “US politicians, commentators misrepresent fictional pride flag skit” https://factcheck.afp.com/doc.afp.com.33VL6VA, 19 September.

Aguirre, M. (2022), Una nueva y diferente Guerra Fría. *OBSERVARE - JANUS 2022 - O país que somos o(s) mundo(s) que temos: um roteiro para o conceito estratégico na próxima década*, 102-103. http://hdl.handle.net/11144/5547

Araújo, H. (2022), “Malos tiempos para los pensadores chinos”, *El País* https://elpais.com/ideas/2022-11-01/malos-tiempos-para-los-pensadores-chinos.html, 1 November.

Arteaga, F. and Simón, L. (2021), NATO gets an update: the Madrid Strategic Concept, *Elcano Royal Institute* https://www.realinstitutoelcano.org/en/analyses/nato-gets-an-update-the-madrid-strategic-concept/

Arteaga, F. and Simón, L. (2022), El Concepto Estratégico de Madrid: una (auto)evaluación de los resultados, *Elcano Royal Institute* https://www.realinstitutoelcano.org/analisis/el-concepto-estrategico-de-madrid-una-autoevaluacion-de-los-resultados/

Bartolomé, M. C. (2021), Redes sociales, desinformación, cibersoberanía y vigilancia digital: una visión desde la ciberseguridad, *Revista Estudios en Seguridad Internacional*, 7(2), 167-185. https://seguridadinternacional.es/resi/html/redes-sociales-desinformacion-cibersoberania-y-vigilancia-digital-una-vision-desde-la-ciberseguridad/

Belinchón, G. (2022), “El cine de propaganda nunca ha desaparecido: ahora se lanzan a él chinos and rusos”, *El País* https://elpais.com/cultura/2022-07-08/el-cine-de-propaganda-nunca-ha-desaparecido-ahora-se-lanzan-a-el-chinos-y-rusos.html, 8 July.

Bergmanis-Korāts, G. and Haiduchyk, T. (2024), Social Media Manipulation for Sale: Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement, *NATO Strategic Communications Centre of Excellence* https://stratcomcoe.org/publications/social-media-manipulation-for-sale-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/311, 4 November.

Bradshaw, S., Bailey, H. and Howard, P. N. (2020), Industrialized Disinformation - 2020 Global Inventory of Organized Social Media Manipulation, *Oxford Internet Institute, University of Oxford* https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf

Brändle, V. K., Galpin, C., and Trenz, H. J. (2021), Brexit as 'politics of division': social media campaigning after the referendum. *Social Movement Studies, Volume 21 (Issue 1-2)*, 234–253. https://doi.org/10.1080/14742837.2021.1928484

Brime, I. (2021), "La obsesión multipolar de China", *El Español* https://www.elespanol.com/blog_del_suscriptor/opinion/20210314/obsesion-multipolar-china/565763420_7.html, 14 March.

Burgess, C. (2023), The Dark Side of LinkedIn: China's Espionage Playground, *Clearance Jobs* https://news.clearancejobs.com/2023/08/30/the-dark-side-of-linkedin-chinas-espionage-playground/, 30 August.

Center for Defense Reforms (2024), *Toy Soldiers: NATO military and intelligence officers in Russian active measure* https://acrobat.adobe.com/id/urn:aaid:sc:EU:2df9e67c-6264-4cec-96c5-ab2d16d19be7

Chan, K. and Thornton, M. (2022), "China's Changing Disinformation and Propaganda Targeting Taiwan", *The Diplomat* https://thediplomat.com/2022/09/chinas-changing-disinformation-and-propaganda-targeting-taiwan/, 19 September.

Cheung, R. (2022), "Anti-Xi Jinping Posters Are Spreading in China via AirDrop", *Vice* https://www.vice.com/en/article/wxn7nq/anti-xi-jinping-posters-are-spreading-in-china-via-airdrop, 19 October.

Christov, A. (2019), ECONOMY OF THE FAKE NEWS: BUSINESS SIDE AND EFFECTS. *Eastern Academic Journal*, Issue 4, pp. 1-7 https://www.e-acadjournal.org/pdf/article-19-4-1.pdf

Cocuyo chequea (2023), #CiberalianzaAlDescubierto: El Mazo y las redes anónimas se unen para desinformar, *Efectococuyo* https://efectococuyo.com/cocuyo-chequea/ciberalianzaaldescubierto-el-mazo-y-las-redes-anonimas-se-unen-para-desinformar/, 22 November.

Condliffe, J. (2017), "Fake News Is Unbelievably Cheap to Produce", *MIT Technology Review* https://www.technologyreview.com/2017/06/14/151233/fake-news-is-unbelievably-cheap/, 14 June.

Cook, S. (2020), Special Report 2020. Beijing's Global Megaphone, The Expansion of Chinese Communist Party Media Influence since 2017, *Freedom House* https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone, 11 January.

Corera, G. (2020), "Why did MI5 name Christine Lee as an 'agent of influence'?", *BBC* https://www.bbc.com/news/uk-62179004, 19 July.

Council of the European Union (2024), *Venezuela: Statement by the High Representative on behalf of the EU on post-election developments* [Press release] https://www.consilium.europa.eu/en/press/press-releases/2024/08/04/venezuela-statement-by-the-high-representative-on-behalf-of-the-eu/, 4 August.

Davidson, H. (2021), Chinese media in fake news claims over Swiss scientist critical of US, *The Guardian* https://www.theguardian.com/world/2021/aug/11/chinese-media-fake-news-claims-swiss-scientist-wilson-edwards-critical-of-us, 11 August.

De la Cal, L. (2022), "Desesperados por escapar de China: 'No podía aguantar la extrema política de restricciones'", *El Mundo* https://www.elmundo.es/internacional/2022/06/05/628618b021efa0801d8b45b8.html, 5 June.

De la Cal, L. (2022), "La nueva era 'democrática' de Hong Kong según Xi Jinping: una ciudad que solo puede ser gobernada por patriotas", *El Mundo* https://www.elmundo.es/internacional/2022/07/01/62bea4f0fdddfff53c8b45f5.html, 1 July.

De la Cal, L. (2022), "China exprime la artillería propagandística con vídeos a la norcoreana", *El Mundo* https://www.elmundo.es/internacional/2022/08/07/62ee82e6fc6c83e91f8b45cc.html, 7 August.

De la Cal, L. (2022), "China empieza a rebelarse contra el 'Covid cero': violentas protestas en la mayor fábrica de iPhone del mundo", *El Mundo* https://www.elmundo.es/internacional/2022/11/24/637dee80e4d4d8704f8b45b2.html, 24 November.

Delage, F. (2019), China y la gobernanza económica global: hacia un orden pluralista, *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, 21(42), 133-153 https://www.redalyc.org/journal/282/28264997007/28264997007.pdf

Department of National Security (27 September 2022), *Lucha contra las campañas de desinformación en el ámbito de la seguridad nacional: propuestas de la sociedad civil*, Publications catalogue of the Spanish Central Administration https://www.dsn.gob.es/es/publicaciones/otras-publicaciones/lucha-contra-campanas-desinformacion-ambitoSN-propuestas

DFRLab (2023), "How China funds foreign influence campaigns", *Medium* https://medium.com/dfrlab/how-china-funds-foreign-influence-campaigns-72d547ad0771, 12 January.

DISARM (2022), DISARM *Framework Explorer* https://disarmframework.herokuapp.com/

Dubow, B., Greene, S., and Rzegocki, S. (2022), "Tracking Chinese Online Influence in Central and Eastern Europe", *Center for European Policy Analysis (CEPA)* https://cepa.org/comprehensive-reports/tracking-chinese-online-influence-in-central-and-eastern-europe/, 28 September.

Economist Intelligence Unit (2023), *Democracy Index 2023* https://www.eiu.com/n/campaigns/democracy-index-2023/

Europa Press (2022), "China oculta ahora sus casos diarios de Covid ante la avalancha de nuevos contagios", *El Confidencial* https://www.elconfidencial.com/mundo/2022-12-25/china-oculta-ahora-sus-casos-diarios-de-covid-ante-la-avalancha-de-contagios_3547742/, 25 December.

European Court of Auditors (2021), Special Report 09/2021: Disinformation affecting the EU: tackled but not tamed https://www.eca.europa.eu/en/publications/SR21_09

European Parliament (March 2021), *Strategic communications as a key factor in countering hybrid threats*. European Parliamentary Research Service (EPRS), Scientific Foresight Unit (STOA) https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323

European Parliament (2022), *Report on foreign interference in all democratic processes in the European Union, including disinformation*, European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html

Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional (2023), *Trabajos 2023*, Presidency of the Government https://www.dsn.gob.es/sites/default/files/documents/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf

Freedom House (2024), *Freedom in the world 2024* https://freedomhouse.org/sites/default/files/2024-02/FIW_2024_DigitalBooklet.pdf

Gadzynska, I., Mikhalkov, S. Tymoshenko, M., Lytvynov, V., Kelm, N. and Drozdova, Y. (2024), *Roller Coaster. From Trumpists to Communists. The forces in the U.S. impeding aid to Ukraine and how they do it* https://texty.org.ua/projects/112617/roller-coaster/

Global Disinformation Index (8 November 2022), Ad-funded Elections Integrity Disinformation, *Disinformationindex.org*

Global Engagement Center (2020), GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem, *U.S. Department of State* https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

Global Engagement Center (2020), GEC Special Report: How the People's Republic of China Seeks to Reshape the Global Information Environment, U.S. *Department of State* https://www.state.gov/wp-content/uploads/2023/09/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_Final.pdf

Global Influence Operations Report (2022), *German Intelligence Says China Seeks to Instrumentalize Diaspora Groups and Journalists; 'Win Over' Politicians as Lobbyists* https://www.global-influence-ops.com/german-intelligence-says-china-seeks-to-instrumentalize-diaspora-groups-and-journalists-win-over-politicians-as-lobbyists/, 20 July.

González Enríquez, C. and Martínez Romera, J. (2022), Barometer of the Elcano Royal Institute. Special edition: War in Ukraine and the NATO Summit, June 2022, *Elcano Royal Institute* https://www.realinstitutoelcano.org/en/surveys/barometer-special-edition-war-in-ukraine-and-nato-summit/

Graham, E. (2022), "China's Reported Manipulation of Twitter Draws Lawmaker Questions", *Nextgov*/FCW https://www.nextgov.com/cybersecurity/2022/12/chinas-reported-manipulation-twitter-draws-lawmaker-questions/380642/, 8 December.

Hao, Z. (2022), How NATO began with confrontation and ends with poisoning world peace? *Global Times* https://www.globaltimes.cn/page/202206/1269264.shtml, 28 June.

Heikkinen, D. (2021), An analysis of fake news and its effects on the economy and society, MPRA Paper 116027, *University Library of Munich, Germany*. https://mpra.ub.uni-muenchen.de/116027/1/MPRA_paper_116027.pdf

Hernández, E. (2022), Interview with Javier Solana: "El actor importante es China, no Rusia", *El Confidencial* https://www.elconfidencial.com/espana/2022-06-26/javier-solana-entrevista_3448509/, 26 June.

Hernández, E. and García, L.M. (2021), Chinese strategic thinking. The fundamentals of the Chinese model of world governance, *Sinología Hispánica. China Studies Review, 12(1), 1–32*. https://revpubli.unileon.es/index.php/sinologia/article/view/7101/5567

Hernández, O. (2022), La prensa oficialista, 'bombero' de Pekín: "Las medidas 'covid cero' son el único camino correcto, *El Confidencial* https://www.elconfidencial.com/mundo/2022-11-29/prensa-china-silencia-protestas-medidas-covid-cero_3530868/, 29 November.

IBERIFIER Iberian Digital Media Observatory (2023), IBERIFIER Reports – *Analysis of the Impact of Disinformation on Political, Economic, Social and Security Issues, Governance Models and Good Practices: The Cases of Spain and Portugal* https://iberifier.eu/2023/06/21/report-analysis-impact-disinformation-june-2023/, 21 June.

International Republican Institute (2022), *Coercion, Capture, and Censorship: Case Studies on the CCP's Quest for Global Influence* https://www.iri.org/wp-content/uploads/2022/09/IRI-Coercion-Capture-and-Censorship-Case-Studies-on-the-CCPs-Quest-for-Global-Influence-September-2022.pdf 28 September.

IT@Priority (2020), "Fake News and its Impact on the Economy", *Priority Consultants* https://priorityconsultants.com/fake-news-and-its-impact-on-the-economy/, 11 August.

Keown, A. (2018), "China's 'Thousand Talents Plan' Recruits Western Scientists and Researchers", *BioSpace* https://www.biospace.com/china-s-thousand-talents-plan-recruits-western-scientists-and-researchers, 27 November.

Kerr, N. (2023), "What RFK Jr., now a presidential candidate, has said about Ukraine, vaccines, the economy and more", *ABC News* https://abcnews.go.com/Politics/rfk-jr-now-presidential-candidate-ukraine-vaccines-economy/story?id=100247005, 22 June.

Krenz, N. (2022), An Analysis of the 2020 Zoom Breach, *Cloud Security Alliance* https://cloudsecurityalliance.org/blog/2022/03/13/an-analysis-of-the-2020-zoom-breach, 13 March.

Ling, L. (2022), "How China's Party Congress Actually Works. Unpacking the institution of the National Party Congress – its essential concepts and some common misunderstandings", *The Diplomat* https://thediplomat.com/2022/08/how-chinas-party-congress-actually-works/, 1 September.

Ling, L. [@lingli_vienna] (2022), *I wrote a long-form piece for The Diplomat, explaining how the Party Congress works. I also identify the formally authorized group who makes the final approval of nominated candidates for the membership of the Central Committee. Main takeaways. A thread, X* https://twitter.com/lingli_vienna/status/1566798991781765120, 5 September.

Ling, L. [@lingli_vienna] (2022), *A thread about my last [thread] on How the Party Congress Actually Works. This [thread] includes: A correction Some response to questions posted to me about the Chairmen-league Standing Committee (SCOCL). Its members sit in the front row. Ordinary members of the League sit at the back*, X https://x.com/lingli_vienna/status/1567543444997914631, 7 September.

Luna, J. (2022), Interview with Joshua Kurlantzick. “China igualará pronto a Rusia en fake news”, *La Vanguardia* https://www.lavanguardia.com/internacional/20221128/8621009/china-iguala-ra-pronto-rusia-fake-news.html, 28 November.

M. Martin, C. (2022), “The PRC: International Stimulus, Strategic Culture and Resulting Domestic Policies”, *The Defence Horizon Journal* https://www.thedefencehorizon.org/post/the-prc-international-stimulus-strategic-culture-and-resulting-domestic-policies, 11 August.

Menn, J. (2022), “Twitter grapples with Chinese spam obscuring news of protests”, *The Washington Post* https://www.washingtonpost.com/technology/2022/11/27/twitter-china-spam-protests/, 27 November.

Menn, J. (2024), “News site editor’s ties to Iran, Russia show misinformation’s complexity”, *The Washington Post* https://www.washingtonpost.com/technology/2024/06/02/grayzone-russia-iran-support/, 2 June.

Milosevich-Juaristi, M. (2020), “¿Por qué hay que analizar y comprender las campañas de desinformación de China y Rusia sobre el COVID-19?”, *Elcano Royal Institute* https://www.realinstitutoelcano.org/analisis/por-que-hay-que-analizar-y-comprender-las-campanas-de-desinformacion-de-china-y-rusia-sobre-el-covid-19/, 20 April.

Ministry of Foreign Affairs, European Union and Cooperation (2024), *Joint statement on Venezuela,* [Press Statement 044] https://www.exteriores.gob.es/en/Comunicacion/Comunicados/Paginas/2024_COMUNICADOS/20240816_COMU044.aspx#:~:text=We%2C%20the%20undersigned%20countries%2C%20assembled,restraint%20in%20their%20public%20actions, 16 August.

Mitchell, R. (2024), “Internet Censorship Verging on Service Blocking Ahead of Venezuela Elections”, *Internet Society* https://pulse.internetsociety.org/blog/internet-censorship-verging-on-service-blocking-ahead-of-venezuela-elections, 26 July.

National Cryptologic Centre [CCN] (2021), D*isinformation in Cyberspace,* CCN-CERT BP/13 https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/3558-ccn-cert-bp-13-disinformation-in-cyberspace/file.html

National Intelligence Council (2020), Cyber Operations Enabling Expansive Digital Authoritarianism https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf, 7 April.

Netherlands (2022), *Government-wide strategy for effectively tackling disinformation*, Ministry of the Interior and Kingdom Relations, Directorate-General for Public Administration and Democratic Rule of Law/Democracy and Governance Directorate https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation

IRNA (2023), “Viaje de periodistas españoles a Irán; ‘Los occidentales tergiversan las realidades del país’”, *The Islamic Republic News Agency (IRNA)* https://es.irna.ir/news/85145576/Viaje-de-periodistas-espa%C3%B1oles-a-Ir%C3%A1n-Los-occidentales-tergiversan, 19 June.

Iranwire (2024), “Iranian Authorities Bet on Foreign Influencers to Boost Tourism”, *Iranwire* https://iranwire.com/en/news/125094-iranian-authorities-bet-on-foreign-influencers-to-boost-tourism/, 7 February.

Nimmo, B. (2022), “Removing Coordinated Inauthentic Behavior From China and Russia”, *Meta* https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/, 27 September.

Novelo, A. (2024), “RFK Jr. offers foreign policy views on Ukraine, Israel, vows to halve military spending”, *CBS News* https://www.cbsnews.com/news/rfk-jr-foreign-policy-views-ukraine-israel-military-spending/, 13 June.

Papadogiannakis, E., Papadopoulos, P., Markatos, E.P., and Kourtellis, N. (2023), Who Funds Misinformation? A Systematic Analysis of the Ad-related Profit Routines of Fake News sites, from *Proceedings of the ACM Web Conference 2023*, 2765-2776 https://doi.org/10.48550/arXiv.2202.05079

Pérez Gallardo, M. (2024), “¿Quiénes serán los observadores electorales en las presidenciales de Venezuela?”, *France24* https://www.france24.com/es/am%C3%A9rica-latina/20240727-quienes-ser%C3%A1n-los-observadores-electorales-en-las-presidenciales-de-venezuela, 27 July.

Pollard, M. Q. and Goh, B. (2022), “Blank sheets of paper become symbol of defiance in China protests”, *Reuters* Blank sheets of paper become symbol of defiance in China protests | Reuters, 28 November.

Priego, A. (2022), “Los seis ejes de la cumbre de la OTAN en Madrid”, *The Conversation* https://theconversation.com/los-seis-ejes-de-la-cumbre-de-la-otan-en-madrid-185882, 27 June.

Radio Televisión Española (2022), La movilización contra la política *‘COVID cero’ deja las mayores protestas en China en 30 años* [Video], RTVE https://www.rtve.es/play/videos/telediario-2/movilizacion-contra-covid-cero-deja-mayores-protestas-china-treinta-anos/6746415/, 28 November.

Rathbone, J. P. and Sevastopulo, D. (2022), “‘On a par with the Russians’: rise in Chinese espionage alarms Europe”, *Financial Times* https://www.ft.com/content/282aed88-de6e-4356-8a46-5718943853c4, 29 August.

Repnikova, M. (2022), “The Balance of Soft Power. The American and Chinese Quests to Win Hearts and Minds”, *Foreign Affairs* https://www.foreignaffairs.com/china/soft-power-balance-america-china, 21 June.

Reuters (2022), “U.S. counterintelligence warns of China stepping up influence operations”, *Reuters* https://www.reuters.com/world/us/us-counterintelligence-warns-china-stepping-up-influence-operations-2022-07-06/, 7 July.

Sammarco, A. (2024), “RFK Jr. Repeats Russian Propaganda on Ukraine”, *Los Angeles Magazine* https://lamag.com/news-and-politics/rfk-jr-repeats-russian-propaganda, 5 April.

Service for Vigilance and Protection against Foreign Digital Interference [VIGINUM], (2023), RRN: *A complex and persistent information manipulation campaign* https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf, 19 July.

Service for Vigilance and Protection against Foreign Digital Interference [VIGINUM], (February 2024), PORTAL KOMBAT. *A structured and coordinated pro-Russian propaganda network* https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf

Service for Vigilance and Protection against Foreign Digital Interference [VIGINUM], (2024), MATRYOSHKA, *A pro-Russian campaign targeting media and the fact-checking community* https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf

Solymos, K. K., and Panyi, S. (2023), Imam, Soldier, Diplomat, Interpreter: Meet the Hungarian NewsFront's Propagandists. *VSquare* https://vsquare.org/newsfront-russia-hungary-disinformation-telegram-propaganda/

Sputnik (26 July 2023), *Robert f. Kennedy Jr: Occidente "torpedeó" la paz en Ucrania "porque queremos la guerra con Rusia"* https://noticiaslatam.lat/20230726/robert-f-kennedy-jr-occidente-torpedeo-la-paz-en-ucrania-porque-queremos-la-guerra-con-rusia-1141941972.html

Strategic Communications, Task Forces and Information Analysis (STRAT.2) Data Team (2023), 1st EEAS Report on Foreign Information *Manipulation and Interference Threats: Towards a framework for networked defence, European Union External Action*, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

Strategic Communications, Task Forces and Information Analysis (STRAT.2) (2024), *2nd EEAS Report on Foreign Information Manipulation and Interference Threats. A Framework for Networked Defence, European External Action Service* https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

Surawy Stepney, E. and Lally, C. (2024), D*isinformation: sources, spread and impact*, UK Parliament POST https://researchbriefings.files.parliament.uk/documents/POST-PN-0719/POST-PN-0719.pdf, 25 April.

The Associated Press (2020), "China delayed releasing coronavirus info, frustrating WHO", *The Associated Press* https://apnews.com/article/united-nations-health-ap-top-news-virus-outbreak-public-health-3c061794970661042b18d5aeaaed9fae, 2 June.

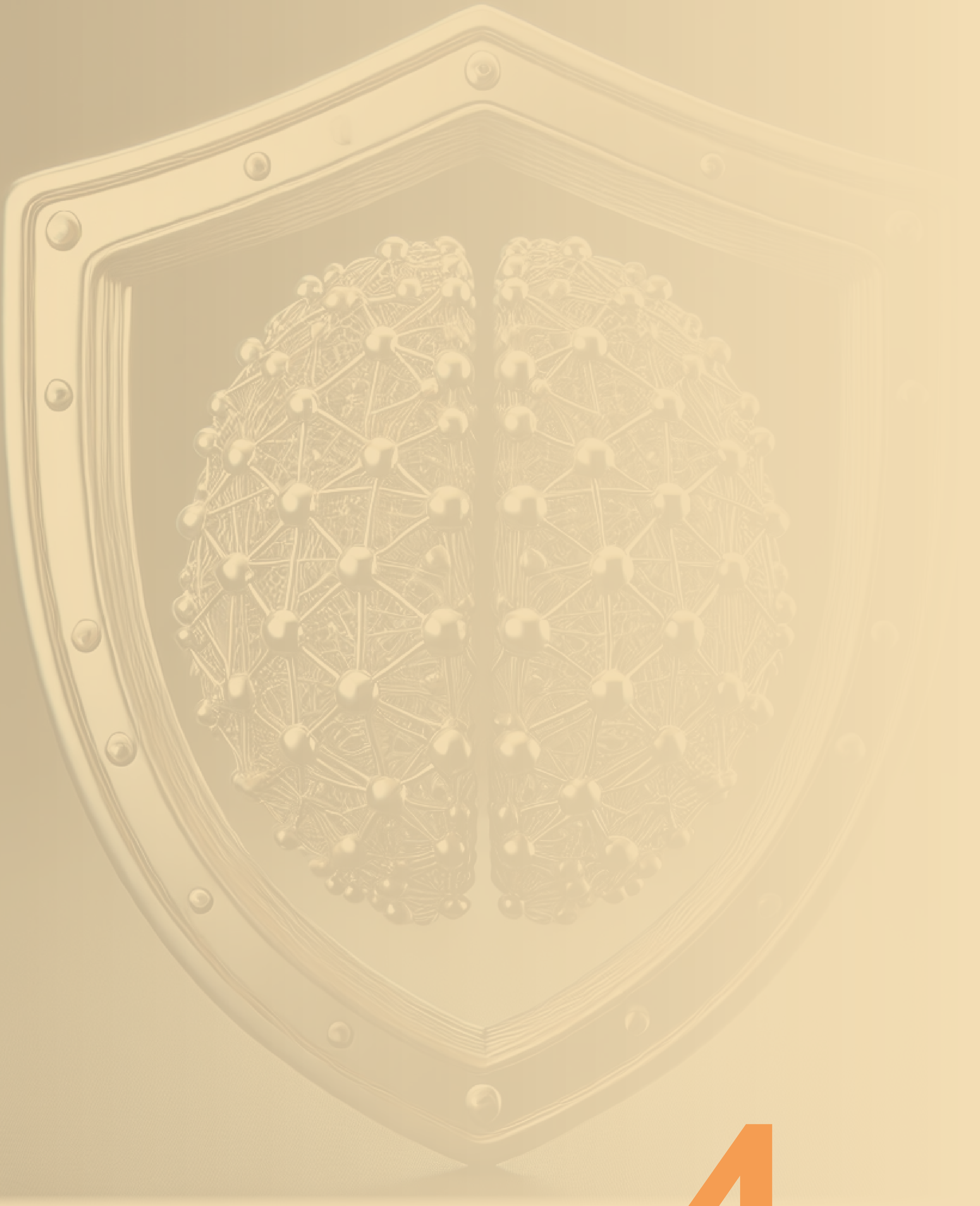
University of Bonn (2024), "Fake News Harms the Economy" https://www.uni-bonn.de/en/news/134-2024, 2 July.

U.S. Attorney's Office, Southern District of New York (2024), *Two RT Employees Indicted For Covertly Funding And Directing U.S. Company That Published Thousands Of Videos In Furtherance Of Russian Interests* ¡https://www.justice.gov/usao-sdny/pr/two-rt-employees-indicted-covertly-funding-and-directing-us-company-published, 4 September.

Wu, J. and Lam O. (2017), "The Evolution of China's Great Firewall: 21 Years of Censorship", *Global Voices Advox* https://advox.globalvoices.org/2017/08/30/the-evolution-of-chinas-great-firewall-21-years-of-censorship/

Yam, K. (2022), “Right-wing disinformation ramps up on WeChat ahead of midterms, report finds”, *NBC News*. https://www.nbcnews.com/news/amp/rcna50539, 3 October.

Zubor, Z. (2023), “A new form of fake news: clickbaiters and Russian propagandists mass-produce staged videos”, *Atlatszo* https://english.atlatszo.hu/2023/10/11/a-new-form-of-fake-news-clickbaiters-and-russian-propagandists-mass-produce-staged-videos/, 11 October.



CHAPTER 4

ENGINEERING DISINFORMATION: TECHNOLOGY INFRASTRUCTURE USED IN DIGITAL OPERATIONS DURING MANIPULATION CAMPAIGNS

Coordinators:

Fran Casino

Ministry of the Interior - Cybersecurity Coordination Office

Authors and contributors:

Marc Almeida Ros

David Arroyo Guardeño

Ivan Homoliak

Andrés Marín López

Rafael Mata Milla

Constantinos Patsakis

Oscar Walsch

INTRODUCTION

This chapter aims to convey two aspects of knowledge in three domains; although each of the three has its own characteristics, they generally appear together in the specific context of influence operations and manipulation campaigns. As set out in Chapter 8 of *Great Power Cyber Competition: Competing and Winning in the Information Environment* (Gioe and Smith, 2024), destabilizing elements in cyberspace can exploit conflict situations or violence to amplify their impact; accordingly, the links between cyberespionage, cybercrime and cyberwarfare are becoming increasingly apparent (Shapiro, 2023).

This chapter provides an analysis of the stages of the kill chain as defined by MITRE for advanced persistent threats (APT). The analysis is accompanied by a high-level assessment of the different spheres of action associated with advanced persistent manipulators (APM). Relationships will be drawn between the cyber domain of APTs and the informational domain of APMs. This will be done by outlining the network infrastructure components and Internet services used to craft and execute disinformation attacks against specific targets. The approach in this chapter is intended to apply the lessons learned in the field of cybersecurity against Foreign Information Manipulation and Interference (FIMI), examining how different technologies and procedures are used to design strategies, tactics and operations against specific targets, based on their vulnerability matrices. Those vulnerabilities are not only technological (Mirza and others, 2023), but also include all of the psychosocial aspects that make certain narratives more viable with respect to a society or a segment thereof.

Over the course of the chapter, the descriptions of the various tools, services and platforms will underscore the dual nature of the digital ecosystem. Tools that were initially designed to protect users' privacy when browsing the Internet have become key components of attackers' strategies for information campaigns, either when executing false flag attacks or simply to hamper subsequent cyberattribution efforts by targets. The success of such attribution efforts depends on the capacity to extract indicators or entities using system tracing, network monitoring or information from online public forums, but also from the deep web and the dark web. The connections between different actors, between actors and resources and between actors and intentions enable FIMI events to be understood and anticipated. This chapter will therefore provide context for the various tools, services and standards used to identify causal relations between the different components of the FIMI ecosystem and the use of network infrastructure components and techniques.

LINKS BETWEEN INFORMATION ATTACKS AND ADVANCED CYBERATTACK TECHNIQUES

A kill chain describes the different stages of an APT attack, as defined in the MITRE ATT&CK framework (Strom and others, 2020). APT attacks that are clearly and recognizably state-sponsored are usually accompanied by hybrid destabilization strategies. Therefore, the data exfiltration stages of the APT kill chain may feed into the design of the stages of selecting targets, resources and tools for deployment of influence and manipulation campaigns (Ahmad and others, 2019). It should be borne in mind that any data breach is a critical event, and especially those that affect personal data that can be used to profile citizens (Privacy International, 2021). The profiles generated are key to designing social engineering attacks and crafting viral content that exploits biases, preferences and psychosocial vulnerabilities of potential targets (Shapiro, 2023).

The following section provides a detailed analysis of the relationships between the different components and elements in the malware ecosystem that are used in APT and in influence campaigns in the area of FIMI. In doing so, reference will be made to the structure shown in Figure 1, explaining the critical importance of the data market and tools on the dark web (darknet market or dark web marketplace, DWM), access to and use of malware and packages of tools for phishing (Phishing as a Service, PhaaS) and social engineering attacks. The text will also look at the two sides of technologies such as artificial intelligence (malicious AI-generated content, MAIGC) and open-source intelligence (OSINT).

Reconnaissance	OSINT
Social engineering	MAIGC
Initial access	PhaaS
Lateral movement	MaaS
Encryption and exfiltration	RaaS
Collection and hijacking	DWM

Figure 1: Full structure of APTs

MALWARE AS A SERVICE (MaaS)

Instrumentalization of data or software by foreign agents is increasingly present in FIMI. In-depth analysis of incidents such as the instability in Georgia in 2019 caused by the Russian intelligence services (Greenberg, 2020) reveals complex attack strategies that combine malware with influence and data operations. **The overlap between cyberoperations (bits) and information operations (bytes) was very clear in the strategy and operations of the Russian attack against Georgia that began in 2006** (Beehner and others, 2018). What was particularly significant was the entire pattern of creation and distribution of malware from the StopGeorgia.ru domain.

"The overlap between cyberoperations (bits) and information operations (bytes) was very clear in the strategy and operations of the Russian attack against Georgia that began in 2006"

Malware is a critical threat to organizations and people around the world. In recent decades, malware has evolved from simple programs designed to cause minor disruption to sophisticated tools used in highly organized cybercrime operations. In this environment, MaaS has emerged as a lucrative business model that provides cybercriminals with access to complex tools for attacks without needing advanced technological skills (Patsakis and others, 2025). In the specific context of FIMI, services and providers in the malware production and distribution ecosystem may serve as proxies for designing, deploying and coordinating hybrid strategies to destabilize an adversary (Borghard and Lonergan, 2016). Here is where MaaS is becoming increasingly critical, especially in terms of the growing difficulty of attributing FIMI activity and of avoiding becoming a victim of false flag attacks (Skopik and Pahi, 2020).

MaaS is a business model whereby malware developers offer their tools and services to other criminals in exchange for payment, generally in cryptocurrency to maintain their anonymity (Casino and others, 2021). This model operates in a way that is similar to software as a service (SaaS) in the legitimate business world, with users able to subscribe or rent software without having to manage or develop it themselves. However, in the case of MaaS, the "customers" are criminals looking to perform cyberattacks who lack the technical skills to develop their own malware. By offering services such as malware kits, command and control infrastructure (C&C or C2), obfuscation and evasion or technical support, MaaS has made cybercrime more widely accessible and more lucrative for a range of different parties (Davidson, 2021), including those directly or indirectly participating in FIMI (Borghard and Lonergan, 2016).

To correctly outline the connection between hybrid information-cyberattack strategies in the context of FIMI, the frame of reference in this report will be based on initiatives such as the Defending Against Deception Common Data Model (DAD-CDM) Open Project[1] and those of OASIS Open[2]. By properly linking the different standards set out by OASIS Open, diagrams can be prepared of the relationships between actors and between actors and actions, enabling an analysis of causality or cyberattribution. The following section will describe the elements, actors and operation of MaaS.

[1] https://dad-cdm.org/

[2] https://www.oasis-open.org/

Elements of MaaS

The MaaS ecosystem includes a number of key elements that facilitate its functioning and success:

- **Malware kits:** These are software packages containing everything needed to perform an attack. Malware kits usually include malicious code, detailed usage instructions and, in some cases, additional tools such as exploit kits or packs and loaders that make deploying malware easier. These kits are designed to be simple to use, enabling even those with little technical experience to perform effective attacks (Meland and others, 2020).

- **Command and control infrastructure:** C&C infrastructure is vital for most malware techniques, and especially for those that call for continuous communication with the attacker. C&C servers enable attackers to remotely control infected machines, send commands, exfiltrate data and update malware in response to new security measures. MaaS suppliers often offer access to C&C servers as part of their packages, making management and control of malware campaigns easier (Huang and others, 2018).

- **Obfuscation and evasion services:** For malware to be effective, it must successfully evade detection by security measures. MaaS suppliers often include obfuscation services that alter malware code to hamper its detection by antivirus systems. In addition, they can implement evasion techniques such as using tailored packers or inserting code into legitimate processes to prevent detection (Patsakis and others, 2025).

- **Technical support and updates:** Under the MaaS model, malware developers not only sell software but also offer technical support to ensure that their customers can use the software effectively. The support may include assistance with configuring malware, fixing problems or updating software to bypass new security measures. As in the case of SaaS, MaaS suppliers seek to keep their customers happy, to guarantee a steady source of future income (Huang and others, 2018).

Key actors in the MaaS ecosystem

The MaaS ecosystem encompasses a number of different actors, each with a specific role in the cybercrime value chain. The key actors are:

- **Malware developers:** these developers are the most technically skilled actors in the MaaS ecosystem. They create and maintain the malware distributed on MaaS markets. Malware developers are generally highly qualified programmers with extensive knowledge of software vulnerabilities, techniques to evade or bypass security measures and strategies for cyberattacks. These individuals or groups frequently operate in secret, using dark web forums and other clandestine channels to sell their products (U.S. Department of Justice, 2022).

- **MaaS operators:** MaaS operators are responsible for managing the infrastructure that enables MaaS services. They distribute malware kits, maintain servers and provide support and update services, among others. MaaS operators act as intermediaries between malware developers and customers, ensuring that the developers are paid and that the customers receive the tools they need to perform their attacks (Europol, 2021).

- **Affiliates:** affiliates are a key group within the MaaS ecosystem. They often lack the technical skills needed to develop their own malware, but are willing to distribute malware provided by MaaS operators. In exchange, affiliates receive a commission tied to the income generated by the malware campaigns they run. This model is exemplified by ransomware-as-a-service (RaaS), which enables ransomware operators to maximize their reach and earnings without having to be directly involved in distributing malware (Europol, 2023a).

- **Customers/criminals:** MaaS customers are the actors who obtain malware services in order to perform their own criminal activities. They may be individuals or organized groups and their motives can range from making money, to personal vendettas, or even espionage. MaaS customers may lack advanced technical skills, but the services provided by MaaS operators enable them to launch effective attacks with minimal investment of time and resources (Cable, n.d.).

- **Intermediaries and resellers:** In addition to the actors directly involved in creating and distributing malware, intermediaries and resellers facilitate transactions between the different actors in the ecosystem. Intermediaries may offer services such as cryptocurrency exchange, access to compromised servers, or resale of malware kits to new customers (Europol, 2023b)

How MaaS markets operate

MaaS markets mirror many of the features of legitimate online businesses, enabling criminals to purchase malware services. These markets generally operate on the dark web, where MaaS suppliers publish detailed adverts of their products and services, including descriptions of the features of their malware, pricing and in some cases even reviews by other users.

- **Ransomware-as-a-service (RaaS):** RaaS is one of the most common models on MaaS markets. Under this model, ransomware operators provide the software needed to encrypt a target's data and demand a ransom to decrypt it again. Affiliates deploy the ransomware, often in phishing emails or by exploiting vulnerabilities of websites or applications. In exchange, affiliates receive a percentage of the ransom actually collected. This model has proven very lucrative, for RaaS operators and for affiliates (Meland and others, 2020).

- **Exploit kits and phishing-as-a-service (PaaS):** In addition to ransomware, MaaS markets also offer exploit kits and phishing services. Exploit kits are software packages that exploit vulnerabilities in popular software (such as browsers or operating systems) to install malware on targets' devices. Phishing-as-a-service offers templates for fraudulent emails and webpages that criminals can use to steal login details or other sensitive information. These services are popular because they enable criminals to perform attacks without having to develop their own tools (Meland and others, 2020).

- **Botnet services:** Botnets are networks of comprised devices that criminals can control remotely. On MaaS markets, it is possible to rent access to botnets to perform a variety of attacks, including distributed denial-of-service (DDoS) attacks, spam mailing lists or cryptocurrency mining. Botnet operators maintain and update the compromised networks, ensuring they are effective and difficult to detect for security systems. Such services enable criminals to scale up their operations quickly without needing their own infrastructure (Huang and others, 2018).

Cybersecurity challenges and threats

The spread of MaaS creates a number of challenges in terms of cybersecurity. Because such services are decentralized and anonymous, it is difficult to identify and prosecute those responsible. Moreover, the ease of access to sophisticated tools for performing cyberattacks has diminished the entry barriers for cybercrime, allowing more actors to participate in criminal activities, without needing advanced technological skills.

- **Swiftly evolving threats**: One of the key challenges posed by MaaS is the speed at which threats evolve. Malware developers and MaaS operators are constantly competing with security systems, updating and improving their products to avoid detection. This means that organizations must always be watchful and regularly update their systems to protect against new malware variants (Casino and others, 2022a).

- **Economic and social impact:** The cybercrime facilitated by MaaS has a devastating impact on the global economy. Not only are there direct costs of recovering from malware attacks, organizations also face damage to their reputations, loss of confidence among customer bases, and potential legal or regulatory penalties. In the social sphere, the attacks facilitated by MaaS may also jeopardize critical infrastructure, such as that for healthcare services, energy or transport, with potentially catastrophic repercussions (Morgan, 2022).

- **International collaboration and mitigation measures:** To address the threat posed by MaaS, it is vital to collaborate at the international level. Cybercriminals often operate from several territories, hampering pursuit and prosecution by national authorities. Law enforcement agencies must work together, sharing information and coordinating activities to dismantle these networks. Organizations must also take a proactive approach to cybersecurity, investing in cutting-edge detection and response technology and training employees on emerging threats (Europol, 2021; Casino and others, 2022b).

DISINFORMATION INFRASTRUCTURE AND CAMPAIGNS

Threat actors implementing disinformation campaigns need the support of technical structures and resources to fulfil their aims; in this respect, the range of tools, services and platforms that can separate the cause of a FIMI strategy from its effects is particularly important. This section will focus on technological resources that can be used to obfuscate FIMI activity, preventing actors and interests from being identified.

As has been explored in a number of studies (including Huang and others, 2018), cybercrime tools and services are seeing growing division of labour and specialization, in general, but also in the specific case of illicit activities to produce, instrumentalize and exploit fabricated or decontextualized content. In other words, over the past 10 years there has been a Fordist transformation of the cybercrime ecosystem and of cognitive warfare and reputational attacks.

> "Over the past 10 years there has been a Fordist transformation of the cybercrime ecosystem and of cognitive warfare and reputational attacks."

Structure and components

Examples of the structures and technical resources employed include:

- **Virtual private networks and residential proxies:** A virtual private network (VPN) enables users to browse the Internet without the exchanged information being intercepted. While VPNs do not guarantee anonymity, they can be used as an additional layer of security to protect the identity of a threat actor, making attribution more difficult. Efforts by national law enforcement agencies to investigate IP addresses used by VPN services are time-consuming and require considerable coordination, especially if the VPN services themselves do not cooperate and have policies of not storing records of users' or customers' activity. As will be highlighted later, here there is a two-faceted situation: protecting a user's privacy may hamper attribution work in investigations of illicit activities in cyberspace and specifically in the FIMI ecosystem. What is more, if the network infrastructure employed is distributed internationally, the work of investigators calls for coordination across different regulatory frameworks that are not necessarily compatible, thus hindering cooperation.

  In the case of proxy servers, a user connects to the service to avoid direct access to an online service or platform. The proxy server is an intermediary between a user and an end server, adding an extra layer between the two. There are various formats of proxy servers, but anonymous proxies and residential proxies are worthy of special attention. In the case of anonymous proxies, IP addresses of users are modified, so that the platform or service being accessed by the user cannot identify the original address. This can be used to hide attacks by cybercriminals or other actors in disinformation campaigns, but the level of protection depends on the server type. In the case of residential proxies, the servers are in specific locations and are not dependent on any data centres or service providers, meaning that courts face more difficulties in obtaining collaboration by the provider of a proxy service.

Like VPNs, residential proxies can enable access to information that is geoblocked. Similarly, use of such proxies by threat actors can be an attempt to misdirect investigations of the real origin of a threat, as they are located in third countries that may also have an interest in spreading disinformation. Residential proxies have been part of the arsenal employed by groups such as APT29, which was particularly active in Ukraine before the 2014 crisis and performed new phishing campaigns from late 2018 onwards. In the context of FIMI, the links between APT29 and diplomatic activities by Russia are particularly significant (Cunningham, 2020).

- ***SIM swap scams and SMS phishing:*** SIM swap scams (also known as simjacking or SIM swapping) have generally been linked to scams relating to finance, but they have taken on a new role in disinformation campaigns. In addition to providing full or partial access to a device or service, meaning that this technique can be used for cyberespionage or to access other items related to the source that may contain information of interest, it can also be used to take over legitimate media, such as reputable user accounts on social networks with high numbers of followers who are of interest to the actor undertaking the scam.

  This technique has other ramifications, as it enables disinformation to be spread and victims whose identities are stolen to be brought into disrepute. Like simjacking, phishing may be used to obtain access to a legitimate account, which can then be used to spread information to a larger audience. This technique also provides access to truthful information that can be manipulated to produce disinformation, as was the case for David Satter, whose email account was accessed illegally, enabling tampering with his emails in order to publish fake information relating to a supposed US-financed operation to destabilize Russia (Hulcoop and others, 2017).

  The SMS phishing ecosystem has also become particularly prominent more recently. The range of server hosting systems for phishing and social engineering campaigns give an idea of the level of sophistication of this activity (Nahapetyan and others, 2024), and of the set of challenges posed by supervision of service providers and platforms, as required by Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (known as the Digital Services Act). Compiling information on hosting services and on patterns of digital certificate issuance through analysis of Certificate Transparency framework logs, and identification and tracking of kits for performing phishing campaigns are all vital elements when developing strategies to contain FIMI.

- **Generative artificial intelligence and human spoofing:** Artificial intelligence (AI) can be used to generate disinformation either in text form or as multimedia. Large language models (LLM) can generate convincing, apparently genuine information on the issue that is targeted by disinformation campaigns. They also enable large volumes of disinformation to be rapidly generated, leading to information overload. AI can also be used to refine disinformation, in an attempt to make it more persuasive and of better quality, or to adapt it to the target audience. Although most language models are censured or prevent such conduct, their safeguards are easily bypassed using different techniques, including chain of thought (CoT), or models can be used that do not have censorship or safeguards (Barman and others, 2024).

In the case of image generation, while previously an image was generally needed that was then de-contextualized, now an image can be created from zero. This is of particular interest in the case of models such as Flux, which do not censure images of public figures and which produce generated images that are increasingly difficult to differentiate from real ones. Access to this technology is straightforward, as it requires no technical skills and the technical specifications required to run the software are not as demanding as might be expected. Human spoofing, which uses generative AI such as those described, makes it possible for disinformation actors to pass themselves off very convincingly as public figures, not only to distribute the content they create but also to mislead and perform social engineering of the public. One example of this was the fake video call between the Mayor of Madrid and supposedly his counterpart in Kyiv, which could be classed as somewhere between a joke and hybrid warfare (Twomey and others, 2023).

"Human spoofing, which uses generative AI such as those described, makes it possible for disinformation actors to pass themselves off very convincingly as public figures"

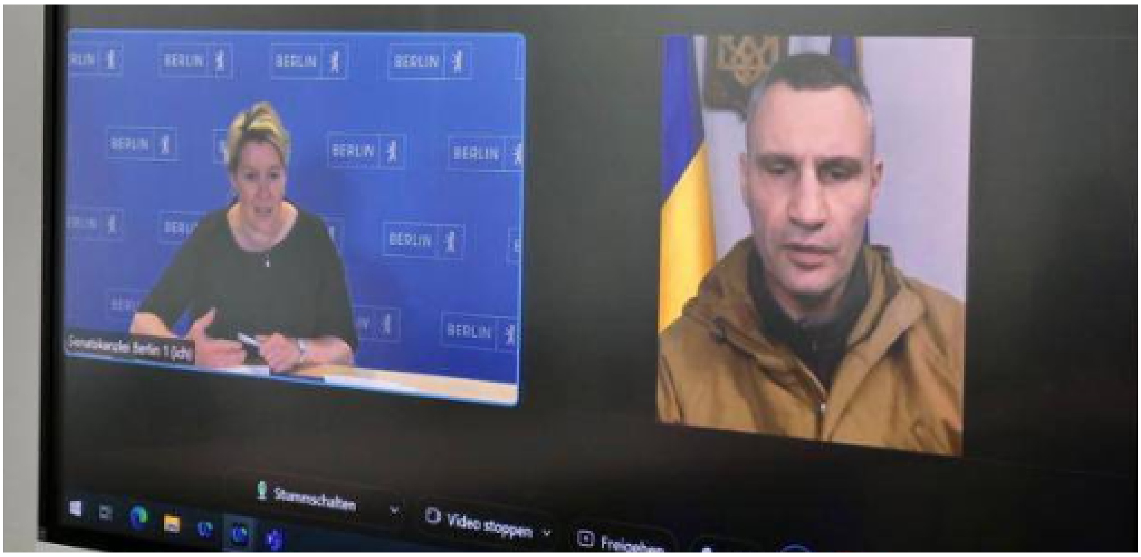


Figure 2. The Mayor of Berlin being manipulated through spoofing of the Mayor of Kyiv, Vitali Klitschko. Source: Fischer, 2022.

- **Social networks, influence and talent recruitment:** Combining social networks, multiplatform approaches and coordinated action. The increasing ease of access to channels for producing and distributing content has facilitated operations to influence decision-making. In terms of investigations, messaging services with end-to-end encryption pose a significant challenge, as they prevent direct interception of traffic and facilitate coordination between those producing manipulative information and those publishing it (Hoseini and others, 2024; Hanley and Durumeric, 2025). As regards the uses of social networks, platforms and even deep web forums, infrastructure is being deployed to train and recruit talent in the cybercrime sphere (Wang and others, 2023; Pandey, 2022).

Dual-use technology

Dual-use technology can be defined as that which can be used for both civilian and military purposes. In this case, we are using the term to refer to technology that has civilian uses but can also be used by threat actors to perform disinformation operations. Dual-use technology is exemplified by social networks. However, this section will focus on the infrastructure needed to perform disinformation operations.

- **Digital marketing.** Digital marketing has become an increasingly vital tool for businesses and organizations to promote their products and services. Strategies such as search engine optimization (SEO) and advertising on social networks enable brands to reach specific audiences efficiently and effectively. However, the same techniques and platforms that are used commercially can also be exploited to perform influence and disinformation operations. Threat actors may make use of data segmentation and analysis tools to identify and target vulnerable audiences, spreading fake or manipulated information to influence opinions, behaviour or political decisions (Di Domenico and others, 2021).

  For example, during elections, State actors and non-State actors have used disinformation campaigns on social networks to sow discord, polarize society or discredit candidates. By creating misleading content and using bots or fake profiles, they can amplify messages and make them seem more genuine or popular than they really are. Indeed, there are State-funded groups and groups offering services to undertake manipulation campaigns on social networks. Cases include troll farms and bot farms (Hughes and Waismel-Manor, 2021) and use of abandoned military infrastructure to link supporting activities for cybercrime and cyberwarfare (Caesar, 2020). In addition, microsegmentation techniques and recommendation systems (Deldjoo and others, 2023) enable specific messages to be tailored to individual groups, making the manipulation more effective (Ó Fathaigh and others, 2021).

- **Wikipedia.** The collaborative encyclopaedia Wikipedia is one of the most visited websites in the world, providing accessible information free of charge to millions of people. The fact that it can be edited by anyone is its greatest strength and its greatest weakness. In the context of disinformation and influence campaigns, this feature can be exploited by threat actors through dishonest and biased editing of its content, coordinated editing attacks, manipulation of sources and references, or dissemination of apparently genuine sources and references that in fact form part of a disinformation campaign.

  Although most misleading content on Wikipedia is detected swiftly and has a limited impact, a small number of articles survive for much longer and are viewed many times (Kumar, West and Leskovec, 2016). There are automatic means of classifying a given article as misleading, resulting in greater accuracy than the manual reviews by human moderators. According to the authors of the cited study, human readers tend to consider short articles to be misleading, while it is in fact long articles that are more likely to be deceptive, as reflected by the fact that the capacity to moderate malicious content is low without specialized automatic tools. Wikipedia is therefore a fertile ground for sowing disinformation, given that editing and access to it are both open and it receives an enormous volume of traffic.

- **Open source intelligence.** Open source intelligence (OSINT) has for many years been a valuable source of information, owing to its ease of access, the availability of information and the low costs compared to other sources. The proliferation of technology and widespread Internet access have transformed how information is compiled and analysed. OSINT has become a key tool for extracting relevant data from a sea of publicly available information. The ease with which such information can be obtained has led to it being actively used not only by intelligence services but also by organizations and individuals, giving them strategic advantages and improving decision-making in multiple areas.

  Although use of OSINT is prevalent and widely accepted, it is important to recognize the significance of disinformation and manipulation in this area. A threat actor may seek to cause information overload by generating artificial content that is inaccurate or slightly misleading, or may produce biased information that can be misinterpreted by enemies or competitors (Flamer, 2023).

- **Web archives.** Web archives, such as the Wayback Machine run by the Internet Archive or Archive.is, store webpages automatically or on demand, enabling any user to access information, even if it has been deleted or changed, or simply to visit an original site. These services play a crucial role in preserving digital history, facilitating academic research and access to information that would otherwise be lost.

  However, although the legitimate aims of such services are clear, threat actors have been found to use the technology for various purposes, such as spreading inaccurate information, retracted information or disinformation; accessing news items from media outlets whose values clash with their own, in order to reduce the advertising revenue of those outlets; evading censorship measures when spreading disinformation on social networks; and scraping social network posts and news items that may be deleted because of controversies (Zannettou and others, 2018; Acker and Chaiet, 2020).

- **Use of legitimate cloud computing services as an evasion strategy.** The use of legitimate services to perform cyberattacks has been frequently observed in deployments of botnets and C&C systems (Al Ielah and others, 2023). Given the overly centralized nature of some platforms, any instrumentalized use of their services to circumvent security filters and controls of institutions, organizations or businesses can be said to be very critical (Alcantara, 2024).

DISCUSSIONS, CHALLENGES AND COMPLICATIONS

This section summarizes the ideas from the preceding analysis, and centres on the implications of disinformation campaigns, examining future steps to take. The main points for discussion relate to the technological progress needed to mitigate disinformation threats.

Formulation of standards and procedures to identify actors, tools and third-party intermediaries in the context of FIMI. When attributing foreign interference campaigns and other FIMI activities, identifying links between States and actors in the MaaS ecosystem is a technological and methodological challenge. The prevalence of the proxies that are typical of tactical and military confrontations has been increased by cybernetic resources. The ever-greater sophistication and specialization of the services, products and platforms for creating and distributing fabricated content and malware has made the concept of a proxy—or rather cyberproxy—increasingly multi-faceted (Borghard and Lonergan, 2016). Analysis of the risks and threats linked to the different types of proxies in cyberspace calls for procedures to identify, annotate and distribute evidence and intelligence nationally and transnationally. In this respect, at the European level, it would be beneficial to incorporate technological solutions derived from theoretical frameworks for risk assessment and attribution of FIMI actions into the Information Sharing and Analysis Centre (ISAC) network.

Digital signatures and secure protocols for content checking. Disinformation campaigns may be effectively combated by adopting secure protocols and digital signatures to authenticate the origin and integrity of content. Technologies such as trusted execution environments (TEEs) and zero-knowledge proofs (e.g. Zero-Knowledge Succinct Non-interactive Arguments of Knowledge or zk-SNARKs) are emerging as viable alternatives for verifying the authenticity of information. These cryptographic technologies ensure that the original creators of digital content are correctly identified, reducing the potential for unhindered distribution of manipulated or fabricated content. Implementing such protocols in environments in which generative AI can produce disinformation will be crucial in the future.

> "Disinformation campaigns may be effectively combated by adopting secure protocols and digital signatures to authenticate the origin and integrity of content"

A well-known case study of combating disinformation using zk-SNARKs is protection of digital images. Cameras need a secure element to sign the pictures they take and the videos they record. This feature acts in a similar way to TEEs, but can be more accurately described as an anti-tamper signature system or secure element. Some companies have already contributed to a standard called C2PA Content Credentials, developed by the Coalition for Content Provenance and Authenticity (C2PA, 2024), which rather than focusing on secure hardware, centres around linking multimedia to trustworthy metadata, such as geolocation. Content Credentials enable users to strike a balance between privacy and authenticity, for example by including geolocation in an image and only disclosing selected information. Thus, any person with access to a high-resolution image, such as a 30 mega-pixel photo and its credentials, can demonstrate that an authenticated camera captured the image at a specific location. This technology can help combat disinformation, such as distribution of fake photos of conflict zones. Possible attack techniques, such as taking a photo of a printed image, remain independent vectors that must be addressed separately.

Preserving integrity when modifying content. News agencies and television networks often modify original photos and videos before publishing them. Changes such as cropping, resizing or greyscaling media result in the loss of the original link between the signed media and its metadata. This poses a substantial challenge in terms of preserving the integrity of content when modifying it. To address this problem, zk-SNARKs can be used to preserve the link between an original image and modified versions. A circuit that represents the modifications applied to the original media would permit the signature and link to be retained, even after modifications have been applied. A number of different authors have examined this approach (Datta and others, 2024), but one of the most significant challenges found was considerable computing overload encountered when generating zk-SNARK tests. The method calls for substantial amount of memory, up to 64 gigabytes (GB), to perform a single test, making it impractical for widespread use. However, a more recent article (Della Monica and others, 2024) optimized the method by taking a divide and conquer approach. The authors propose dividing an image into tiles and modifying the Content Credentials protocol to sign aggregated tiles using a Merkle tree (also known as a hash tree). This method enables zk-SNARKs tests to be performed for individual tiles, significantly reducing the computing load. This optimized approach enables zk-SNARK tests to be performed even on standard hardware, with as little as 4GB of RAM.

While the approaches to still images show promising results, video content poses a much greater computational challenge, as zk-SNARK tests are much slower and require more resources. Research is being performed to run the zk-SNARK tests in parallel, using graphics processing units (GPU), which has resulted in up to a fourfold improvement in speed. However, these efforts have not yet achieved the computational efficiency required for real-time or large-scale processing of videos.

Automatic detection of disinformation using AI and Big Data. LLMs and their ability to produce convincing fake information pose a challenge. Information overload is already rife, and the capacity of AI to produce large volumes of fake information is making the problem worse (Xu and others, 2023). Technological solutions are needed to address this overload (e.g. better algorithms for filtering and automated verification systems) accompanied by drives to educate the public to improve media literacy. In this regard, it is crucial to automate detection of disinformation, using AI systems that employ semantic correlation and natural language processing (NLP). Nevertheless, some hurdles remain in terms of the scalability and accuracy of such systems. Furthermore, maintaining and continuously updating databases with which to trace known sources of disinformation will be key to the effectiveness of such AI systems (Mansurova and others, 2024).

Experts in fact-checking news. While automated systems play an important part, the role of fact-checking experts in verifying the accuracy and validity of content should not be ignored. The roles of fact-checkers, journalists and experts in different fields should be strengthened, to counteract the growing influence of AI-generated disinformation. Integrating feedback from experts into AI systems to identify fake content could create a robust hybrid system (Mahmud and others, 2023). In addition, the concept of "expert" itself needs to be defined, to identify the right workers with the right skills and conduct, among other characteristics, in different information contexts. This represents a line of research in its own right.

Emerging technologies and protection of verified content, blockchain and immutable records: Correctly curating news through experts, efficiently annotating it and distributing it all call for protocols and procedures that ensure its safekeeping and integrity. Blockchain technology is another potential solution to combat disinformation by creating immutable digital records of content. This would enable information to be traced as it spreads on different platforms, thus ensuring that modifications or tampering of original content are visible, traceable and verifiable. This approach could be particularly effective for news platforms and social networks, where false information can spread quickly (Fraga-Lamas and Fernández-Caramés, 2020).

Multidisciplinary collaboration in the fight against disinformation. Modelling of cybersecurity threats may be useful for better profiling of attackers within the disinformation ecosystem, including their attack patterns, their preferred targets and their most frequently used techniques (Mirza and others, 2023). However, to effectively do so, a collaborative approach is needed, including multiple disciplines. Experts in cybersecurity, law enforcement, data analysis psychology and semantics must work together to create effective countermeasures. This multidisciplinary collaboration should also encompass lawmakers, ensuring that the legal framework keeps pace with technological advances (Casino and others, 2022b). The protocols designed to detect and combat disinformation should be based on legal standards, safeguarding privacy and security (Ramašauskaitė, 2023).

Challenges in cyberattribution. One of the most recurrent challenges in the fight against disinformation relates to cyberattribution. Identifying a source of disinformation, especially in the case of sponsored campaigns, calls for sophisticated tools and international cooperation. Although some progress has been made, particularly by employing AI and OSINT, the constantly mutating tactics of threat actors make attribution increasingly difficult. False flag operations, anonymized Internet infrastructure (such as VPNs and proxies) and encrypted communication channels hamper work to identify those responsible for disinformation campaigns. Future efforts should focus on improving cyberattribution frameworks, to hold those responsible accountable, at the international level (Maesschalck, 2024).

CONCLUSIONS

This chapter has explored the complex interactions between disinformation campaigns, technological progress and the resulting sociopolitical effects. Over the course of the chapter, we have seen how disinformation and sophisticated cybercampaigns often rely on organized infrastructure and platforms that use malware and AI technology. Descriptions of APM reflect the stages of APTs, whereby information wars exist alongside cyberattacks, and manipulated content is distributed that has the potential to destabilize society.

MaaS exemplifies the commercialization of cybercrime tools, enabling even those without technical skills to orchestrate disinformation campaigns. This process is reinforced using botnets, ransomware and PaaS models. In addition, although AI tools can be used to generate large volumes of fake or manipulated content, they also facilitate detection of such content. In short, this chapter has highlighted a number of key technologies and strategies that should be explored, such as using blockchain to ensure the integrity of content, more efficient use of zk-SNARK, the need for multidisciplinary collaboration and how to address the challenges of cyberattribution.

BIBLIOGRAPHY

Acker, A. and M. Chaiet (2020), “The weaponization of web archives: Data craft and COVID-19 publics”, *Harvard Kennedy School (HKS) Misinformation Review*, https://doi.org/10.37016/mr-2020-41, 28 September.

Ahmad, A., J. Webb, K. C. Desouza and J. Boorman (2019), “Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack”, *Computers & Security,* Volume 86, pp. 402– 418, https://doi.org/10.1016/j.cose.2019.07.001.

Alcantara, J. M. (2024), “Phishing with Cloudflare Workers: Transparent Phishing and HTML Smuggling”, https://www.netskope.com/blog/phishing-with-cloudflare-workers-transparent-phishing-and-html-smuggling, 23 May.

Al lelah, T., G. Theodorakopoulos, P. Reinecke, A. Javed and E. Anthi (2023), “Abuse of Cloud-Based and Public Legitimate Services as Command-And-Control (C&C) Infrastructure: A Systematic Literature Review”, *Journal of Cybersecurity and Privacy, 3 (3)*, pp. 558–590, https://doi.org/10.3390/jcp3030027.

Barman, D., Z. Guo and O. Conlan (2024), “The Dark Side of Language Models: Exploring the Potential of LLMs in Multimedia Disinformation Generation and Dissemination”, *Machine Learning with Applications, 16*, *100545,* https://doi.org/10.1016/j.mlwa.2024.100545.

Beehner, L., L. Collins, S. Ferenzi, R. Person and A. Brantly (2018), “Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia. A Contemporary Battlefield Assessment by the Modern War Institute”, *Modern War Institute at West Point*, https://mwi.westpoint.edu/wp-content/uploads/2018/03/Analyzing-the-Russian-Way-of-War.pdf.

Borghard, E. D. and S. W. Lonergan (2016), “Can States Calculate the Risks of Using Cyber Proxies?”, *Orbis*, 60 (3), pp. 395-416, https://doi.org/10.1016/j.orbis.2016.05.009.

C2PA (Coalition for Content Provenance and Authenticity) (2024), “Content Credentials: C2PA Technical Specification (2.0)” https://c2pa.org/specifications/specifications/2.0/specs/C2PA_Specification.html.

Cable, J. (n.d.). “Ransomwhere: A Crowdsourced Ransomware Payment Dataset (1.1.0)”, Zenodo. https://doi.org/10.5281/zenodo.6512122.

Caesar, E. (2020), “The Cold War Bunker that Became Home to a Dark-Web Empire”, *The New Yorker,* https://www.newyorker.com/magazine/2020/08/03/the-cold-war-bunker-that-became-home-to-a-dark-web-empire, 27 July.

Casino, F., T. K. Dasaklis, G. P. Spathoulas, M. Anagnostopoulos, A. Ghosal, I. Borocz, A. Solanas, M. Conti and C. Patsakis (2022a), “Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews”, *IEEE Access,* 10, 25464-25493, https://doi.org/10.1109/ACCESS.2022.3154059.

Casino, F., N. Lykousas, V. Katos and C. Patsakis (2021), “Unearthing malicious campaigns and actors from the blockchain DNS ecosystem”, *Computer Communications, 179*, pp. 217–230, https://doi.org/10.1016/j.comcom.2021.08.023.

Casino, F., C. Pina, P. López-Aguilar, E. Batista, A. Solanas and C. Patsakis (2022b), “SoK: Cross-border criminal investigations and digital evidence”, *Journal of Cybersecurity, 8 (1)*. https://doi.org/10.1093/cybsec/tyac014.

Cunningham, C. (2020), “A Russian Federation Information Warfare Primer”, *The Henry M. Jackson School of International Studies, (University of Washington),* https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/, 12 November.

Datta, T., B. Chen and D. Boneh (2024), “VerITAS: Verifying Image Transformations at Scale”, *Cryptology ePrint Archive*, https://eprint.iacr.org/2024/1066.

Davidson, R. (2021), “The fight against malware as a service”, *Network Security, 2021 (8)*, 7–11. https://doi.org/10.1016/S1353-4858(21)00088-X.

Deldjoo, Y., D. Jannach, A. Bellogín, A. Difonzo and D. Zanzonelli (2023), “Fairness in recommender systems: research landscape and future directions”, *User Modeling and User-Adapted Interaction, 34 (1)*, 59–108. https://doi.org/10.48550/arXiv.2205.11127.

Della Monica, P., I. Visconti, A. Vitaletti and M. Zecchini (2024). “Trust Nobody: Privacy-Preserving Proofs for Edited Photos with Your Laptop”, *Cryptology ePrint Archive,* https://eprint.iacr.org/2024/1074.

Di Domenico, G, J. Sit, A. Ishizaka and D. Nunan (2021). “Fake news, social media and marketing: A systematic review”, *Journal of Business Research*, 124, pp. 329–341. https://doi.org/10.1016/j.jbusres.2020.11.037.

Europol (European Union Agency for Law Enforcement Cooperation) (2021), “DarkMarket: world’s largest illegal dark web marketplace taken down”, https://www.europol.europa.eu/media-press/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down, 12 January.

(2023a), “288 dark web vendors arrested in major marketplace seizure”, https://www.europol.europa.eu/media-press/newsroom/news/288-dark-web-vendors-arrested-in-major-marketplace-seizure, 2 May.

2023b), “Takedown of notorious hacker marketplace selling your identity to criminals”, https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals, 5 April.

Fischer, D (2022), “Fake Video Calls Aim to Harm Ukraine Refugees”, *Human Rights Watch*, https://www.hrw.org/news/2022/07/01/fake-video-calls-aim-harm-ukraine-refugees, 1 July.

Flamer, N. (2023), “‘The enemy teaches us how to operate’: Palestinian Hamas use of open source intelligence (OSINT) in its intelligence warfare against Israel (1987-2012)”, *Intelligence and National Security, 38 (7)*, 1171–1188. https://dx.doi.org/10.1080/02684527.2023.2212556

Fraga-Lamas, P. and T. Fernández-Caramés (2020), "Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality". *IT Professional, 22 (2)*, pp. 53–59, https://doi.org/10.1109/MITP.2020.2977589.

Morgan, S. (2022), "Cybercrime to cost the world 8 trillion annually in 2023", *Cybercrime Magazine*, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/, 17 October.

Gioe, D. V. and M. W. Smith (eds.) (2024), *Great Power Cyber Competition: Competing and Winning in the Information Environment*, Routledge.

Greenberg, A. (2020); The US Blames Russia's GRU for Sweeping Cyberattacks in Georgia, *Wired,* https://www.wired.com/story/us-blames-russia-gru-sweeping-cyberattacks-georgia/, 20 February.

Hanley, H. W. A. and Z. Durumeric (2025), "Partial Mobilization: Tracking Multilingual Information Flows amongst Russian Media Outlets and Telegram", https://doi.org/10.48550/arXiv.2301.10856

Hoseini, M., P. de Freitas Melo, F. Benevenuto, A. Feldmann and S. Zannettou (2024), "Characterizing Information Propagation in Fringe Communities on Telegram", *Proceedings of the Eighteenth International AAAI Conference on Web and Social Media, 18*, 583–595. https://doi.org/10.1609/icwsm.v18i1.31336.

Huang, K., M. Siegel and S. Madnick (2018), "Systematically Understanding the Cyber Attack Business: A Survey", *ACM Computing Surveys (CSUR),* 51(4), pp. 1–36, https://doi.org/10.1145/3199674.

Hughes, H. C. and I. Waismel-Manor (2021), "The Macedonian Fake News Industry and the 2016 US Election", *PS: Political Science & Politics, 54 (1)*, pp. 19-23. https://doi.org/10.1017/S1049096520000992.

Hulcoop, A., J. Scott-Railton, P. Tanchak, M. Brooks, and R. Deibert (2017), *Tainted Leaks: Disinformation and Phishing with a Russian Nexus, Research Report #92*, The Citizen Lab (University of Toronto), https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/, 25 May.

Kumar, S., R. West and J. Leskovec (2016), "Disinformation on the Web: Impact, Characteristics, and Detection of Wikipedia Hoaxes", *Proceedings of the 25th International Conference on World Wide Web,* International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, 591-602. https://doi.org/10.1145/2872427.2883085

Maesschalck, S. (2024), "Gentlemen, you can't fight in here. Or can you?: How cyberspace operations impact international security", *World Affairs, 187(1)*, pp. 24-36. https://doi.org/10.1002/waf2.12004.

Mahmud, M. A. I., A. A. T. Talukder, A. Sultana, K. I. A. Bhuiyan, M. S. Rahman, T.H. Pranto y R. M. Rahman (2023), "Toward News Authenticity: Synthesizing Natural Language Processing and Human Expert Opinion to Evaluate News", *IEEE Access,* 11, pp. 11405–11421. https://doi.org/10.1109/ACCESS.2023.3241483

Mansurova, A., A. Mansurova and A. Nugumanova (2024), “QA-RAG: Exploring LLM Reliance on External Knowledge”, *Big Data and Cognitive Computing, 8(9)*, 115, https://doi.org/10.3390/bdcc8090115

Meland, P. H., Y. F. F. Bayoumy and G. Sindre (2020), “The Ransomware-as-a-Service economy within the darknet”, *Computers & Security,* 92, 101762, https://doi.org/10.1016/j.cose.2020.101762

Mirza, S., L. Begum, L. Niu, S. Pardo, A. Abouzied, P. Papotti and C. Pöpper (2023), “Tactics, Threats & Targets: Modeling Disinformation and its Mitigation”, *Network And Distributed System Security (NDSS) Symposium*. https://doi.org/10.14722/ndss.2023.23657u.

Nahapetyan, A., S. Prasad, K. Childs, A. Oest, Y. Ladwig, A. Kapravelos and B. Reaves (2024), “On SMS Phishing Tactics and Infrastructure”, *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 1-16. https://doi.org/10.1109/SP54263.2024.00169.

Ó Fathaigh, R., T. Dobber, F. Zuiderveen Borgesius and J. Shires (2021), “Microtargeted propaganda by foreign actors: An interdisciplinary exploration”, *Maastricht Journal of European and Comparative Law*, 28 (6), pp. 856–877, https://doi.org/10.1177/1023263X211042471.

Pandey, R. (2022), “Exploring HackTown: A College for Cybercriminals”, Information Systems Audit and Control Association, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/exploring-hacktown-a-college-for-cybercriminals, 9 March.

Patsakis, C., D. Arroyo and F. Casino (2025). “The Malware as a Service ecosystem”, in Gritzalis, D., K-K. R. Choo and C. Patsakis (eds.), *Malware: Handbook of Prevention and Detection. Advances in Information Security 91*, Springer, https://doi.org/10.1007/978-3-031-66245-4_16.

Patsakis, C., F. Casino and N. Lykousas (2024), “Assessing LLMs in malicious code deobfuscation of real-world malware campaigns”, *Expert Systems with Applications, 256 (6)*, 124912, http://dx.doi.org/10.1016/j.eswa.2024.124912.

Ramašauskaitė, O. (2023), “The Role of Collaborative Networks in Combating Digital Disinformation” in the proceedings of the “Regional Development - Digital Economy” International Conference on Economics, Scientific-Research Institute of Economic Studies (Azerbaijan State University of Economics), pp. 432-437. https://gs.elaba.lt/object/elaba:184652082/.

Shapiro, S. J. (2023). *Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks*. Farrar, Straus and Giroux.

Skopik, F. and T. Pahi (2020), “Under false flag: using technical artifacts for cyber attack attribution”. *Cybersecurity, 3*, 8. https://doi.org/10.1186/s42400-020-00048-4Strom, B. E., A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington and C. B. Thomas (2020), *MITRE ATT&CK®: Design and Philosophy*, The MITRE Corporation, https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf.

Twomey, J., D. Ching, M. P. Aylett, M. Quayle, C. Linehan and G. Murphy (2023), “Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine”, *PLOS ONE, 18 (10)*, e0291668. https://doi.org/10.1371/journal.pone.0291668

Privacy International (2021), “The UN report on disinformation: a role for privacy”, https://privacyinternational.org/news-analysis/4515/un-report-disinformation-role-privacy, 17 May.

U.S. Department of Justice (2022), “Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace”, https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace, 5 April.

Wang, Y., S. Roscoe, B. Arief, L. Connolly, H. Borrion and S. Kaddoura (2023), “The Social and Technological Incentives for Cybercriminals to Engage in Ransomware Activities” in B. Arief, A. Monreale, M. Sirivianos and S. Li (eds.), *Security and Privacy in Social Networks and Big Data, SocialSec 2023, Lecture Notes in Computer Science*, vol 14097, Springer, Singapore, https://doi.org/10.1007/978-981-99-5177-2_9.

Xu, D., S. Fan and M. Kankanhalli (2023), “Combating misinformation in the era of generative AI models” in *Proceedings of the 31st ACM International Conference on Multimedia (MM ‘23)*, Association for Computing Machinery, New York, pp. 9291–9298. https://doi.org/10.1145/3581783.3612704.

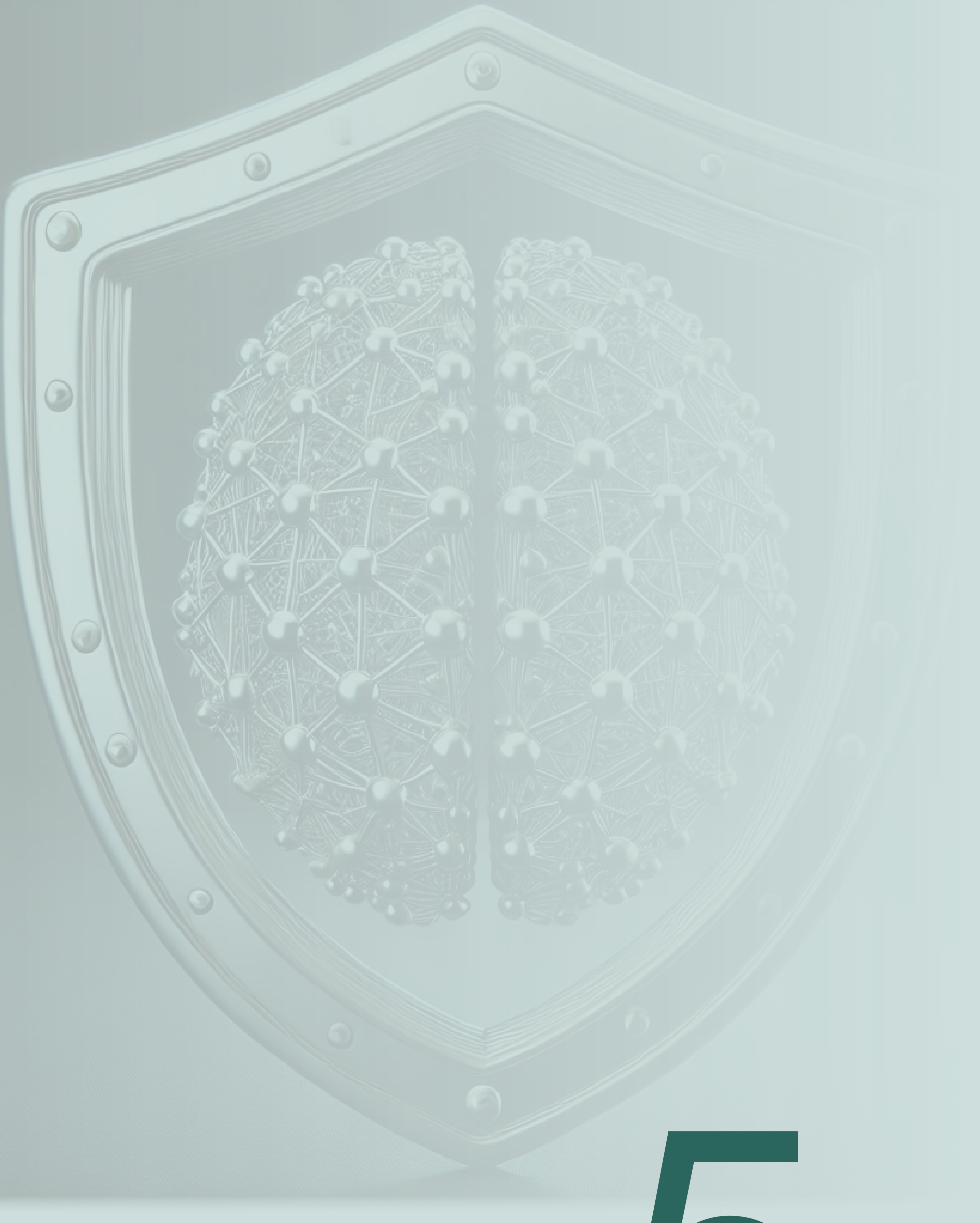
Zannettou, S., J. Blackburn, E. De Cristofaro, M. Sirivianos and G. Stringhini (2018), “Understanding Web Archiving Services and Their (Mis)Use on Social Media”, *Proceedings of the International AAAI Conference on Web and Social Media*, 12 (1), https://doi.org/10.1609/icwsm.v12i1.15018, 15 June.

U.S. Department of Justice. (2022). *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace*. https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

Wang, Y., Roscoe, S., Arief, B., Connolly, L., Borrion, H., y Kaddoura, S. (2023). The Social and Technological Incentives for Cybercriminals to Engage in Ransomware Activities. En Arief, B., Monreale, A., Sirivianos, M., Li, S. (Eds.), *Security and Privacy in Social Networks and Big Data. SocialSec 2023. Lecture Notes in Computer Science*, 14097. Springer, Singapore. https://doi.org/10.1007/978-981-99-5177-2_9

Xu, D., Fan, S., y Kankanhalli, M. (2023). Combating misinformation in the era of generative AI models. En Proceedings of the 31st acm international conference on multimedia. *Association for Computing Machinery,* pp. 9291-9298. https://doi.org/10.1145/3581783.3612704

Zannettou, S., Blackburn, J., De Cristofaro, E., Sirivianos, M., y Stringhini, G. (2018, junio). Understanding Web Archiving Services and Their (Mis)Use on Social Media. *Proceedings of the International AAAI Conference on Web and Social Media, 12 (1)*. https://doi.org/10.1609/icwsm.v12i1.15018



CHAPTER 5

DISINFORMATION CAMPAIGNS AND INCITEMENT OF HATE SPEECH

Coordinators:

Mario Hernández Ramos

Miguel Camacho Collados

Departamento de Seguridad Nacional

Authors and contributors:

Rubén Arcos Martín

Jesús Díaz Carazo

Carlos Edmundo Arcila

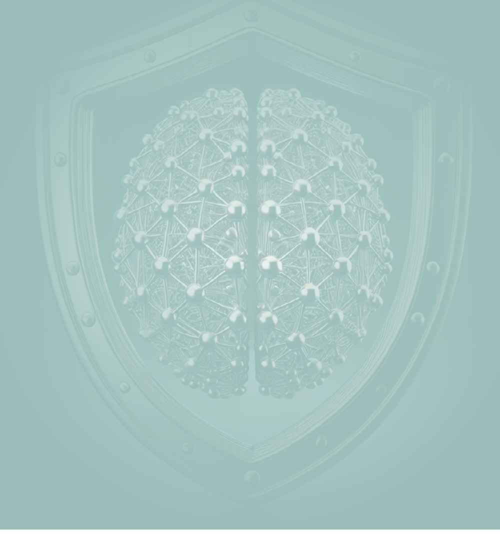
Carmen Girón Tomás

Beatriz Marín Garcia

María Teresa Martín Valdivia

Hate Crimes and Discrimination Unit of the Office of the Public Prosecutor-General

Cybercrime Unit of the Office of the Public Prosecutor-General



INTRODUCTION

The risk posed by disinformation campaigns to fuel and incite hate speech against specific groups within democratic countries—especially campaigns by hostile State actors to create rifts in societies—has already been examined by the European Parliament (Szakács and Bognár, 2021), the European External Action Service (EEAS Stratcom Division, 2023) and the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (Hoogensen Gjørv and Jalonen, 2023). Campaigns of this type are also deployed in third countries (primarily in Africa and Eastern Europe) as a means of attacking the West and the liberal democratic model, putting certain groups in those countries at risk.

There is also growing concern over the power of disinformation to drive violent radicalization, particularly when it takes the form of conspiracy theories that portray specific groups as threats (RAN, 2020).

Therefore, on 29 February 2024, the Forum against Disinformation Campaigns Affecting National Security decided to establish a working group. The main purpose of the working group is to examine the threat that disinformation campaigns can pose in terms of inciting hate speech, focusing on the case of Spain, and to discuss instruments and initiatives that could curtail their impact on society. The working group is also intended to raise awareness and foster insight into these threats among the different stakeholders in civil society and public authorities who are involved in protecting the groups that may be targeted by disinformation campaigns.

It was decided that the working group would be coordinated by Mario Hernández Ramos and Miguel Camacho Collados, and in the case of the public authorities by the Department of National Security. The working group comprises the persons listed at the beginning of this chapter.

IMPLEMENTATION OF THE INITIATIVE

To better understand the threat posed and the existing framework for countering it, and to raise awareness of the problem within communities linked to the fight against disinformation campaigns and against hate speech, a decision was made to hold a seminar with experts on the issue.

The seminar took place on 18 September 2024 in the buildings of the Faculty of Law of Complutense University of Madrid, with the support of the Institute of Parliamentary Law as part of the research project "Strengthening democracy and the rule of law using artificial intelligence". The event included four round tables, to address different aspects of the threat and the available tools to mitigate its effects.

The panellists for the first roundtable, which centred on better understanding of the threat, the techniques employed and how they relate to modern-day disinformation campaigns and hate speech, were Beatriz Marín, of the European External Action Service; Ruben Arcos Martín, Senior Lecturer at Rey Juan Carlos University; Alicia Moreno Delgado, Lecturer at La Rioja International University; Raquel Godos, from EFE Verifica. The round table was moderated by Alejandro González, from the Department of National Security.

The second roundtable focused on examining the regulatory and legal tools that exist in Spain to combat such threats and the challenges and opportunities of new instruments such as the EU Digital Services Act (DSA). The panellists were Miguel Ángel Aguilar, Senior Public Prosecutor and Coordinator of the Hate Speech and Discrimination Unit of the Office of the Public Prosecutor-General; Karoline Fernández de la Hoz Zeitler, Director of the Spanish Racism and Xenophobia Observatory of the Ministry of Inclusion, Social Security and Migration; Carlos Aguilar Paredes, from the National Commission on Markets and Competition; and Alfonso Peralta Gutiérrez, Trial Judge and Investigating Judge. The round table was moderated by Rafael Bustos Gisbert, Professor of Constitutional Law at Complutense University of Madrid.

The third roundtable addressed the opportunities offered by technology to detect threats and combat them, in the field of communication. The panellists were Emilio Delgado López Cózar, Professor from the University of Granada; David Blanco Herrero, post-doctoral researcher at the University of Amsterdam (Netherlands); Gavin Abercrombie, Assistant Professor at Heriot-Watt University (United Kingdom); and Flor Miriam Plaza del Arco, researcher at Bocconi University (Italy). The round table was moderated by Maite Martín Valdivia, Professor of the University of Jaén and Carlos Arcila Calderón, tenured lecturer at the University of Salamanca.

The fourth and final round table discussed media literacy and the role of the third sector, bringing together experts on the issue such as Manuel Gértrudix Barrio, Professor from Rey Juan Carlos University; Alberto Izquierdo Montero, Assistant Professor at the National University for Distance Education (UNED); Pablo Hernández Escayola, Academic Research Coordinator at Maldita.es; Natalia Sancha, from the European External Action Service; and Marisa Gómez, Director of the NGO platform Plataforma de ONG de Acción Social. The round table was moderated by Carmen Girón Tomás, doctoral student in Law and Social Sciences at UNED.

The seminar was attended by more than 70 people, including academics, experts from civil society organizations and think tanks, and representatives of public authorities.

CONCLUSIONS

Conceptualisation of the threat

In the context of national security, disinformation campaigns are currently understood to be patterns of coordinated and intentionally manipulative behaviour that aim to undermine principles, values and democratic processes. Their manipulative nature is reflected in how messages are crafted (e.g. using deepfakes), the sources used (e.g. spoofing media outlets or official accounts) and in how messages are distributed (e.g. using automated accounts or bots).

The actors behind these disinformation campaigns driven by geopolitical aims often exploit vulnerabilities in society, be they social, economic, political or historical. In recent years, there has been increasing use of identities as a vector of attack, including those linked to gender, sexual orientation, race, ethnicity and religion.

The hostile actors behind campaigns of this type frequently seek to sow social discord and erode social cohesion, as well as attacking political or social leaders whose standpoints conflict with their interests. Campaigns may also aim to discourage a particular group in society from participating in public life and in political processes, thus weakening the democratic system. Such strategies should be categorized as coercive influence activities (Alonso-Villota and Arcos, 2024).

The strategies employed in disinformation campaigns that target identities include: accusing a person of having a particular identity, attempting to alter public perception of an identity, inciting online harassment or even encouraging offline harassment or hate crimes.

To date, in Spain, academic research has found that online hate speech is predominantly racist in nature. On the same point, analysis by fact-checkers has also determined that the falsehoods that accompany racist or xenophobic narratives constitute the most frequent form of disinformation in the Spanish ecosystem. For example, 20% of disinformation debunked by fact-checkers during the European Parliament elections in 2024 aimed to link crime levels with immigration.

While not all disinformation concerning identities can be said to be hate speech, one of the challenges that must be addressed is determining the extent to which disinformation campaigns may incite hate, discrimination or even violence towards the targeted groups in society. This kind of disinformation campaign is usually long-running, producing a constant flow of events and narratives that must be analysed together to assess the risk of radicalization. Another important factor that must be analysed is the identity of the actors that systematically run disinformation campaigns.

A comprehensive approach to this threat is required, involving all of society, educating the public and building relevant skills. Consideration should also be given to anticipatory analysis of future scenarios or situations that could be exploited by disinformation campaigns. Such analysis would enable preventive responses to be deployed, such as prebunking, and warnings for media outlets and fact-checkers.

Lastly, there is a need for better safeguarding of civil society actors who work to expose and raise awareness of this threat, as in recent years they have been exposed to harassment, lawfare and even threats from State actors behind these campaigns.

Legal and regulatory framework

The defining characteristics of Spain's democracy and its legal system—primarily the direct applicability of the Constitution and certain fundamental rights—shape the possible judicial and administrative responses to hate speech. Spain is not a defensive democracy; this means that freedom of expression cannot be guaranteed through censorship, and although as a freedom it is not limitless, it does take precedence, even over other fundamental rights. Regulations, proportional measures and carefully considered decisions are required to ensure that all fundamental rights may be enjoyed. It follows that no public authority may therefore elevate itself to the position of "custodian of the truth". Freedom of expression is a pillar of any democratic society. Authorities or courts must therefore act with utmost caution when deciding whether to order removal of content, ensuring their decisions are based on legal and institutional frameworks that respect constitutional values and principles.

In Spain, a number of different laws and protocols exist to combat online hate speech, in hard law and soft law, enabling a variety of different actions, ranging from regulation of platforms and media outlets to administrative or criminal penalties.

Key pieces of legislation include the Digital Services Act (DSA) (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC), Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, the Council of Europe European Commission against Racism and Intolerance (ECRI) General Policy Recommendation No. 15 on Combating Hate Speech adopted on 8 December 2015, Council of Europe Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech (adopted by the Committee of Ministers on 20 May 2022) and the Protocol to Combat Illegal Hate Speech Online (signed by the executive, the judiciary and the Public Prosecution Service), and all other applicable elements of the national legal system, such as the Criminal Code.

How these tools are employed depends on the form of hate speech: firstly, that which can be prosecuted under criminal law; secondly, that which cannot be prosecuted under criminal law, but can be addressed under civil law or administrative law; and thirdly, offensive messages that do not merit a legal response, but which do call for a counternarratives.

Therefore, a deliberate lie or unintentional lie—i.e. failing to be truthful—may not necessarily result in criminal liability. Following on from this, since one of the guiding principles of criminal law is that of minimum intervention, any form of criminal liability must first be ruled out, without prejudice to other forms of responsibility, in cases of involuntary dissemination of false or skewed content.

For disinformation to be potentially criminally prosecutable, it must meet four criteria: it must be untruthful; it must be deliberately disseminated (with intent to discriminate); it must be malicious; and it must aim to influence or manipulate public opinion.

The possible legal response to such conduct is imprecisely defined in the Spanish Criminal Code for the different criminal conducts set out in the various sections of its Article 510. However, consideration is being given to opening a debate—for some exceptional cases and in terms of policy on crime—on this delicate subject, in terms of the need to prosecute certain conduct in which the perpetrator manifestly and wilfully disregards the truth by publicly disseminating false or deliberately manipulated content, the author of which expected or could reasonably expect the content to produce hateful, hostile, violent, discriminatory, humiliating or denigratory public reactions to certain persons or groups, with discriminatory intent.

This is the case because under the current provisions of Spain's Criminal Code, it is somewhat challenging to identify how hoaxes and fake news correspond to the crimes defined in Article 510 thereof.

An analysis of the conduct described in paragraphs 1.A) and 2.A) of Article 510 of the Criminal Code suggests that dissemination of hoaxes may correspond more closely to the definition of defamation of the group or groups targeted by a hoax in the latter paragraph. Nonetheless, the lack of a specific provision in Article 510 for such conduct hinders its categorization, and leaves considerable room for interpretation.

There is no case law regarding disinformation in the context of hate crimes. The only two cases that have gone to court to date ended in guilty pleas.

If the facts are not considered to constitute a crime, they may nonetheless constitute a punishable offence under administrative law, calling for a brief administrative procedure to be performed to ensure the conduct does not go unpunished. Effective application of the legal framework for penalties under administrative law (Comprehensive Act (Act 15/2022 of 12 July) on Equal Treatment and Non-Discrimination and Act 4/2023, of 28 February, for the real and effective equality of trans persons and to guarantee the rights of LGBTI people) calls for rapid action to establish efficient coordination mechanisms that ensure swift and efficient administrative responses that reflect the same criteria throughout Spain, as responsibility for applying penalties is divided among to the different Autonomous Communities; new legislative solutions are also needed to prosecute actions on the Internet, including on social networks, because the geographical location of the action often cannot be determined; accordingly, an administrative authority is required that is not tied to a regional office in an Autonomous Community.

Frequently, it is necessary to identify the user of a social network account from which certain actions are perpetrated in order to determine who is responsible. Such identification is not limited to investigation of serious crime, as the user data do not affect the fundamental right to confidentiality of communications and they are obtained in order to facilitate and expedite investigations; consequently, Article 588 ter m) of the Criminal Procedure Act allows the data to be obtained directly by the Public Prosecution Service or the Judicial Police in any form of investigation and without the need for a court order. This provision removes the impediments that were previously invoked by communications operators when requested to disclose such data, based on the argument that the data was stored together with the data on traffic they are obligated to store pursuant to Act 25/2007, on retention of data relating to electronic communications and publicly available communications networks—which transposes Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, which was subsequently annulled by the Court of Justice of the European Union in its ruling of 8 April 2014. Act 25/2007 limits access to (traffic) data retained by communications operators to investigation, identification and trial of serious crimes, and a court order is required to obtain access.

As regards the administrative sphere, it is important not to forget the possibilities offered by Article 10 of the DSA, whereby the relevant national judicial or administrative authorities, on the basis of the applicable Union law or national law in compliance with Union law, may issue information requests to providers of intermediary services, so that they may provide information on the recipient(s) of a service, in the context of which hate speech has been published. Given its importance, the key challenge in this area is streamlining and developing the implementing internal regulations that enable these provisions to be applied. It is also important to take into account the powers of the Spanish Data Protection Agency (AEPD) in the context of the investigations that fall within its remit (Article 51 of Organic Law 3/2018, of 5 December, on personal data protection and guarantees of digital rights).

Another question is identification of the parties responsible for the specific posts that constitute hate speech on a certain social network, pursuant to the existing procedures for punishing hate speech (Act 15/2022 and Act 4/2023, among others), which still poses some challenges. On this point, a court order is required to obtain the IP addresses and other connection data relating to posts, because they are traffic data, as stipulated in Article 588 ter j) of the Criminal Procedure Act. In addition, in accordance with the criteria of Article 588 bis a) of the Act, such data must only be accessed in cases in which the access is considered proportional.

The importance of the DSA, which focuses on very large online platforms (VLOPs), is unquestionable, but for it to be fully effective in Spain, the National Commission for Markets and Competition (CNMC) must be accorded relevant powers at the national level. Based on the text of the DSA, it can be said that the concept of disinformation has three key components: firstly, the untruthfulness of the content; secondly, intent to cause harm; and thirdly, systematic dissemination.

Based on joint regulation of mandatory codes of conduct for VLOPs, resulting from an agreement between the European Commission and the platforms themselves, the role of the CNMC in application of the DSA can contribute in the following ways: firstly, selecting trusted flaggers to report content as key actors, defending freedom of expression of trusted outlets (forming a link with the European Media Freedom Act); secondly, since the content is distributed on platforms, CNMC can require a platform to analyse systemic risks, establish risk mitigation measures (with supervision from national agencies and the European Commission), to perform joint self-supervision and monitoring, to demonetize this type of content and even to draft protocols for crisis situations; thirdly, it can adopt measures concerning transparency of content moderation rules, either by prohibiting dark patterns, forbidding profiling for adverts using protected data, or requiring entities to assemble repositories of adverts.

The Protocol to Combat Illegal Hate Speech Online is a useful tool in the fight against hate speech online, with key features such as accreditation and training of trusted flaggers by the administration and providers of data storage services (Section IV), thus enabling hate speech to be identified (in contrast with the DSA, which provides for training, but not for accreditation). The entry into force of the DSA and the creation of the new role of Digital Services Coordinator will necessitate changes to the Protocol to ensure a new coordinated response concerning removal of illegal content.

From applying the Protocol, it can be concluded that most of the hate speech identified has four traits: firstly, the most targeted groups, which are currently people from North Africa, muslins and black people; secondly, the type of discourse, with 53% displaying serious dehumanization and 54% overt aggressiveness; thirdly, drawing links with events relating to a lack of public safety; and lastly, use of false information.

Technology

Technology plays a two-faceted role in the context of disinformation and hate speech. On one hand, it has been found that technology can exacerbate these problems; social networks and other online platforms are used to spread disinformation quickly and to a large audience, fuelling polarization of societies and hate speech. The recent democratization of advanced language models, such as generative AI models, may add to this situation by facilitating production of manipulated and fabricated content that is more difficult to see through and more effective.

On the other hand, there is a responsibility to make the best use possible of these technologies to counteract harmful effects. Advances in artificial intelligence and natural language processing technologies can be used not only to identify patterns of inappropriate behaviour (such as hate speech, offensive language and disinformation) but also to mitigate them by crafting counternarratives that enable a response to hate speech in the form of positive language that promotes much more respectful and constructive interaction online.

The giant leaps in generative artificial intelligence in the last few years, and especially in large language models (LLMs) has put the spotlight on the many researchers who work on identifying online hate speech and producing counternarratives.

However, use of such models to detect hate speech poses certain challenges, such as the need for models that have been trained in the languages being used (Spanish and Spain's co-official languages), better detection of sarcasm and irony, and improved handling of ambiguous language, changes in language over time, and regional dialects. Employing models of this kind also offers opportunities. For instance, there are numerous resources in Spanish that can be used to train the models, they can continue to learn, and multidisciplinary cooperation among experts is steadily increasing, ranging from sociologists to psychologists, and even jurists.

The huge volume of information currently found on social networks makes automated detection of hate speech insufficient on its own, as even if hate speech is identified, there are not enough resources available to ensure a comprehensive human response. Therefore, artificial intelligence models are also being tested for work to mitigate and automatically generate counternarratives. This is an alternative to blocking users or deleting messages and is less damaging to freedom of expression, and is also a potential tool for preventing radicalization.

Generation of counternarratives is based on automated or supervised generation of responses to hate speech, offering an alternative and positive viewpoint. Different counternarrative strategies are currently being studied. Each is effective in different ways, depending on the situation and the audience. In the same way that threat actors that promote or spread disinformation exploit vulnerabilities in the societies they target, the defence against disinformation and hostile influence in the information space based on positive narratives must be analysis-based. That analysis should examine not only vulnerabilities and what divides people, but also strengths and what unites people and brings them together as a democratic, plural society that respects differences in identity traits.

At present, wider implementation and improved mechanisms are needed to enable evaluation of the effectiveness of the counternarratives.

Although progress is steadily being made on studies of the algorithms that platforms use to promote and recommend content, further work is needed to understand the implications in terms of polarization, and how the over-stimulation caused by the existing attention models of certain networks are disrupting the cognitive processes needed to correctly evaluate and absorb information.

Media literacy, awareness raising and the role of the Third Sector

Better media literacy and information literacy is a key challenge in the fight against disinformation. In the sphere of education, not only is it important to publish an official curriculum on disinformation, it is also important to work to ensure that the curriculum is followed effectively in classrooms.

Educational establishments' current capability to improve media literacy is not sufficient, as the education sector's capacity for action is limited. In the current informational context, the media and online platforms are the parties with the greatest public reach.

Training of the public, and especially young people, must effectively improve their ability to spot hoaxes, their critical thinking, their analysis of context and their assessment of given indicators, so that they can weigh up the factors that may increase or reduce the credibility of the source. This applies for written, audio and audiovisual material.

The advances in understanding of the different tactics used to spread hate speech and disinformation are also key to media literacy.

For example, messages that include hateful elements are much more likely to be shared; however, they tend to be considered less credible in general. This is crucial when raising awareness and improving media literacy.

Furthermore, families can play a vital role, in collaboration with teachers, in facilitating classroom work on accepting disagreement, dissenting opinions, multiple viewpoints and conflict, all of which form part of social relations. This will contribute to combating and even preventing hate speech on social networks. Education has proven effective in cutting short the process that leads to hate and violence.

Fact-checking of messages, in any media, has also proved effective in identifying and neutralizing unnoticed disinformation. However, such efforts are time-consuming and call for considerable expertise and resources. Moreover, exposing or tagging disinformation is not enough on its own; explanations are also needed of why something is disinformation. Collaboration between fact-checkers and transparency on the approaches and methods employed are also crucial. In this respect, features such as community notes and systems for crowdsourced content tagging, adding context or fact-checks to misleading content, can complement content moderation, which also needs to be improved.

In addition, professionals in information science and all forms of social media need ongoing training and awareness-raising activities—while respecting freedom of expression—with an intercultural and intersectional approach. It is important to include educators in discussions on strategies, not only for media literacy but also for communication. This can take into account and consider the long-term effects of strategies. Awareness-raising is also needed in the business sector, to limit the monetization of disinformation campaigns, by eliminating or limiting pecuniary incentives.

At present, organizations in the third sector do not have the necessary resources or shared procedures to combat this threat. Cooperation with other stakeholders from civil society, such as fact-checkers, has produced good results in terms of better understanding of the threat.

In this regard, under current circumstances, the DSA is the right tool with which to organize the necessary responsible triangular collaboration between national authorities, providers of global digital services—especially but not only social networks—and civil society organizations. Ideally, this collaboration would be carried out using platforms that bring these stakeholders together and empower them, to go beyond current participatory processes, and position them as strategic influencers. It would set the basis for specialized public policies and lines of reasoning to prevent and combat disinformation and hate speech.

Lastly, because disinformation is international, it is important to work alongside other countries in promoting instruments for awareness-raising and media literacy, and ensuring that tools for detecting and moderating in different languages are sufficient. This would help to limit the impact that campaigns can have on groups in third countries and reduce their reach, preventing them from spreading to Spain by exploiting the permeability of networks and even through the diaspora. When undertaking communication and media literacy activities focused on other regions, it is vital to consider their cultural and social circumstances, to avoid ultimately amplifying the effect of disinformation.

RECOMMENDATIONS

Greater progress is needed in the area of awareness-raising, to improve understanding and recording of this threat and its impact. This will also provide a basis for participation by all stakeholders in society, who must join forces to combat the threat.

The narratives have been identified. The strategies are also being identified. Fully identifying the whole (narratives and strategies) will enable increasingly effective initial pinpointing of intent (especially if artificial intelligence is used to achieve this). This could result in very substantial progress in the fight against hate speech, because it would determine one of the most elusive characteristics: the author's intent. Naturally, in the event of a dispute, this identification would only be provisional and would be subject to review by a court.

Identifying answerable parties seems a promising area for action. This is particularly true if work has been done on the previous points (identifying narratives, strategies and intent). Consideration could be given to treating parties that habitually spread or produce disinformation to fuel hate speech in a way similar to criminal organizations.

In terms of law, this would require assessment of a possible amendment of Article 510 of the Criminal Code to include prosecution of public and malicious dissemination of patently false content as described above. On this same point, thought should be given to discussing, at the national and European levels—but without assuming a particular outcome—the policy opportunity of establishing and defining a new form of crime, with all of the provisos and limits outlined in this text. This would enable prosecution of planned and coordinated conduct that clearly and intentionally disregards the truth to publicly disseminate false or deliberately manipulated content, whereby the author expects or can be reasonably said to expect to produce hateful, hostile, violent, discriminatory, humiliating or denigratory public reactions towards people or groups, with the intent to cause discrimination. The purpose of all of this would be to prevent forced recourse to interpretation as the existing crime of defamation with discriminatory intent, set out in Article 510.1.A) of the Criminal Code, as conduct that constitutes dissemination of hoaxes is proving extremely difficult to include therein. The legal definition of the new crime should be limited to cases of direct intentional action to spread hoaxes or doing so with constructive malice or recklessness, to avoid omitting any conduct from the definition.

However, excessive measures must not be applied in the punitive response, or in the potential threat to the values being defended. A collaborative and measured response is much more advisable. Recourse must be available to administrative proceedings for actions that are not serious and do not put the targeted group in danger.

Improvements are needed to regulation and application of the administrative system of penalties and the possibility of disclosure of traffic data for administrative proceedings to impose penalties and civil proceedings concerning defamation, violations of privacy, and violation of image rights. Better coordination is also needed among national and regional institutions, to ensure that penalties are applied effectively and do not expire. Solutions must be applied to ensure that responses under administrative proceedings to impose penalties are coordinated, uniform and expedient, and involve all of the national and regional authorities, to limit the reach and impact of these threats; throughout the entire process, whether the proceedings are criminal or administrative, the Digital Services Coordinator must play a key role, within the framework established by the DSA, in removal of illegal content that is subject to criminal or administrative penalties. To enable the Coordinator to do this, relevant regulations must swiftly be established to authorize them to take action.

Lastly, the provisions of the DSA and the protocol for removal of illegal online content must be implemented without delay.

One of the key challenges in terms of technology is the transfer of the various ongoing investigations to identify and respond to these threats. Opportunities must be pinpointed for effective implementation of these technologies.

Use of AI tools to combat disinformation relating to hate speech seems the most promising way forward, but the technology needs further development. There are also technical and legal hurdles. As a result, two needs arise: firstly, greater efforts in terms of material and human resources to design effective tools; secondly, ensuring interdisciplinary collaboration on design, to factor in the ethical and legal values that are to be safeguarded.

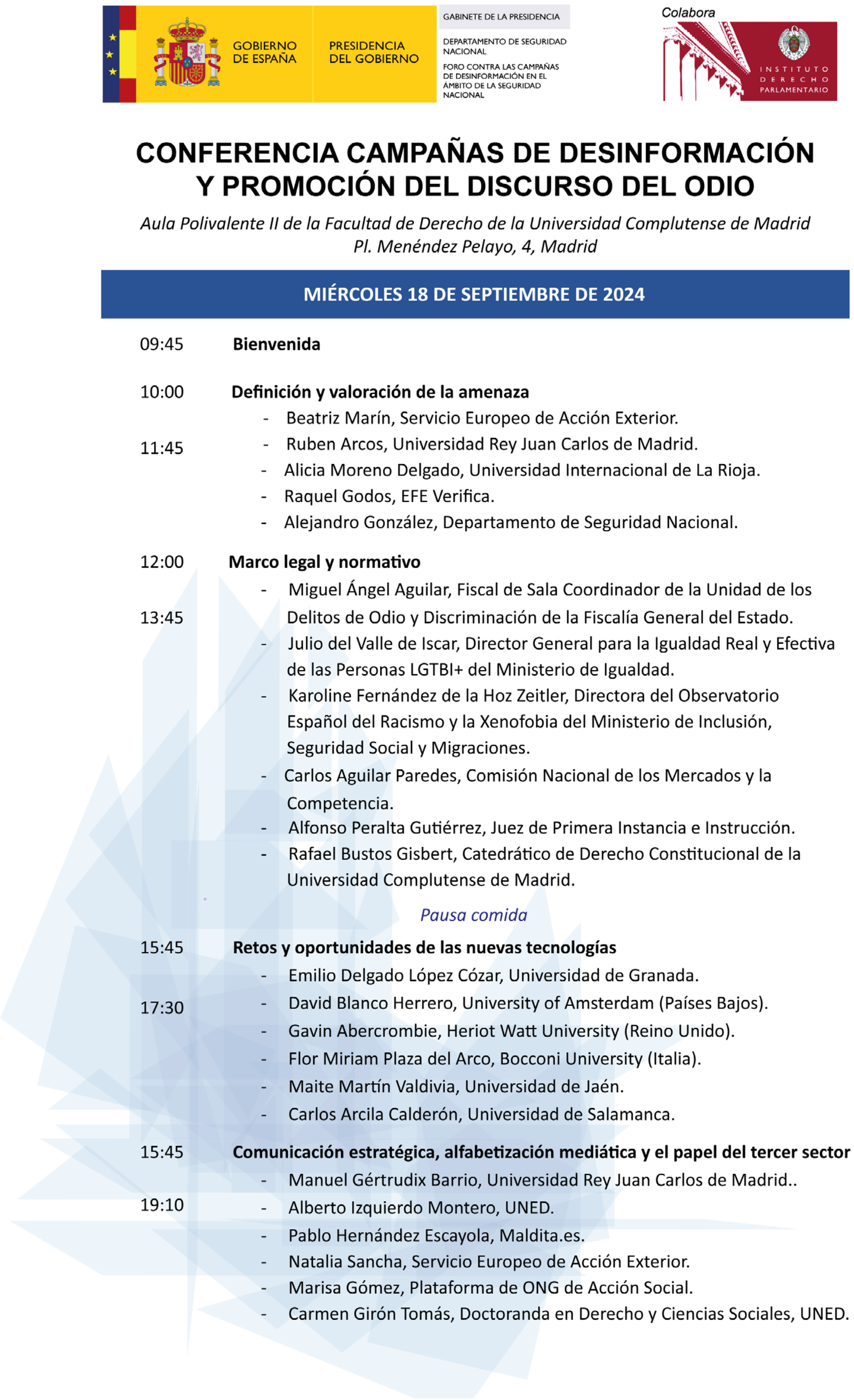
Use of AI tools also calls for adequate supervision and classification of such tools as high-risk. It would entail meeting technical requirements (EU Artificial Intelligence Act) and establishing procedures for public authorities to authorize, recognize, implement and supervise (governance of the AI-enabled fight against hate speech based on disinformation).

In the area of media literacy, it is essential to identify strategies that ensure the public are actually acquiring skills. To achieve this, media outlets and online platforms must be involved, and curricula on disinformation must be effectively applied in classrooms.

Moreover, it would be beneficial to build not only a counternarrative, but also “countermarketing”, aiming to publicly expose influence, disinformation and manipulation operations to the people of Spain.

Lastly, further training is needed for workers in third sector organizations, exploring mechanisms for cooperation with other stakeholders such as fact-checkers, academics and online platforms. It would also be advantageous to foster development of shared procedures that facilitate organizations’ work in this area.

.



GOBIERNO DE ESPAÑA PRESIDENCIA DEL GOBIERNO

GABINETE DE LA PRESIDENCIA

DEPARTAMENTO DE SEGURIDAD NACIONAL

FORO CONTRA LAS CAMPAÑAS DE DESINFORMACIÓN EN EL ÁMBITO DE LA SEGURIDAD NACIONAL

Colabora

INSTITUTO DERECHO PARLAMENTARIO

CONFERENCIA CAMPAÑAS DE DESINFORMACIÓN Y PROMOCIÓN DEL DISCURSO DEL ODIO

Aula Polivalente II de la Facultad de Derecho de la Universidad Complutense de Madrid
Pl. Menéndez Pelayo, 4, Madrid

MIÉRCOLES 18 DE SEPTIEMBRE DE 2024

09:45 **Bienvenida**

10:00 **Definición y valoración de la amenaza**

- Beatriz Marín, Servicio Europeo de Acción Exterior.

11:45
- Ruben Arcos, Universidad Rey Juan Carlos de Madrid.
- Alicia Moreno Delgado, Universidad Internacional de La Rioja.
- Raquel Godos, EFE Verifica.
- Alejandro González, Departamento de Seguridad Nacional.

12:00 **Marco legal y normativo**

- Miguel Ángel Aguilar, Fiscal de Sala Coordinador de la Unidad de los Delitos de Odio y Discriminación de la Fiscalía General del Estado.

13:45
- Julio del Valle de Iscar, Director General para la Igualdad Real y Efectiva de las Personas LGTBI+ del Ministerio de Igualdad.
- Karoline Fernández de la Hoz Zeitler, Directora del Observatorio Español del Racismo y la Xenofobia del Ministerio de Inclusión, Seguridad Social y Migraciones.
- Carlos Aguilar Paredes, Comisión Nacional de los Mercados y la Competencia.
- Alfonso Peralta Gutiérrez, Juez de Primera Instancia e Instrucción.
- Rafael Bustos Gisbert, Catedrático de Derecho Constitucional de la Universidad Complutense de Madrid.

Pausa comida

15:45 **Retos y oportunidades de las nuevas tecnologías**

- Emilio Delgado López Cózar, Universidad de Granada.

17:30
- David Blanco Herrero, University of Amsterdam (Países Bajos).
- Gavin Abercrombie, Heriot Watt University (Reino Unido).
- Flor Miriam Plaza del Arco, Bocconi University (Italia).
- Maite Martín Valdivia, Universidad de Jaén.
- Carlos Arcila Calderón, Universidad de Salamanca.

15:45 **Comunicación estratégica, alfabetización mediática y el papel del tercer sector**

- Manuel Gértrudix Barrio, Universidad Rey Juan Carlos de Madrid..

19:10
- Alberto Izquierdo Montero, UNED.
- Pablo Hernández Escayola, Maldita.es.
- Natalia Sancha, Servicio Europeo de Acción Exterior.
- Marisa Gómez, Plataforma de ONG de Acción Social.
- Carmen Girón Tomás, Doctoranda en Derecho y Ciencias Sociales, UNED.

ANEXO: Agenda de la conferencia celebrada el 18 de septiembre de 2024

BIBLIOGRAPHY

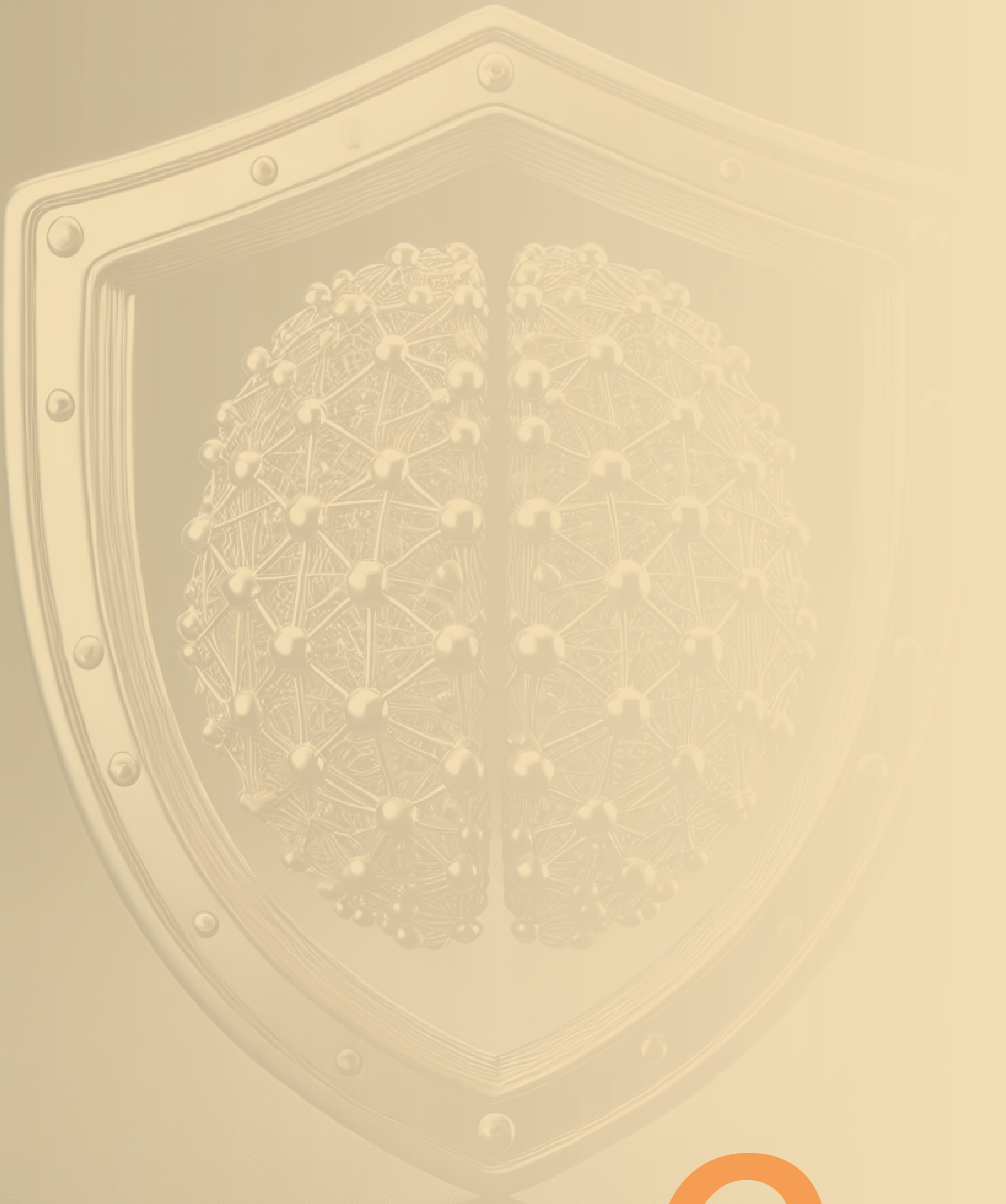
Alonso-Villota, M., and R. Arcos (2024), “The Coercion-Manipulation-Persuasion Framework: Analyzing the Modus Operandi of Systems of Non-State Actors”, *Terrorism and Political Violence*, June, pp. 1–19, https://doi.org/10.1080/09546553.2024.2357082

EEAS Stratcom Division (European External Action Service Strategic Communication Division) (2023), *FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-LGBTQ-Report.pdf

Hoogensen Gjørv, G., and O. Jalonen (2023), “Identity as a tool for disinformation: Exploiting social divisions in modern societies”, *Hybrid CoE Strategic Analysis 34*, November, https://www.hybridcoe.fi/wp-content/uploads/2023/11/20231108-Hybrid-CoE-SA-34-Identity-as-a-tool-for-disinformation-WEB.pdf

RAN (Radicalisation Awareness Network) (2020), Conclusion Paper: *The Impact of Conspiracy Narratives on Violent RWE and LWE Narratives*, November, https://home-affairs.ec.europa.eu/system/files/2021-01/ran_c-n_concl_pap_impact_consp_narr_on_vrwe_vlwe_24-25_112021_en.pdf

Szakács, J. and É. Bognár (2021), *In-depth analysis requested by the INGE Committee: The impact of disinformation campaigns about migrants and minority groups in the EU*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/653641/EXPO_IDA(2021)653641_EN.pdf



CHAPTER 6

SCEPTICISM IN THE MEDIA AND IN PUBLIC OPINION IN SPAIN REGARDING DISINFORMATION CAMPAIGNS THAT AFFECT NATIONAL SECURITY

Coordinators:

Emilio Andreu

Department of National Security

Authors and contributors:

Maria Inmaculada López Núñez

María Penedo Jiménez

Jordi Rodríguez Virgili

INTRODUCTION

IIf only this scepticism was that of Hume, which woke Kant from his “dogmatic slumber”, as the Königsberg philosopher himself acknowledged. But it is not. This scepticism is far-removed from its etymological origin—the Ancient Greek verb sképtesthai, which means to examine, consider or think—as we must inescapably refer to the mental no man’s land between tedium and indifference.

No reasonable person has any doubt that there is foreign interference—by Russia in particular—in the countries of the European Union and of the North Atlantic Treaty Organization (NATO), aiming to undermine society’s trust, specifically in these two multilateral organizations but also generally in the pillars of the democratic rule-based system. What is more, much trust already seems to be undermined, given the results of the Social Trends Survey conducted by the Centre for Sociological Research. The findings of the most recent survey, in October 2023, painted a disheartening picture in terms of the overall percentages of society’s minimum-maximum trust in major political and official organizations.

Today’s irrelevance of the mass media is not unique to Spain. In the latest report by the Reuters Institute for the Study of Journalism, covering 2024, just 40% of survey respondents from 47 different countries said they trusted most news items. This reluctance among the public to believe information from the press, radio and television is nothing new. In 1991, 67% of French people did not consider printed or broadcast news to be even minimally trustworthy, according to a survey conducted by the privately run polling body Études et Sondages d’Opinion Publique (ESOP). At that time, 33 years ago, experts attributed this to manipulation through an avalanche of information dressed up as entertainment.

In the present day, in the age of the fifth generation of mass media, of social networks and instant messaging, the saying attributed to Saint Agustine that “contra facta non valent argumenta” (you can’t argue with facts) seems to have become obsolete. In fact, truth and facts no longer matter and are being overrun by post-truth narratives.

On 29 February 2024, the Forum against Disinformation Campaigns Affecting National Security approved the creation of a working group whose main purpose was to determine whether it was plausible that the media and public opinion were sceptical with regard to warnings over disinformation campaigns and State actors that repeatedly resort to such tactics, such as Russia.

It is vital to identify the starting point for public opinion in terms of awareness-raising and knowledge of these threats, as it will determine and be exploited by threat actors' strategies, and should be factored into public policies to improve awareness and media literacy.

Emilio Andreu, spokesperson for the Spanish Federation of Associations of Journalists (FAPE), was selected to coordinate the working group, and the Department of National Security was selected to coordinate the public authorities. The working group comprises the experts listed at the beginning of this chapter

Question 4
In general, could you rate from 1 to 10 the confidence that you have at this moment in each of these political and institutional organizations, understanding that 10 would represent "maximum confidence" and 1 "minimum confidence"?

Degrees of evaluation	1 minimum confidence	2	3	4	5	6	7	8	9	10 maximun confidence	N.S.	N.C.	(N)
In the political parties	26,3	8,3	10,3	11,8	18,3	11,3	7,0	3,6	1,0	1,1	0,3	0,7	(4.121)
In the trade unions	29,6	7,9	9,8	9,3	14,8	10,1	8,4	4,9	1,6	1,6	1,5	0,4	(4.121)
In the Spanish Government	33,7	6,8	6,6	8,7	11,5	9,2	9,7	7,4	2,6	3,1	0,3	0,4	(4.121)
In the Spanish Parliament	21,2	7,4	8,9	11,1	17,9	11,1	10,0	6,4	1,9	2,7	1,1	0,3	(4.121)
In the mass media (press, radio, television)	19,3	9,7	11,8	12,5	18,9	10,9	7,9	5,0	1,3	1,8	0,3	0,5	(4.121)
In Justice	12,4	6,6	8,4	10,3	18,5	13,9	13,9	10,2	2,4	2,6	0,4	0,2	(4.121)
In the Constitution of 1978	6,9	2,9	4,4	5,3	12,4	9,8	12,3	16,9	11,9	14,6	1,9	0,6	(4.121)

TABLE: Social Trends Survey prepared by the Spanish Centre for Sociological Research (CIS). October 2023

IMPLEMENTATION OF THE INITIATIVE

The purpose of the group was to analyse whether public discourse in Spain was trivializing foreign interference that sought to undermine society's trust in institutions. The group of experts considered that the way to assess this possible scepticism over disinformation campaigns was through discussion groups.

A discussion group is a qualitative research tool that consists of bringing together a set of respondents to express their views, debate and answer questions on an issue that is of interest to a researcher. It is a proven research method for corroborating hypotheses or proposals.

The group of experts decided to form two separate discussion groups: one focused primarily on public opinion and the other concentrating on the role of the media. The two groups were closely interrelated, as was demonstrated by the debates, but the view was that by separating the two areas more in-depth conversations would take place.

Two discussion groups were therefore held to assess whether or not there was scepticism in Spain regarding the existence of disinformation campaigns that affected national security, in terms of public opinion and in terms of the media.

The group of experts selected the respondents to participate in the two groups. The public opinion discussion group benefited from the experience of:

- Sergio Hernández. Head of the EFE news agency's fact-checking division, EFE Verifica.
- Helena Matute. Professor of Experimental Psychology at the University of Deusto.
- Andrés Medina. Founding partner of Gravitas.
- José Javier Olivas. Researcher and lecturer in the Department of Political Science and Government of the National University for Distance Education (UNED).
- Hélène Verbrugghe. Public Policy Manager for Spain and Portugal at Meta

The media discussion group comprised:

- César González Antón, Director of La Sexta Noticias.
- Jose Antonio Zarzalejos, Chair of the Editorial Board of El Confidencial.
- María Rosa Berganza Conde, Professor of Political Communication and Director of the Center for Media and Political Communication Research of Rey Juan Carlos University.
- Xavier Colás, journalist.

Prior to the meeting, the process was explained to the participants, and they were sent key questions:

- Research question: Is there scepticism in public opinion in Spain regarding whether there are disinformation campaigns that affect national security? Short explanation of the reasoning behind their answers.

Questions to prompt initial expressions of views:

- According to Eurobarometer data, in the Citizenship and Democracy category (EB 528), 82% of Spanish citizens agreed (54% totally agree, 28% tend to agree) that foreign interference in our democratic systems is a serious problem that should be addressed. In view of these results, it seems that the answer to the research question put to the discussion group is “no”. Do you agree with this interpretation? If not, how do you explain the results?

- Based on your knowledge and professional experience, which factors are key to perception of disinformation campaigns by the public, which may contribute to increasing or decreasing scepticism about such campaigns?.

For the discussion group on the media, the research question was the same, but the supporting questions were slightly different:

- Whatever your answer to the research question (including any qualification), what do you think are the main causes of the perception, especially by the media?

- Based on your knowledge and professional experience, what can journalists and the media do to support and improve public awareness of disinformation campaigns?.

The two groups were provided with links to various reports and surveys on the perception of disinformation in Spain

The first discussion group met on Thursday, 26 September 2024, at the Moncloa Complex. From the group of experts, Inmaculada López Núñez, lecturer from the Department of Social, Industrial and Differential Psychology of the Complutense University of Madrid, and Jordi Rodríguez Virgili, lecturer in Political Communication from the University of Navarra, acted as moderators for the debate. The other experts attended the meeting, but did not address it.

The second discussion group met on Thursday, 3 October 2024, at the premises of the Madrid Press Association. From the group of experts, Emilio Andreu, spokesperson for the Spanish Federation of Associations of Journalists (FAPE), and María Penedo, Communications Director from the Union of Free-to-air Television Broadcasters (UTECA), acted as moderators for the debate. The other experts attended the meeting, but did not address it.

Based on the conversations in each discussion group and the experience and knowledge of the participants, the most frequent and interesting conclusions and recommendations were selected, without this denoting unanimity among the experts or the working group.

CONCLUSIONS

There is awareness of the general risk posed by disinformation and foreign interference. However, greater insight is needed into the specific aims of such threats and how they affect the public; there is no perception of a specific threat. Some possible causes of this are:

- Not enough information on these threats reaching the public.

- Foreign interference operations being hidden, downplayed or trivialized in Spain.

- The public potentially feeling that they are treated as victims of disinformation, and that only public authorities or the Government should combat it. The public is thus not being held jointly responsible for combating disinformation or at least curtailing it.

- Instances of foreign interference being politicized. Partisanship and polarization favour politicization of these issues, and this may be exploited by threat actors.

- The threat being complex. Although manipulation strategies are not a new occurrence, the tactics used and their complexity hamper detection and exposure and prevent society from correctly identifying the extent of the manipulation and therefore the nature of the threat.

- Persons in academia, fact-checking and civil society who work on identification of such threats being harassed or attacked. This limits public exposure of threats and more open reporting of them.

- Media detoxes, media fatigue and news avoidance becoming more widespread. This may lead to a perception that one is not exposed to a threat or even to indifference about a threat.

- Perception of a threat inside a democratic system overshadowing or hindering perception of an external threat. Some surveys suggest that society is disenchanted with how democracy is functioning in Spain.

- Key stakeholders responsible for raising awareness of threats not being the most trusted by society (the Government, political leaders and the media).

- Disinformation campaigns by foreign State actors being ever-present. This hampers identification and exposure. One of the main aims of disinformation campaigns, rather than merely selling a lie, is to have people believe nothing, fuelling widespread distrust. The goal is for the public to become sceptical, withdrawn from public life, undermining social cohesion and thus weakening the structure of the State.

- An increasingly disengaged society connecting only in polarized ways. As a result, confirmation biases are strengthened and the public may even applaud or at least downplay disinformation that harms political opponents. This lack of connection is also a result of information overload.

- The threat from foreign enemies dating, in Spanish history, from distant times, such as the French invasion, while more recent conflicts have been internal. This may mean that domestic threats are perceived more intensely than those from abroad.

- There not being a culture of security and defence in the country. There is a view that discussing a culture of security and defence is a thing of the past, linked to ideological and political values rather than democratic values.

The media has encountered a number of difficulties when conveying information on disinformation campaigns tied to foreign interference. These difficulties include:

- National security not being on the agenda of the media. National security not having a defined profile, which enables grouping of news items on the issue. The term being considered wide-ranging and poorly defined in public opinion.

- There being no well-defined information system for national security, which journalists can consult for information on related issues.

- There being a shortage of official spokespersons who are skilled communicators and able to connect with audiences, to participate in public debate on these issues.

- As a result of the above, few journalists specializing in national security.

The media system is also often a key target for threat actors. They exploit vulnerabilities in the model of the sector to erode society's trust in the media and redirect the public to "alternative" sources, such as channels on social networks and messaging apps, to drive intake of unsubstantiated information. Some of these vulnerabilities originate from the new media ecosystem and technological disruption.

The media remains the public's preferred source of information, as found by the First Study on Disinformation (*I Estudio sobre desinformación*) by UTECA and the University of Navarra, published in 2022. In the survey, 84.6% of respondents said they preferred to obtain information from media outlets rather than social networks and 80.9% answered that media was the best safeguard against the spread of disinformation. The sector also faces other challenges:

- The anonymity offered by social networks is contributing to polarization and a lack of fact-checking. This situation has been mirrored by the comments sections and forums on the sites of newspapers, which also offer anonymity.

- Removing the barriers to entry into content production and distribution (and therefore also journalism) has led to a chaotic and competitive environment, in which news businesses swiftly appear and disappear, with all sorts of different approaches to "journalism", competing in an increasingly fragmented and divided attention market. In this market, the economic and institutional weaknesses of traditional media outlets have fuelled practices to influence and control them.

- The media sector must compete on an unequal footing with other industries, and especially the technology sector. Media outlets, which are subject to stricter regulation, are competing at a disadvantage.

- Less profitability for traditional media outlets, with fewer staff, worse pay and less resources, is preventing them from having specialized journalists, sending correspondents to other locations and performing in-depth investigations.

- The current social environment calls for dissemination of engaging messages, to compete with intentionally misleading narratives that resort to sensationalism or alarmism over facts. Facts are losing the battle to spin. Journalists must therefore explain the facts that disprove disinformation in an engaging, emotive, exciting and energetic way.

RECOMMENDATIONS

Promote media literacy and raise awareness:

- Promote media literacy and raise awareness (to improve understanding of a threat and the impact it could have on the immediate environment of a person, and foster appreciation of high-quality information in a context of information overload).

- Ensure that information on foreign interference operations is not downplayed or exaggerated. Also, prevent such operations from being concealed, trivialized or politicized. Encourage a culture of transparency that simplifies access to data for journalists, researchers and the public.

- Foster an active population. Raise awareness of the role of the public and their duties when consuming information, and convey that they are an active part of the fight against disinformation. The work of the public can be key to identifying and reporting untruthful, manipulated content, and to preventing it being shared.

- Conduct more targeted studies, to better understand public perception and the process of trivialization of threats and foreign interference.

- Promote a culture of national security and defence among the public. Raise awareness of the concept of national defence as a democratic value.

- Foster dissemination of engaging messages, to compete with deliberately misleading narratives. Raise awareness and promote media literacy, in terms of the communication work of the media and the communications of public authorities.

Promote inclusion of national security in the media agenda:

- Establish an information system in the area of national security, clearly identifying points of contact for journalists and fostering training for those persons on the subject.

- Foster training of journalists in the area of national security.

- Promote work that is more informative by media outlets on the issue of foreign interference. Build engaging narratives that connect with society.

- Promote the role of official spokesperson on national security, with the capacity to communicate effectively, believably and in an engaging way.