In 1998, General Vladimir Slipchenko, then Vice President of the Russian Academy of Military Sciences, stated that “information is a weapon just like missiles, bombs, torpedoes, etc. It is now clear that the informational confrontation becomes a factor that will have a significant impact on the future of the war themselves, their origin, course and outcome”.

Military logic and technological transformation have converged in a digital space in which the internet has become one of the crucial fields of destabilisation. In The Road to Unfreedom: Russia, Europe, America (2018), Timothy Snyder writes that the most important part of Russia’s 2014 invasion of Ukraine was the information warfare designed to undermine reality. Between that initial cyber offensive, the largest in history, according to Snyder (although it didn’t make headlines in the West), and the digital frontline of the Russian invasion of Ukraine that began on February 24th 2022, the hybridisation of the conflict and the contestation of the global order underwent their own acceleration.
For the West, the war in Ukraine is the first to go viral, being broadcast over social media in real time and narrated on the basis of fragments of images that attempt in just a few seconds to convey the threats, fears, heroic acts and devastation. The online story does not always match the offline facts. In truth, though, it is not the first war to be mediated by social networks. Syria was the laboratory for evading an international media blackout using a torrential flow of online content provided by local activists and journalists from within the country. This, in turn, raised major ethical questions about information circuits and the veracity of sources.

But Ukraine could become the first war to pit the two major global digitalisation models and their respective platforms against one another. Russian and Chinese techno-authoritarianism versus the US Silicon Valley model. Telegram and Tik Tok’s power to shape the global narrative about the war versus US technology giants’ involvement in the conflict as private actors aligned with Western strategies to exert political pressure, to capture and control data (from mapping to censorship), or to provide analysis and technical information to strengthen the Ukrainian government’s security.

(Dis)information is a weapon in wartime and a hybrid threat to peace. It is a non-military tool that can be used to disrupt and destabilise civic spaces, with consequences for local, regional and national security. But its truly offensive capacity resides less in the content of the message than in the power social networks grant it to go viral and penetrate. Hence, it is first essential to understand how digital interconnection has transformed social relations and power balances at a global scale, both between major powers and between the new international relations actors (state, non-state and private). Disinformation cannot be separated from the socio-psychological factors, technical drivers and incentives that are intrinsic to our hyperconnected times (Van Raemdonck and Meyer, 2022).

**Algorithmic order**

The internet is the infrastructure on which our daily life is built. Technology has transformed our experience of immediacy, plunging us into an infinity of (dis)information possibilities, a profusion of sources and stories – true or not – offered to us by the internet with no need for intermediaries. Post-truth does not just mean lies. It means a distortion of the truth that is above all laden with intentionality. In this space, information competes with contradictory stories, hoaxes and half-truths, conspiracy theories, messages of hatred and attempts to manipulate public opinion. The explosion of online disinformation has led «a new social harm» (Del Campo, 2021) to
emerge via a range of types of falsehood – both legal and illegal – that impact public discourse and human security.

Old-style propaganda has been exponentially amplified by technology and hyperconnectivity and its power and sophistication have multiplied. The possibilities are vast: social networks (open or encrypted); bots (software applications that execute automated tasks) and microtargeting techniques, such as dark advertising, which is psychometrically targeted to influence public opinion and poison the discursive atmosphere; artificial intelligence systems fed data and trained to mimic humans or reproduce human cognition; and audio and video manipulation techniques that change our perceptions and lead us to distrust even our ability to discern what is and is not true.

For Byung-Chul Han (2022), «infocracy», or the digital world’s «information regime», is a form of dominance in which information and its processing through algorithms and artificial intelligence decisively determine both economic and political social processes. The ability to alter information and data – so decisive for obtaining power – poses a threat to democratic processes.

Algorithms are exploited by companies like Cambridge Analytica to create profiles based on people’s gender, sexual orientation, beliefs and personality traits to be used for political manipulation. Societies are vulnerable because we are vulnerable as individuals. We are exposed to the opaque order and will of algorithms that Cathy O’Neil elevates to the category of «weapons of math destruction».

Disinformation, defined by the European Commission as «false information, deliberately created to harm a person, social group, organisation or country», aims to destabilise societies and directly attacks civic spaces with the aim of fomenting polarisation and unease, if not outright conflict (Freedman et al., 2021; Medina, in this volume). But misinformation does not spread in a vacuum. Its ability to penetrate public debates, to confuse, and to undermine trust in institutions and electoral processes, for example, is often based on existing socio-cultural divisions. It targets pre-existing
vulnerabilities and groups of people supposedly inclined to trust such sources and narratives, and who may willingly or unwillingly contribute to their dissemination. Abuses of power, dysfunctional political systems, inequalities and exclusion are breeding grounds for disinformation (Van Raemdonck and Meyer, 2022).

The identification of these vulnerabilities in order to generate messages that exacerbate them is considered to pose a hybrid threat to democratic systems, which are more exposed due to their open nature. In Chantal Mouffe’s (1999) agonistic model, conflict and challenging the political and social status quo are essential parts of pluralism in deliberative democracies. But when disinformation violates the right to hold opinions without interference (article 19 of the ICCPR), increases citizens’ vulnerability to hate speech or strengthens state and non-state actors’ ability to undermine freedom of expression it becomes a threat to human rights and the bases of democracy. Disinformation in all its forms – from lies to incitement to hatred, via memes and audiovisual manipulation – are, thus, not only «weapons of mass distraction», they often form part of deliberate disruption strategies to alter the perceptions of public opinion. In these cases, along with the goal of causing harm or making profit that characterises this false content, there are usually strategies and techniques designed to maximise their influence. The aim is to undermine the adversary’s values and the legitimacy of their political system (Bargués and Bourekba, in this volume).

When analysing the actors responsible for disinformation, UNESCO’s Working Group on Freedom of Expression and Addressing Disinformation distinguishes between the authors of the content and those in charge of distributing it: between instigators (direct or indirect), who are active at the origin of the disinformation; and agents (influencers, individuals, organisations, governments, companies and institutions), who are in charge of spreading the falsehoods (Bontcheva and Posetti, 2020). The agents who spread the falsehoods, conspiracies and threats – voluntarily or involuntarily – and act as amplifiers of the disinformation may, in turn, be victims of manipulation or attempts to
exploit social vulnerabilities. The result is increased scepticism and lower trust in institutions. Today, the consensuses that structure democratic societies are weaker.

This is by no means solely a Western phenomenon, and the threats do not only come from outside. The polarisation that has grown in global politics, especially over the last five years, has shown social media's power to radicalise public discourse. From the January 6th insurrection on Capitol Hill in Washington to the Rohingya genocide in Myanmar; and from the exploitation of the US racial conflict using fake accounts and online trolling to the «brutal and unrelenting» disinformation campaign promoted by the Russian and Syrian governments (according to a Bellingcat investigation in 2018) against the White Helmets, the NGO in charge of investigating the flagrant human rights violations committed by both countries’ armies during the Syrian war.

Post-truth geopolitics has transformed threats and strategies. As the World Economic Forum’s Global Risks Report warned in 2019, «[n]ew technological capabilities have amplified existing tensions over values—for example, by weakening individual privacy or deepening polarization—while differences in values are shaping the pace and direction of technological advances in different countries».

**Geopolitical order**

There are no geographical limits to the manipulation attempts, and they do not have a single origin. In recent years, Facebook and Twitter have listed seven countries (China, India, Iran, Pakistan, Russia, Saudi Arabia and Venezuela) that use the platforms to conduct foreign influence campaigns to sway global audiences. Social networks are a new instrument of geopolitical power that have enthroned certain recently emerged global disinformation actors and are disrupting the traditional hegemonies over the international narrative.

As well as digitalisation processes, the COVID-19 pandemic also accelerated what Josep Borrell, the EU’s High Representative for Foreign and Security Policy, calls a «global battle of narratives», further fuelling the sense of Western vulnerability. It is not a new sensation. For over a decade, the digital world had been shaking the structures of the post-1945 order. In 2011 then Secretary of State Hillary Clinton warned the United States Congress that her country was immersed in «an information war and we are losing». Clinton was referring to the global presence of RT (Russia Today), China’s CCTV (launched in 2009) and the power Al Jazeera demonstrated when covering the Arab Springs. The Global South had its own narrative about the
transformations challenging traditional power structures and longstanding instruments of US soft power like CNN were losing global presence. Ironically, Clinton’s White House candidacy ended up falling victim to this information war and the central role online tools and discourse played in deciding the outcome of the 2016 US elections.

Since the pandemic infodemic broke out, the magnitude and speed of this transition have increased the feeling not only of vulnerability but of both the United States and the European Union losing influence, as they have felt compelled to rethink their roles amid the new dynamics of political and technological power.

The internet has been the great multiplier of this process of hegemony loss in the global discourse, as the United States must face its own tactics being deployed by Russia and China, the new political, economic and security allies of much of the Global South. Paradoxically, the hybrid threats challenging Washington’s spheres of influence are deployed via the large platforms that have globalised the power of Silicon Valley.

Through the varied ways it uses technology, geopolitics is shaping the information society. As General Slipchenko foresaw, a conflict is underway in this information space not only because of a power struggle, but because of a clash between the models that shape it. Words carry implicit mental frameworks and specific values. That is why they have become the hybrid weapon in this conflict. Disinformation provides fertile space for influence to the new state and private actors that are increasingly decisive in the power struggle underway in the new digital global order.

**References**


Freedman, Jane; Hoogensen Gjørv, Gunhild and Razakamaharavo, Velomahanina. «Identity, stability, Hybrid Threats and Disinformation», ICONO 14, Revista de comunicación y tecnologías emergentes, vol. 19, no. 1, June 2021, pp. 38–69

Han, Byung-Chul. *Infocracia. La digitalización y la crisis de la democracia*, Penguin Random House, April 2022.


