KATARÍNA KLINGOVÁ

Information operations

Information and data are the new driving forces and currency of modern times and warfare. Spreading particular (dis)information and waging information operations can be equivalent to firing a missile. Disinformation is a cheap and more subtle form of influencing operations or hybrid threats. Various malign and disinformation narratives targeting whole societies or a specific audience, among others, undermine democratic processes and trust in institutions or increase the polarisation of society. The full-scale invasion of Ukraine by Russia went hand in hand with the Kremlin's intensive and large-scale information operations waged not only in Ukraine, but also in Europe and in numerous other countries around the world. Regulation of social media platforms, increased transparency of media ownership and limitations of advertising are legislative initiatives driven by the EU. Whether these measures, including the adoption of the new Code of Practice on Disinformation, will reduce the impact of information operations remains to be seen.

Spreading disinformation, smear campaigns or waging various information operations is not a new phenomenon. Lying is as old as time and various scholars have theorised the use of information manipulation since antiquity. Among them are Plato's *Dialogues*, Aristotle's *Rhetoric*, Pascal's *Art of Persuasion* and Arthur Schopenhauer's *The Art of Being Right*.[1]

With the development of television and radio, state actors have increasingly utilised information operations and propaganda in the 20th century. One of the most successful state disinformation campaigns, which still resonates with various audiences worldwide, was the KGB Operation *Infektion* in the 1980s. The USSR and its allies spread the narrative that the HIV/AIDS virus was man-made and invented as a part of a research project on biological weapons at a US Army installation in Maryland. The aim of the operation was to sow distrust towards the US, foster anti-Americanism, isolate the US abroad and cause tensions in countries with the presence of US military bases, which were often portrayed

[1] Jeangène Vilmer, J.-B., A. Escorcia, M. Guillaume et al. (2018) "Information manipulation: A challenge for our democracies". Policy Planning Staff of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces.

as the cause of AIDS outbreaks in the local populations.[2] The development of new information communication technologies, social media platforms and internet access have, however, significantly increased the speed with which propaganda and disinformation are disseminated within societies. A widely accepted typology of Claire Wardle and Hossein Derakhshan differentiates between three forms of false information based on the intent of actors that disseminate the messages:

- *misinformation*: when the information is not true, but it is not created and shared with the intent of doing harm;
- *disinformation*: when untrue content is created and shared with the intent of doing harm; and
- *malinformation*: when the information that is based on reality is used to inflict harm on a person, organisation or country. (The authors include some types of hate speech and harassment under the category malinformation, as people are often targeted because of their personal history or affiliations. For example, when private information is made public or when people's affiliations, like their religion, are used against them).[3]

Furthermore, the Covid-19 pandemic has been accompanied by what the World Health Organization (WHO) describes as 'infodemic':[4] an information chaos brought on societies through the accelerated dissemination of misinformation, disinformation and all kinds of conspiracy theories, which have had devastating consequences on individual lives and societies.

Information operations are one of many tools used within hybrid threats or foreign information manipulation and interference (FIMI).[5] They include, among others, the spread of disinformation and propaganda; the systematic suppression of information and internet takedowns; the manipulation of social media platforms and the use of their algorithms to create information bubbles that are polarising society and inciting hate against societal groups. In addition, paid advertisement and targeted content; hack-and-leak operations during electoral processes; threats and harassment against various members of society, including journalists, political opponents and representatives of civil society organisations, are used in information operations.[6]

Investigations of national security authorities and the work of numerous researchers have provided evidence that malicious and authoritarian (foreign) state and non-state actors, such as Russia, China, Turkey and Saudi Arabia, have spread disinformation, conducted information operations and deployed other interference tactics to influence democratic processes in the EU and other parts of the world, including Africa and Latin America. As Peter Pomerantsev wrote in his book *This Is Not Propaganda: Adventures in the War Against*

[2] Boghardt, T. (2009) "Operation Infektion: Soviet bloc intelligence and its AIDS disinformation campaign". *Studies in Intelligence*, 4(53), pp. 1-24.

[3] Wardle, C. and H. Derakhshan (2017) "Information disorder: Toward an interdisciplinary framework for research and policy making". Council of Europe Report DGI(2017)09.

[4] 1st WHO Infodemiology Conference. Online, 30 June and 1, 7, 9, 14 and 16 July 2020.

[5] "Tackling disinformation, foreign information manipulation & interference". European External Action Service, 27 October 2021.

[6] Kalniete, S. (2022) "Report on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI))". European Parliament, 8 February.

Reality, while autocratic regimes once controlled the narrative by silencing opponents, now they seek to confuse their populations by bombarding them with false information, half-truths and competing narratives. It is a strategy that Pomerantsev describes as "censorship through noise".[7] Individual countries, or institutions such as the EU, consider these FIMI activities as violations of international law, aiming, for example, to manipulate and deceive citizens and affect their voting behaviour; divide, polarise and exploit the vulnerabilities of societies; and sow distrust in national governments and public institutions, and thus, democratic processes. FIMI, therefore, constitutes a severe threat to the security and sovereignty of individual states as well as international organisations, such as the EU and NATO.[8]

One of the most eye-opening cases of state-funded subversive efforts in the past few years was Russian interference during the 2016 US presidential election. According to Facebook's testimony at the US Senate,[9] Russia's information operations with Kremlin-planted ads and fraudulent posts, only on Facebook, reached more than 126 million users in the US.[10] Furthermore, researchers at the Oxford Internet Institute, who analysed over 19 million posts on Twitter before the US presidential election, found high automatisation (and thus, inauthenticity) of the most active accounts. According to this research, the 100 most active Twitter accounts posted an average of 500 tweets per day.[11] These tweets, polarising US society, spreading false information about election fraud and supporting particular candidates, were disseminated by networks of bots on Twitter.

In addition, the Kremlin used hackers to get hold of the Democratic party's emails and its media and propaganda[12] machinery, including RT and Sputnik, to wage a smear campaign against Democratic representatives and Hillary Clinton, who was the Democratic presidential candidate. Similar methods of Russian information operations were observed during elections across numerous EU countries, including in the French presidential elections, the 2021 German federal election and the Brexit referendum. Ironically, it is the openness of democratic institutions and society that have provided various venues and tools for malign domestic or foreign actors to undermine democracy.

[7] Pomerantsev, P. (2019) *This Is Not Propaganda: Adventures in the War against Reality* (New York: Public Affairs).

[8] Kalniete, S. (2022) "Report on foreign interference".

[9] Committee on the Judiciary (2017) "Extremist content and Russian disinformation online: Working with tech to find solutions". US Senate, 27 October.

[10] Solon, O. and S. Siddiqui (2017) "Russia-backed Facebook posts 'reached 126m Americans' during US election". *The Guardian*, 31 October.

[11] Kollanyi, B., P. N. Howard and S. C. Woolley (2016) "Bots and automation over Twitter during the U.S. election". Project on Computational Propaganda, Data Memo 2016.4.

[12] For the purpose of this paper, the term 'propaganda' is understood as the dissemination of information – facts, arguments, rumours, half-truths or lies – to influence public opinion. Read more in Jack, C. (2017) "Lexicon of lies: Terms of problematic information". Data & Society Research Institute, 9 August.

Incentives to spread disinformation

There are a plethora of reasons why particular people, organisations or states pursue information operations and spread disinformation. Different motivations for pursuing information operations and spreading false narratives depend on whether such activities are conducted by state-sponsored or state-led actors, or if it is insurgent disinformation disseminated by non-state actors.

Information operations pursuing *geopolitical goals* are usually the most insidious; they require multiple actors and tools and can be conducted for years or even decades. A historic example is the USSR's propaganda campaign during the Cold War in Eastern Europe. The goal of geopolitical and subversive information operations or propaganda could be the creation of a sphere of influence, the projection of power, change of the political orientation of a country, delegitimisation and corrosion of state institutions or the creation of a so-called fifth column within a country.[13]

Politically motivated disinformation is pursued by particular individuals, groups, political representatives or even foreign subversive actors with the aim of provoking domestic conflict or spreading particular narratives to promote their cause, to delegitimise a particular politician or political party or to influence public debate. While smear campaigns or attempts to discredit opponents are common and normal in politics, the utilisation of inauthentic social media accounts, pretending to be ordinary people or the use of paid supporters and commentators have become increasingly normalised. Automated networks of bots and armies of trolls might systematically produce a particular point of view. This can create a bias perception, suggesting that there is organic grassroots support for a given candidate, while, in reality, it is all artificially generated.

Another motivation to conduct information operations is an attempt to persuade a selected audience or nation to adopt the ideological worldviews of the propagator. Convincing the masses of one's own ideology or dogma has always been part of every political, religious or societal system. The ability to achieve this by peaceful means and in a way that the recipients of the message give up their values and adopt those of the foreign actor is the ultimate goal of hybrid threats.[14] Access to the internet and information communication technologies became, for example, perfect tools for operations and recruitment for right-wing or Islamic extremist groups.[15]

The spread of disinformation is also a lucrative business model. For actors producing disinformation, for social media platforms and other companies providing services to amplify malign and polarising content, the hope for financial gain is among the incentives for spreading disinformation and conspiracy theories.

[13] A clandestine group or faction of subversive agents who attempt to undermine a nation's solidarity by any means at their disposal, usually in favour of an enemy group or another nation.

[14] For more information on hybrid threats/war, see: Giannopoulos, G., H. Smith and M. Theocharidou (2020) "The landscape of hybrid threats: A conceptual model". European Commission, Ispra, PUBSY No. 123305.

[15] Lia, B. (2007) "Al-Suri's doctrines for decentralized Jihadi training – part 1". *Terrorism Monitor*", 1(5), pp. 1-11.

The interest of social media platforms is to keep their users on the platforms for as long as possible. As a result, massive amounts of personal data are used and monetised in the social media business model solely based on advertising. Harvard Professor Shoshana Zuboff refers to this trend as the "age of surveillance capitalism".[16] In 2021, Facebook earned $114 billion from ads.[17]

Disinformation websites, as social media platforms, use 'clickbait': content attracting attention and encouraging visitors to click on a link to a particular web page and online advertising. PR experts estimate that approximately 60% of the revenue generated by ads goes to owners of websites. According to the Global Disinformation Index, in 2019, approximately $235 million of advertising ended up on 20,000 domains flagged for disinformation.[18]

Various companies or individuals that provide services of paid trolls, false followers or automated bots, in order to promote particular content or to generate likes or reshares, are equally attracted by potential gains. The NATO Strategic Communication Centre of Excellence, in cooperation with the Ukrainian social media analytics company Singularex, mapped the online market for social media manipulation tools and services. Their research revealed a thriving black-market infrastructure for generating fictitious accounts and providing various proxies. This market and its services are open and accessible – just a few clicks away from their potential customers – and often promoted via advertisements on internet search engines or social media platforms. This research also found that Russian service providers seemed to dominate this social media manipulation market.[19]

All this contributes to a huge industry, with giant political-economic profits, dedicated to intentionally fuelling disinformation. Therefore, the regulation of big tech platforms and social media companies is necessary. The EU has launched a series of legislative processes and initiatives, including the Digital Services Act, the Digital Markets Act and the new EU Code of Practice on Disinformation, aiming to establish accountability, algorithmic transparency, and the openness of advertising patterns and business models of big-tech companies. The EU is thus establishing oversight of and enforcement mechanisms for social media platforms. The recent layoffs at Twitter, Meta and other big-tech companies, however, raise concerns for whether these social media platforms will be able to comply with new EU regulation.[20]

[16] Kavenna, J. (2019) ″Shoshana Zuboff: 'Surveillance capitalism is an assault on human autonomy'". *The Guardian*, 4 October.

[17] Dixon, S. (2022) ″Meta: Advertising revenue worldwide 2009-2021". Statista, 27 July.

[18] „The quarter billion dollar question: How is disinformation gaming ad tech?". Global Disinformation Index, 1 September 2019.

[19] NATO StratCom COE and Singularex (2019) "The black market for social media manipulation". NATO Strategic Communications Centre of Excellence.

[20] Lomas, N. (2022) "Twitter layoffs trigger oversight risk warning from Brussels". TechCrunch, 24 November.

The Kremlin's disinformation and propaganda machinery

Since the collapse of the Soviet Union, the Kremlin, aiming to restore its regional supremacy and weakening the West, has been successfully waging information operations. Among the narratives it uses is that of a decadent, liberal West, which is falling apart. Other narratives depict the West as trying to destroy the traditional values of certain countries or calling for the cooperation of Slavic countries. The Kremlin, its media machinery and various pro-Kremlin actors have been exploiting various polarising and sensitive issues, such as migration, the Covid-19 pandemic and the impact of the war in Ukraine – inflation, increased prices of food and energy, and hunger in various regions of world – to discredit and undermine western democracies. For many years, Russian representatives have been accusing western and US operations of being responsible for a deteriorating security environment and international relations. In addition, Russia portrays itself as a victim that is unjustly accused by the West or as the protector of small nations.

In 2020, the US Department of State's Global Engagement Center (GEC) outlined the five pillars of Russia's disinformation and propaganda ecosystem: 1) official government communications; 2) state-funded global messaging; 3) the cultivation of proxy sources; 4) the weaponisation of social media; and 5) cyber-enabled disinformation. This machinery reflects both the sources of disinformation and the tactics used by the Kremlin. Its backbone is, however, state-controlled media, TV and news agencies, with RT (formerly Russia Today) and Sputnik being the most important of these state-funded global messengers.[21] In 2021, the budget for the Kremlin's media machinery was more than $1.5 billion. Furthermore, in the first quarter of 2022, it was tripled in comparison to the same period in 2021.[22]

RT is a multilingual network of television stations, websites and social media channels operating in six languages (English, Spanish, French, German, Arabic and Russian). It serves as a Russian state-controlled media agency and political influence tool in the world. Its budget in 2022 was more than $350 million. RT, with its social media accounts, has become a popular source of information in Latin America, especially during the Covid-19 pandemic: RT's Spanish-language Facebook page has more followers than the English one. In November 2022, RT Balkan was launched in Serbian. Another avenue targeting foreign audiences is the international news service Sputnik. It runs radio broadcasts, websites and social media channels in more than 30 languages. By October 2022, the East StratCom Task Force of the European External Action Service had debunked over 14,000 articles from disinformation websites tied to the Kremlin on its EUvsDisinfo database.[23]

According to the US Department of State, apart from its media machinery, Russia has also spent over $300 million since 2014 on covert information operation operations

[21] US Department of State Global Engagement Center (2022) "Kremlin-funded media: RT and Sputnik's role in Russia's disinformation and propaganda ecosystem". GEC Special Report, January.

[22] Michałowska-Kubś, A. and J. Kubś (2022) "Coining lies. Kremlin spends 1.5 billion per year to spread disinformation and propaganda". Debunk.org, 8 August.

[23] "Disinfo database". EUvsDisinfo.

in Europe, with Brussels being identified as a "hub for foundations and other fronts" to support various political representatives with pro-Russian affinity.[24] In recent years, various political parties and their representatives were revealed to have close ties to the Kremlin or Russian oligarchs, including Marine Le Pen and her National Rally party, Italy's Matteo Salvini with his far-right League party[25] and Viktor Orbán, who was described in the past as the Kremlin's Trojan horse in the EU.[26] In 2022, several Bulgarian politicians, as well as other opinionmakers, including prominent journalist and analysts, were paid by the Kremlin for spreading propaganda and malign narratives, according to the Bulgarian secret service.[27]

In recent years, an increasing number of domestic political parties and their representatives have been taking on board pro-Russian narratives and spreading various polarising narratives that are undermining democratic processes. Indeed, Donald Trump, Nigel Farage, Matteo Salvini, Viktor Orbán and other populist, far-right or anti-system politicians have been effectively spreading disinformation, pro-Russian narratives or malign narratives at the centre of public debate in various countries. Believers in various conspiracy theories, disinformation and polarising narratives have thus moved from the fringes of the information environment to prime-time debates.

In September 2022, EU DisinfoLab, a Belgian NGO analysing and countering disinformation, reported on an 'operation Doppelganger', an information operation during which the websites of at least 17 media providers, including the German tabloid *Bild*, French newspaper *20minutes*, Italian news agency Ansa, UK newspaper *The Guardian* and news agency RBC Ukraine, were cloned using very similar internet domain names and used to spread pro-Russian war propaganda and disinformation, targeting both Ukraine and the West. False content from the Doppelganger websites was further amplified via false accounts of these alleged media on various social media platforms. This cross-platform information operation, which impersonated authentic and investigative media, also focused on instigating fear in the populations of Germany, Italy, France, Latvia and the UK that sanctions against Russia would ruin their lives.[28]

Another avenue through which the Kremlin attempted to influence public opinion in western European countries was various influencers. In 2021, several French and German YouTubers and bloggers were approached by the allegedly UK-based PR agency Fazze to spread false information about the Pfizer/BioNTech vaccine among their followers, and thus, discourage them from being vaccinated. Researchers eventually found out that the alleged PR agency was tied to a Russian entrepreneur.[29]

[24] "Russia covertly spent $300 million to meddle abroad - US". BBC, 10 October 2022.

[25] Horowitz, J. (2019) "Audio suggests secret plan for Russians to fund party of Italy's Salvini". *NY Times*, 10 October.

[26] Coackley, A. (2022) "Putin's Trojan horse inside the European Union". Foreign Policy, 3 August.

[27] Nikolov, K. (2022) "Bulgarian secret services: Russia pays public figures to spread propaganda". EurActiv, 4 July.

[28] Alaphilippe, A., G. Machado, R. Miguel et al. (2022) "Doppelganger – media clones serving Russian propaganda". EU DisinfoLab, 27 September.

[29] Henley, J. (2021) "Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine". *The Guardian*, 25 May.

In March 2022, in the wake of the Russian invasion of Ukraine, the EU took the unprecedented measure of suspending five Russian state-owned outlets (Sputnik, Russia Today, Rossiya RTR, Rossiya 24, TV Centre International) from broadcasting into its territory;[30] these outlets were just a few actors in a well-oiled propaganda machinery and widespread networks of pro-Russian websites and actors operating at national and international levels. Although these outlets' websites and TV channels were blocked in the EU, their activities remained unchanged in other parts of the world, including the Western Balkans. The impact of such takedowns can thus be questioned and requires further investigation.

The war in Ukraine and the impact of year-long information operations

Russia was waging various information operations against Ukraine, even before the annexation of Crimea or the occupation of the eastern part of Ukraine in 2014, undermining the legitimacy of the Ukrainian government and distorting citizens' trust towards it. These operations were accompanied by narratives depicting the West and the US as 'bloodthirsty' and needing to wage war to secure their economic primacy, and narratives accusing Ukraine of conducting a genocide against the country's Russian-speaking minority and being a Nazi nation.

The EU has blocked five Russian outlets and some member states have actively taken down or blocked numerous disinformation outlets spreading the Kremlin's war propaganda. However, the impact of Russia's long-term information operations on public perceptions in Central and Eastern Europe (CEE) or in countries of the Western Balkans is visible, especially when it has been systematically eroding citizens' trust in public institutions and democratic processes.

In 2018, a flash Eurobarometer on fake news and disinformation revealed that 85% of respondents believed fake news to be a problem in their country and 83% perceived false or misrepresentative information as a problem for democracy.[31] A survey conducted by Ipsos Public Affairs and the Centre for International Governance Innovation in 2019 found that, due to the spread of disinformation, many citizens have less trust in media (40%) and government (22%). Furthermore, 83% of respondents agreed that disinformation had a negative impact on their country's politics and political discussions.[32]

The impact of information operations and pro-Russian propaganda in CEE was also revealed after the Russian invasion of Ukraine. While for a majority of central and eastern Europeans the February invasion was a wake-up call, and now they perceive Russia as a security threat, 30-40% of the CEE population remains vulnerable to the Kremlin's

[30] European Commission (2022) "EU sanctions against Russia explained".

[31] European Commission, Directorate-General for Communications Networks, Content and Technology (2018) "Fake news and disinformation online". Publications Office of the European Union.

[32] Ipsos Public Affairs and Centre for International Governance Innovation (2019) "CIGI Ipsos Global Survey: Internet security and trust".

propaganda and information operations.[33] A well-established network of pro-Kremlin actors, including domestic political representatives, social media pages and malign websites, are successfully disseminating Russian war propaganda and disinformation in central Europe. According to Detector Media, a Ukrainian NGO, Kremlin war propaganda and disinformation about Ukraine have been successfully spread, especially in Hungary, Slovakia and Poland.[34] Furthermore, increasing apathy for the war in Ukraine, rising social and economic implications of the war for EU societies, as well as the Kremlin's information operations are slowly undermining support for Ukraine and Ukrainian refugees. In August 2022, 32% of respondents in Germany thought their country providing weapons to Ukraine went too far,[35] but, so far, support for Ukraine remains stable among Germans, despite the rise in energy prices. On the other hand, rising energy prices are undermining support for Ukraine in the Netherlands.[36] In Slovakia, where 37% of respondents still considered Russia to be a strategic partner after the invasion in February, one fifth of the population preferred Russia to win the war, and 24% of respondents did not care when asked the question "how would you want the war in Ukraine to end?" in September.[37]

Rising anti-government protests in central Europe organised, among others, by people with connections to the Kremlin underscore the fact that domestic politics pose a parallel battlefield for the war in Ukraine. Addressing domestic issues and social policies is as important as maintaining a united foreign policy front and support for Ukraine. Therefore, the information war for 'hearts and minds' in the EU and beyond is far from over.

Ukraine fights back

The success of Ukrainian efforts to counter Russian information operations in Ukraine surrounding the full-scale invasion in February is closely tied to prior systematic investments in public infrastructure, the capability building of Ukrainian civil society since the annexation of Crimea in 2014 and a mobilisation of the entire population. As targets of intensive smear and disinformation campaigns, the political leadership of Ukraine has understood the importance of good strategic communication by public institutions, building societal resilience and an approach concerning the entire population in the fight against disinformation. The Ukrainian Centre for Countering Disinformation, of the National Security and Defence Council, the Ministry of Culture and the Information Policy's Centre for Strategic Communications, along with President Volodymyr Zelensky and his office, have

[33] Hajdu, D., K. Klingová, J. Kazaz et al. (2022) "GLOBSEC trends 2022: CEE amid the war in Ukraine". GLOBSEC, 31 May.

[34] Detector Media (2022) "Ukrainian Nazis for the Czech Republic, bio laboratories for North Macedonia, and Russophobia for Georgia. Analysis of Russian propaganda in 11 European countries". 12 September.

[35] Statista (2022) "Opinion on German government's policy on the war in Ukraine August 2022".

[36] DG Communication's Public Opinion Monitoring Unit (2022) "Public opinion on the war in Ukraine". European Parliament, 6 October.

[37] Klingová, K. and D. Hajdu (2022) ″New poll: Slovaks want Ukraine to win the war, not Russia". GLOBSEC, 5 October.

been leading strategic communication and counter-disinformation activities at the state level. In addition, each ministry has a special unit focusing on strategic communication. However, it was the years-long activities of civil society organisations, researchers, journalists and activists that made a big difference in the increase of Ukraine's resilience between 2014 and 2020.

Russia's full-scale invasion of Ukraine, coupled with the spread of narratives of a "special operation" and the need to "de-Nazify" Ukraine, has dehumanised 45 million Ukrainians, resulting in a Ukrainian 'no surrender' and 'fighting till the end' mentality. The all-hands-on-deck approach of Ukrainian society, which was not an easy target of the Kremlin's propaganda, resulted in Ukrainian strategic communication and countermeasures being compared to a tireless beehive. From powerful videos of citizens fighting back against occupiers and providing important logistical information on the movement of Russian soldiers to stories of soldiers on the frontlines; real-time evidence of atrocities conducted by Russian soldiers; and President Zelensky regularly addressing his fellow Ukrainians and the international community, despite being bombed – all these stories, pictures and videos have showcased the Ukrainian determination. Everyone became a communicator and witness to the Kremlin's atrocities and war crimes in Ukraine.

With support from the international community and big-tech companies, Ukraine was able to take down Russian trolls, withstand cyberattacks and successfully communicate its narratives and achievements to both its citizens and the wider international audience. Videos or recordings of telephone conversations of captured Russian soldiers calling their families, who often did not know that their relatives were deployed and fighting in Ukraine, as well as recordings of phone calls of Ukraine officials informing Russian families that their sons had been killed, revealed the information bubble and impact of the Kremlin's propaganda on its own domestic population. They have been an important part of Ukraine's psychological tactics.

Creative content produced by both Ukrainian citizens and public channels showed the importance of humour for the morale of the whole society. Trolling the enemy and its trolls has been an important element of Ukrainian information operations, often supported by armies of 'elves'.[38] And while the Kremlin has used a plethora of tools in an attempt to discredit Ukrainian political leaders, including AI-generated deepfake videos of President Zelensky surrendering, Ukrainians are still standing strong in the information operations' battlefield of the war.[39]

While Ukraine and the West might be winning the battle of narratives in Europe and the wider transatlantic community, the Kremlin has used its propaganda machinery to undermine international order and confuse audiences in numerous countries of the Global South about its actions in Ukraine.[40] As the war in Ukraine continues, it is necessary to understand and address its various battlefields.

[38] Abend, L. (2022) "Meet the Lithuanian 'elves' fighting Russian disinformation". *Time*, 6 March.

[39] Wakefield, J. (2022) "Deepfake presidents used in Russia-Ukraine war". BBC, 18 March.

[40] Flores-Saviaga, C. and D. Guerrero (2022) "In Latin America, fact-checking organisations and cross-regional collaborations attempt to counter Russia's disinformation". Power3.0, 6 July.