THE EVOLUTION OF SOCIAL MEDIA PLATFORMS AS INSTRUMENTS OF PROPAGANDA, DISINFORMATION AND MEDIA SUBVERSION IN MODERN CONFLICTS

George-Adrian AIONESEI

"Henri Coandă" Air Force Academy, Brasov, Romania

Over the past two decades, social media platforms have evolved from simple means of communication into critical infrastructures of modern conflicts. Existing literature has documented the roles of propaganda, disinformation and media subversion, but often through isolated case studies (Gaurino, et al. 2020) or one-dimensional analyses (Marigliano, Hui Xian Ng and Carley 2024). Although valuable, these approaches fail to capture the evolutionary dynamics and interconnections of these phenomena across time and space. On this matter, this article proposes a comparative analysis of six key-events in recent history: jihadist propaganda in Iraq and Afghanistan, the mobilizations during the Arab Spring, the hybrid campaign in Ukraine (2014), the U.S. presidential elections (2016), the COVID-19 infodemic, and the full-spectrum information warfare between Russia and Ukraine. This article is intended to offer an evolutionary comparative framework of disinformation, propaganda and media subversion, with both academic and practical values.

Key words: *social media, disinformation, propaganda, media subversion, modern conflicts.*

1. INTRODUCTION

Once Russia's full-scale invasion of Ukraine started in February 2022, the world witnessed not only a conventional military conflict, but also the emergence of the digital domain as a central component of warfare. On social media platforms, millions of users around the world followed in real-time videos and posts presenting military convoys, missile attacks and strong emotional reactions. Both sides disseminated contradictory narratives through pro-Russian and pro-Ukrainian channels, manipulated images, stories and rumors at an uncontrollable pace, making the phenomenon difficult to manage. For the first time, social media platforms were more than

secondary means of communication; they were a central battleground, where public opinion has become a strategic target.

This new reality was not a technological revolution, but an evolution, where different situations added to social media platforms new dimensions, tactics and strategies (Benkler, Faris and Roberts 2018). In the era of traditional mass media, where propaganda was linked more to state actors and centralized channels, social networks changed this dynamic and created opportunities for multiple actors to participate, including civic movements, terrorist organizations or authoritarian governments. Traditional propaganda, viewed by Ellul (1965) as a systemic process of shaping opinions, was redefined in modern times. It is no longer acting vertically, from the powerful elite downwards, but also generates horizontal and viral narratives across all user levels (Bösch and Divon 2024). Nowadays, there are no issues regarding who produces the messages, but rather the ways used by media entities and partisan networks to create fertile environments for content amplification and polarization.

Disinformation, a phenomenon that took multiple forms throughout history (Rid 2020), can be simply defined as the deliberate creation and dissemination of false content for strategic purposes. It has become one of the main interests in information research, especially after 2016, when there was a massive interference in the US presidential elections (Vosoughi, Roy and Aral 2018) (Howard, Woolley and Calo 2018). More recently, the COVID-19 pandemic demonstrated that disinformation affects not only politics, but also other aspects of everyday life, such as public health and social trust (Ferreira Caceres, et al. 2022). Disinformation can be analyzed from different points of view, such as the actors that disseminate it and the impact that it has on people. When we think about actors, there are studies that show that digital bots and automated networks play an essential role in accelerating the spread of false information (Zannettou, et al. 2019) (Chengcheng, et al. 2018), and other studies that show the opposite, that humans themselves are the ones that spread false content more, because they find it more attractive, shocking and impactful than fact-checked information (Vosoughi, Roy and Aral 2018). Switching to the impact that disinformation might have on people, studies such as of Ferreira et al. (2022) present clear effects on trust in public institutions and on health system.

If propaganda focuses on persuasion and disinformation on deception, media subversion aims to manipulate the truth in order to control and erode the functions

of main institutions in a state. Researchers such as Pomerantsev (2019) or Rid (2020) emphasize the idea that in current times, the main objective of information operations is not necessarily to convince, but rather to spread confusion and cynicism, creating an appropriate environment for narrative domination. One of the best strategies in this regard is the *firehose of falsehood*, attributed to Russia's strategic actors. They do not seek coherence, but saturation and repetitiveness, flooding the information space with so much content that users can no longer distinguish between truth and falsehood.

These phenomena are an important element of the social media platforms today, they mediate them; each platform shapes content flows and the methods used for propaganda and disinformation. For example, TikTok uses its algorithmic feed and focus on short-form video content to enforce emotional reactions and to weaponize audio-visual narratives in conflict. The encrypted channels and fast-spreading mechanisms of Telegram are the ideal infrastructure for coordinated campaigns to control digital communities, whilst Twitter (X) remains a relevant public visibility space. These approaches of different platforms demonstrate that there are no universal formula for digital propaganda, and that its techniques work to the extent that they align with the attention architecture and community rules of each platform (Marino 2024) (Schrijver 2025). This system where the three phenomena are involved must keep pace with the latest technology in order to be effective and efficient, therefore there is a new dimension that needs to be taken into account: artificial intelligence and synthetic content. If initially deepfakes (Atlam, et al. 2025) were generating sparks of alarmism, recent studies (Diel, et al. 2024) (Ching, et al. 2025) show that their impact mostly depends on the audience biases and context. When spreading around key events, such as elections, they can destabilize and create confusion around users, however, their effects intensify where trust is already fragile. From this perspective, AI and its products (e.g., deepfakes) do not fundamentally change the way information operations work, but rather amplify existing vulnerabilities in the digital space.

Another aspect that is constantly changing lies in digital regulations. The European Union, through the Digital Services Act (DSA), and the Code of Conduct on Disinformation, introduced mandatory mechanisms for transparency and online responsibility, yet EDMO reports (Botan and Trisha Meyer 2025) show that there is a significant gap between norms and their application, while NATO StratCom Center of Excellence

emphasizes the capacity of both state and non-state actors to adapt faster to changes than regulatory frameworks. All these adaptations in real time and the applicability of norms push the actors to constantly find new ways and tactics that can be used in digital operations.

All these aspects put together create a broad picture of what digital environment has become over the last few years, and also it raises a question of *How have social media platforms evolved to become the strategic instruments in modern conflicts?* There are no straightforward answers for this, yet it has become clearer that propaganda, disinformation and media subversion cannot be treated as separate phenomena, but rather as a range of interconnected practices that overlap and complete one another. Another important aspect is that all these phenomena do not concern only the content's value of truth, but the focus is directed more on the institutions, the place where information gets validated, channels it goes through and what techniques are appropriate for what audience. Also, each phase of social media evolution added a new layer of sophistication, instead of entirely changing the way information operations unfold. What once served as an environment for civic interactions has been transformed into a conflictual informational space, where the rush for attention, high intensity emotions and polarization shape the stability of current society.

2. COMPARATIVE ANALYSIS

In order to have a clearer picture of the way social media platforms have evolved into the instruments of propaganda, disinformation and media subversion as we know it today, we will use the comparative analysis method. The choice of this method is grounded in the very nature of the object of study: the phenomenon cannot be understood by analyzing a single case, but only by comparing multiple historic moments throughout past years that served as milestones regarding social media implications in modern conflicts. In this regard, we are able to capture both, what is specific for each event and the continuities that shape an evolutionary path.

For this comparison, we chose six representative cases: the jihadist propaganda in Iraq and Afghanistan (2003-2010), civilian mobilization during Arab Spring (2011), hybrid campaigns in Ukraine (2014), online interference during US presidential elections (2016), infodemic during COVID-19 (2020) and full-spectrum informational warfare in Ukraine (2022-2025). All of these were chosen based on three main criteria:

- Historical relevance – each event marked a significant change in the use of social media;

- Contextual diversity – the cases cover different situations – from conventional conflicts to hybrid warfare, up to political and worldwide health crises. This variety of situations emphasizes continuous adaptability of social media;
- Documentary availability – the selected episodes were well documented because of their importance for each period, providing a solid analysis.

In this sense, we opted for a comparative analysis between key-events, guided by an analytical matrix, approaching dimensions inspired both from earlier studies and from contemporary debates regarding informational security: *conflictual context, dominant platforms, main actors involved, tactics, target audience, impact on social cohesion, institutional responses* and lastly *evolutionary stage*. This structure offers a comparative framework that goes beyond the descriptive style and focuses more on pattern identification, and also, encompasses the complexity of this phenomenon on every layer, from the geopolitical context to the social and institutional effect. This approach allows us to articulate an evolutionary narrative and highlights the ways in which conflicts and crises have reshaped the use of social media instruments. This helps to view social media differently, from a simple passive communication environment, to a strategic vector that transforms from one situation to another.

Conflictual context is a mandatory element, since neither propaganda nor disinformation operate randomly in a vacuum. Classical literature (Lasswell 1938) and current one (Benkler, Faris and Roberts 2018) show that the nature of the conflict, either conventional, hybrid or global, determines the way social media instruments are used. When we refer to an insurgent warfare, a protest movement or a global sanitary crisis, we also refer to the reasoning of what platforms become dominant and why specific informational tactics are preferred over others.

The second dimension of the matrix consists of the **dominant platforms**, because each social network has its technical and cultural characteristics, which for the most part conditions the flow of content. Recent studies show that TikTok promotes emotional behaviors (Bösch and Divon 2024), or that Telegram creates confused and decentralized information campaigns (Schrijver 2025). These environments have their own logic, presenting the fact that algorithms, networks and norms can drive to different results even though they are being used the same way.

A third dimension is represented by the **main actors** that use these platforms. Studies from Oxford Internet Institute (Bradshaw and Howard 2019) (Howard, Ganesh and Liotsiou 2019) highlighted that various actors involved in campaigns (state, non-state or hybrid) approach differently the coordination of resources for the same objective. State-sponsored troll farms, decentralized networks such as ISIS or spontaneous civic movements differentiate through strategies and capabilities, based on the actors involved, which justifies their part in this analysis.

Disinformation, propaganda and subversion cannot be possible without the use of specific **informational tactics** by these actors. Academic literature (Vosoughi, Roy and Aral 2018) (Chengcheng, et al. 2018) has shown that fake news spreads six times faster than the fact-checked news, due to the use of cognitive and emotional tactics, and most importantly the use of automated networks. Additionally, tactics have become layered: from rudimentary audio-video messages and influencing forums, to memes, micro-targeted elections, viral conspiracies and artificial intelligence deepfake content.

Also, this study needs to focus on **target audience** in order to justify the effort of the actors. This dimension derives from the psycho-social literature on persuasion and polarization (Pasquetto, Lim and Bradshaw 2024) (Yang, et al. 2021). Disinformation and propaganda are chose based on the audience predisposition such as: local combatants, global population, political elite, institutional parties. The evolution of all cases, based on other dimensions too, shows a clear shift from small audiences to global masses, fact that amplifies more and more the complexity of the phenomena.

The sixth dimension defines the **impact on social cohesion**, which represents the objectives to attain through the other dimensions. Pomerantsev (2019) and Rid (2020) highlight that the central objective of current informational operations goes beyond the mere persuasion, but rather on controlling the population, undermining collective trust and diminishing the trust in legitimate institutions. Measuring this impact is not easy, but is mandatory to understand the effect on political and social stability in the long term.

After impact, there come the **institutional responses**, which constitute a crucial variable. As Carnegie Endowment (Bateman and Jackson 2024) or EDMO reports (EDMO 2023) show that technological companies, international organizations and state governments react to disinformation and propaganda campaigns,

supported by subversion techniques, they also reconfigure the war field in order to limit the phenomena. The results are not always what they expect, but rather push the aggressors toward new and more sophisticated alternatives.

Finally, the **evolutionary stage** dimension integrates the others above into a chronological and comparative frame. Its role is to describe the shift from the rudimentary dissemination (broadcast), to civil mobilization (weaponization) and ultimately to full cognitive battlespace. This dimension shows a longitudinal evolution, focusing on how each case not only reflects a particular moment, but also adds a new layer to the digital threats.

The eight dimensions are not chosen randomly, but emerge from an integration of multiple literature sources, which helps construct a methodological framework, capable of capturing the evolution of the social media phenomena shown below Table 1.

Based on this matrix, the six case studies will be analyzed in order to identify and understand how social media has evolved and how propaganda, disinformation and media subversion have grown to the phenomena that define the informational warfare today.

Table 1 Comparative analysis matrix

Dimension	Key-questions / Indicators	Analytical relevance
Conflictual context	- What type of conflict is being analyzed (asymmetric, conventional, hybrid, global)?	Situates digital propaganda, disinformation and media subversion in their historical and geopolitical context.
Dominant platforms	- What are the main platforms used? - What are the key characteristics of the platform? - Were any other platforms involved?	Highlights the role of the platforms in attaining the objective and its relevance for the situation.
Main actors	- Who did create/distributed the content (state, non-state)? - What was the coordination regarding resources?	Clarifies the source/ sources of the content.

Dimension	Key-questions / Indicators	Analytical relevance
Tactics	- What type of content was used (written, video, meme, deepfake)? - What techniques were used (bots, trolls, algorithms, microtargeting)?	Allows the comparison of sophistication levels across cases.
Target audience	- Who was the main target (local, regional, global)? - Why was the target selected?	Shows the evolution from small to global audiences.
Impact on social cohesion	- What were the effects on trust on institutions? - Was there polarization, mobilization, radicalization? - What consequences have been documented?	Shows the links between tactics and final objectives of each case.
Institutional responses	- What was the reaction of the governments? - Have there been any international initiatives?	Assesses the degrees of institutional implication on resilience and adaptation.
Evolutionary stages	- Where does the case fit into: broadcast, mobilization, weaponization, cognitive battlespace?	Integrates each case into a comparative evolutionary framework.

2.1. Afghanistan and Iraq (2001, 2003)

Conflictual context – Afghanistan (2001) and Iraq (2003) wars took place in a geopolitical context dominated by "war against terrorism", launched after 9/11 attacks and were the first global conflicts of the digital era: The USA and other allies were promoting narratives related to democracy and national security, whilst insurgent and jihadist groups were fighting to demonstrate the legitimacy of resistance and recruiting new members.

Dominant platforms – YouTube, jihadist forums, blogs and other independent websites were the main channels for this conflict. The content dissemination was based mainly on open access to forums and viral audio-video materials, rather than sophisticated algorithms.

Actors – *State actors*: The USA and other countries (the United Kingdom, Germany, Australia and

others) used strategic communication campaigns to justify war and maintain the public support. *Non-state actors*: Jihadist groups (Al-Qaeda, and later ISIS) used forums for recruitment and video content dissemination (taped executions, leaders' messages). *Global mass-media*: Al-Jazeera played an important hybrid role, spreading images and messages, that later went online.

Tactics – Jihadist groups introduced propaganda videos and motivational religious messages on a large scale. On the U.S. side, there were digital campaigns focused on positive narratives regarding the intervention and counter-messages against insurgent propaganda.

Target audience – *Local and Regional*: Iraq and Afghanistan population. *Globally*: international jihadist audience for propaganda and recruitment. The USA aimed for the Western countries.

Impact – Jihadist propaganda amplified radicalization and international recruitment fluxes, but at the same time fear and insecurity in the West. In western countries, continuous exposure to violence images led to political polarization and diminishing trust in official justifications of the war.

Institutional responses – The USA and others developed strategic communication programs and counter-narrative initiatives, but most of them were reactive. Social media platforms did not have specific regulations against violent content, and the responses were more of a censorship than a specific strategy.

Evolutionary stage – This case relates more to a *broadcast*, where social media is used as a megaphone for visual propaganda and mobilization messages. Still rudimentary (absence of algorithms) the two conflicts have laid the groundwork for the use of social media instruments.

2.2. The Arab Spring (2011)

Conflictual context – Between 2010-2011, a series of protests unfolded in Tunisia, Egypt, Libya, Syria and other Arab states. The initial purpose was socio-economic (corruption, unemployment), but it switched quickly to political protest movements and civilian conflicts. The geopolitical context was one of authoritarianism where regimes had full control of traditional media.

Dominant platforms – Facebook and Twitter were the main platforms, completed by YouTube with videos. Hashtags such as *#Jan25* became international symbols. In addition to the previous conflicts, the platforms were also used for direct coordination between protesters.

Actors – *Civilians and activists* used platforms for mobilization and protest organization. *Authoritarian regimes* tried to block Internet access. *Mass-media*: CNN, Al-Jazeera

amplified the visibility of protests.

Tactics – The use of hashtags was the new way to synchronize collective actions, spread images and send appeals for international solidarity. The focus was on visual authenticity.

Target audience – *Local* – local population. *External* – international community, for political support and movement legitimacy.

Impact – Social media was for the first time a parallel communication space, that destabilized state control over information. The civilian mobilization expanded rapidly, whilst the state-citizen relations were strongly affected.

Institutional responses – Local regimes tried to block Internet access and the functioning of networks. During that time, platforms still did not have robust mechanisms for moderation and presented the protests with minimal moderation and little censorship.

Evolutionary stage – This conflict marks the *mobilization* phase, where social media becomes an instrument for organization and coordination for people.

2.3. Ukraine – Crimea annexation and Donbas conflict (2014)

Conflictual context – In 2014, Russia annexed Crimea and supported the separatist conflict in Donbas. It was a hybrid confrontation, where conventional and irregular military operations were combined with massive disinformation and propaganda campaigns, aimed at undermining the Ukrainian government and justifying the Kremlin actions. There were also tensions between NATO/EU and Russia, Ukraine being caught in the middle.

Dominant platforms – Facebook, Twitter and VKontakte were the main channels. VKontakte was very popular in the post-soviet space, and was used for aggressive pro-Russian propaganda. Also, YouTube and different forums were used to disseminate video and written content.

Actors – *State actors* – Russian government orchestrated propaganda campaigns. *Troll farms* (Internet Research Agency) created false networks to amplify messages. *Ukrainians (government and civilians)* replied with counter-narratives. *International mass-media*: western press documented the phenomenon.

Tactics – Kremlin used the "firehose of falsehood" strategy (multiple contradictory narratives, disseminated rapidly and repetitively, to create confusion and diminish trust in institutions. Also, news fabrication was used, imitating western press articles.

Target audience – *Internal* – Ukrainian population through "liberation" messages. *External* –

Russian population, for legitimacy. *Global* – international public opinion, bombarded with alternative narratives, creating confusion of what was actually happening in Ukraine.

Impact – Russian propaganda managed to destabilize Ukrainian informational space, enforce separatism in the East and diminish trust in national institutions. Globally, it created various perceptions about the Russian intervention legitimacy. For the first time, social media was considered a strategic weapon.

Institutional responses – Ukraine responded slowly through counter measures regarding propaganda and disinformation. EU and NATO started developing dedicated entities to combat these phenomena.

Evolutionary stage – Ukraine conflict marks the *weaponization* phase where social media platforms are considered part of the hybrid weapons used by a state.

2.4. US Presidential Elections (2016)

Conflictual context – The US presidential elections campaign (Trump vs. Clinton) took place in a polarized climate, marked by social tensions over immigration, globalization and national identity. On the other side, Russia conducted a systemic campaign of digital interference to create confusion and polarization.

Dominant platforms – Facebook and Twitter were the main channels for disinformation. The algorithms were used more on these platforms and also on YouTube for aggressive content recommendation. Platforms became instruments for political micro-targeting.

Actors – *Internet Research Agency (IRA)*, based in Russia, with thousands of fake accounts and web pages managed to influence discourse. *Botnets* on Twitter amplified hashtags and attacked both candidates. *Internal actors*: partisans that amplified digital content.

Tactics – Fake pages that mimicked American organizations (veterans, minority groups, religious groups). Visual disinformation (memes, fake images). Micro-targeting through advertisements on Facebook for specific groups (based on occupation, beliefs or affiliation).

Target audience – Local: American electorate – amplify polarization. *Global*: creating an image of USA as unstable politically and socially.

Impact – This campaign amplified political polarization and diminished trust in the electoral process and traditional mass media. Social cohesion and democratic legitimacy have been affected.

Institutional responses – The interference triggered federal investigations and official reports that confirmed Russian presence in the process. Social media platforms introduced stricter regulations regarding political content and fake

accounts.

Evolutionary stage – This event marks the consolidation of *weaponization* stage, with different focus than before. Rather than focusing only on external destabilization, platforms are now considered means for manipulating internal affairs.

2.5. COVID-19 Pandemic (2020)

Conflictual context – The global 2019 pandemic was accompanied by a massive informational crisis. The lack of scientific certainties in the beginning meant that digital environment could easily be flooded by conspirative theories, rumors and deliberate disinformation campaigns. The World Health Organization (WHO) called this phenomenon an **infodemic**, an informational oversaturation, where there are no limits between truth and falsehood.

Dominant platforms – Facebook, Twitter and YouTube were the main dissemination spaces, alongside WhatsApp and Telegram (private channels) and TikTok, which grew bigger amongst young generation.

Actors – *Individual users* – millions of people distributed conspirative content voluntarily. *State actors* – Russia and China were accused of disinformation campaign in order to erode trust in public institutions.

Tactics – Infotainment – viral memes and videos with fake content. Image and video manipulation to create panic. Conspirative theories (laboratory-made virus, Covid caused by 5G), fear and anger appeals.

Target audience –*Local* – particular communities, especially vulnerable and skeptical groups. *Institutionally* – WHO, EU, national governments for eroding legitimacy. *Global* – worldwide population, targeted according to cultural specifications.

Impact – Massive confusion, polarization and resistance to public-health measures. Many conspirative anti-vaccination campaigns provoked violent protests against authorized institutions.

Institutional responses – WHO, helped by national governments globally, launched fact-checking campaigns and collaborated with social media platforms to eliminate fake content. Not all platforms responded the same, Telegram and WhatsApp remaining difficult to regulate.

Evolutionary stage – This case marks the switch to cognitive battlespace phase, where social media instruments are considered beyond their potential to manipulate public opinion, but rather to undermine state capacity for crisis management.

2.6. Russia's invasion of Ukraine (2022-present)

Conflictual context – Initially perceived as a conventional war, the Russian invasion unfolded an unprecedented informational

warfare. Unlike the 2014 situation, the new digital confrontation is officially part of the military and diplomatic strategy. Both parties use social media as a parallel battlefield.

Dominant platforms – TikTok has become a crucial dissemination platform, either for propaganda or disinformation. Telegram represents the main channel of communication on the battlefield and worldwide. The rest of the platforms contribute to one side or the other, or neutrally, just presenting the situation.

Actors – *State actors* – Russian state – official and non-official campaigns of propaganda, trolls, botnets, pro-Kremlin Telegram channels. Ukrainian state – proactive digital campaigns (strategic communications). *Non-state actors* – civilians and journalists – videos from the battlefield; influencers – memes, campaigns, crowdfunding.

Tactics – Visual disinformation – reuse of older conflict images to spread confusion; divergent narratives – Russia promotes ideological ideas of "denazification" "NATO challenges", whilst Ukraine focuses on narratives of resistance and victimization: deepfakes and AI generative content.

Target audience – *Locally* – Russian and Ukrainian populations for mobilization and justification. *Globally* – worldwide public opinion.

Impact – In Russia, digital propaganda consolidated authoritarian control over population. In Ukraine, social media became a social resiliency instrument, creating a strong sense of unity.

Institutional responses – Platforms introduced new rigid measures, such as eliminating Russian media accounts, labeling manipulative content, collaborating with governments towards countering disinformation.

Evolutionary stage – This event marks the maturity of cognitive battlespace, where the main objective is to shape each user's perceptions through strong emotions and cognitive behavior.

3. EMERGENT PATTERNS IN DIGITAL WARFARE

The analysis of the six cases, from jihadist propaganda in Iraq and Afghanistan, to informational full-spectrum Ukraine war, provides a detailed picture of how social media platforms have been instrumentalized in various warfare contexts. Besides each conflict particularities (culture, geopolitics, technology), a set of recurring dynamics emerges, adapted and refined over time, but also significant differences that mark the transition between particular phases. From a comparative point of view, the six cases present a series of common features that reveal the logic of how disinformation, propaganda and media subversion works, as well as the constant vulnerabilities of society

exposed to these phenomena.

Looking across the six cases chronologically, we can observe that alongside the evolution of tactics used in these conflicts, platforms also adapted accordingly in order to meet the new standards and expectations. Social media can no longer be considered a neutral entity, but it must be understood as an active actor that both shapes and is shaped by contemporary conflicts (Table 2).

The first common element is that social media has been used as the *main information infrastructure* in all cases. From the jihadist forums, to Telegram and TikTok, social networks have been used as a vector of amplifying messages, rising the visibility of actors, and challenging the informational power of states, regardless of the nature of the conflict.

The *dependence of emotions* was another fundamental aspect for communication on social media. Fear and anger were exploited by jihadists, hope and solidarity during Arab Spring, resentment and confusion in Ukraine, identity rage and polarization during U.S. elections, anxiety and distrust during COVID-19 and both empathy and hatred in current Ukraine war.

Another common aspect is the *asymmetry* between offensive and

defensive actions. In each case, the aggressors exploited platforms characteristics before official institutions did. The new hashtags were difficult to be countered initially, western countries have discovered election interferences too late, and fact-checking during the pandemic was not able to keep the pace with conspirative theories. Therefore, the *responses* to these new threats such as education, regulations or counter narratives were always **reactive**, giving the attackers a clear advantage.

Table 2 Evolution of social media aspects in modern conflicts

Case	Dominant platforms	Actors	Tactics	Objectives	Impact level
Iraq-Afghanistan	Forums, rudimentary websites, early YouTube	Non-state insurgents	Extreme videos, forum discussions	Radicalization and recruitment	Local
Arab Spring	Facebook	Civil activists, local citizens	Hashtag activism, viral posts	Mobilization and opposing regimes	National, regional

Case	Dominant platforms	Actors	Tactics	Objectives	Impact level
Ukraine (2014)	VKontakte, Facebook	State actors (Russia)	Troll farms, fake news, coordinated campaigns	Destabilization, justification of Crimea annexation	Regional destabilization with global effect
U.S. Elections	Facebook, Twitter	State actors (Russia), private intermediaries	Micro-targeting ads, bots	Undermine trust in democracy	Electoral legitimacy with global concern
COVID-19	WhatsApp, Telegram	Transnational groups, influencers, conspiracy groups	Conspirative theories, memes	Undermine science, promote distrust	Global, institution trust
Russia invasion in Ukraine	TikTok, Telegram	Poly-actors: state, non-state, platforms, influencers, AI	Deepfakes, coordinated narratives	Perception control, polarization	Direct effect on regional, with global resonance

On the same note, we can observe a gradually *tactics stratification.* No technique has disappeared entirely, instead, it has been added to the existing collection. The extreme videos of jihadists were not replaced entirely, but rather are combined with trolling, activism, electoral micro-targeting or deepfakes. All of these tactics together create the stratified informational arsenal that can be adapted to current times based on objectives.

Besides disinformation and propaganda, social media has employed *subversion* throughout all cases. In each scenario the indirect objective was to delegitimize a form of authority, from western military authority in Iraq and Afghanistan, to Ukrainian government, democratic institutions in the U.S. and scientific authority around the world.

On the other hand, if similarities of the six cases confirm transversal logic of propaganda, disinformation and media subversion on social media, the differences highlight a dynamic evolution of the three phenomena.

Firstly, the *main actors* have changed radically; from non-state

insurgent groups (Iraq-Afghanistan), civic activists (Arab Spring), and state actors (Russia), to multi-actor groups where states, technological platforms, civilians, influencers and AI algorithms work together.

The *objectives* have evolved from local recruitment and mobilization (2001) to state and electoral destabilization (2014 - 2016). The pandemic was the opportunity to undermine trust in science (2020) and the Russian invasion in Ukraine showed the power of perception controlling through parallel realities (2022-present).

Dominant platforms have undergone the most substantial evolution, due to technology advancement: starting with forums and YouTube videos as simple dissemination platforms, continuing with message viralization on Facebook and Twitter, up to globally and instantaneously distribution on TikTok and Telegram in the present.

Finally, the *degree of visibility* of operations has changed from explicit propagandistic messages, to covert and ambiguous campaigns (trolls, fake news, masked political advertisements), making it impossible in the present to distinguish a clear line between reality and manipulation.

4. CONCLUSIONS

This comparative analysis of the six cases shows not just similarities, differences, or patterns, but also a conceptual evolution that requires rethinking how we conceptualize propaganda, disinformation and media subversion. In academic literature, the three phenomena are usually addressed separately: propaganda as a persuasion instrument, disinformation as false news spreading and subversion as a process to erode authority legitimacy and social cohesion. However, this comparison suggests that this separation is no longer relevant in the context of modern conflicts. They need to be seen as an informational ecosystem that provides the basis for threats identification and anticipation. We do not need to focus on propagandistic messages and fake news, but on how these phenomena are part of a long-term cognitive erosion strategy.

The main takeaway of this study is that *cognitive dimension* of modern conflicts must be treated the same as the military one. Actors that control digital narratives influence directly regimes legitimacy, social cohesion and states capacity to act accordingly. In this sense, there is a need for institutional mechanisms to monitor, anticipate and react to informational campaigns.

Also, the results show the fact that *late defensive actions* are not sufficient. All six cases present that offensive actors have exploited platforms faster than institutional authorities could respond. This leads to the need of a change in strategy, from mere reactive cognitive defense, to a proactive strategy

of *cognitive resilience*, based on digital education, regulations and collaboration between governments, platforms and civilians.

Additionally, the three phenomena have been studied and approached separately for specific contexts. Current reality suggests that *propaganda, disinformation and media subversion function as a unit* in the big picture of social media, creating the need for predictive instruments capable to identify not only fake content, but also patterns regarding emotions, algorithms and social vulnerabilities. This approach could serve as basis for new early warning models, useful for research, and most importantly national security policy.

REFERENCES

[1] Atlam, El-Sayed, Malik Alamliki, Ghada Emarhomy, Abdulqader Almars, Awatif Esiddieg, and Rasha ElAgamy. 2025. "SLM-DFS: A systematic literature map of deepfake spread on social media." *Alexandria Engineering Journal* 446-455.

[2] Bateman, Jon, and Dean Jackson. 2024. *Countering Disinformation Effectively: An Evidence-Based Policy Guide.* Carnegie Endowment for International Peace.

[3] Benkler, Yochai, Robert Faris, and Hal Roberts. 2018. *Network Propaganda - Manipulation, Disinformation, and Radicalization in American Politics.* Oxford University Press.

[4] Bösch, Marcus, and Tom Divon. 2024. "The sound of disinformation: TikTok, computational propaganda, and the invastion of Ukraine." *Sage Journal* 5081-5106.

[5] Botan, Madalina, and Trisha Meyer. 2025. *Implementing the EU Code of Practice on Disinformation.* European Digital Media Observatory.

[6] Bradshaw, Samantha, and Philip Howard. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organized Social Media Manipulation.* Oxford UK.

[7] Chengcheng, Shao, Giovanni Luca Ciampaglia, Onur Varol, Kai-Cheng Yang, Alessandro Flammini, and Filippo Menczer. 2018. "The Spread of Low-credibility Content by Social Bots." *Nature Communications.* doi:https://doi.org/10.1038/s41467-018-06930-7.

[8] Ching, Didier, John Twomey, Matthew Aylett, Michael Quayle, Conor Linehan, and Gillian Murphy. 2025. "Can deepfakes manipulate us? Assessing the evidence via a critical scoping view." *PLOS One* 20 (5).

[9] Diel, Alexander, Tania Lalgi, Isabel Carolin Schröter, Karl MacDorman, Martin Teufel, and Alexander Bäuerle. 2024. "Human performance in detecting deepfakes: systematic review nad meta-analysos of 56 papers." *Computers in Human Behavior Reports* 16.

[10] EDMO. 2023. *European Digital Media Observatory D.17 Public Report.* EUI - School of Transnational Governance.

[11] Ellul, Jacques. 1965. *Propaganda - The Formation of Men's Attitudes.* New York: Vintage Books.

[12] Ferreira Caceres, Maria Mercedes,

Juan Pablo Sosa, Jannel Lawrence, Cristina Sestacovski, Atiyah Tidd-Johnson, Muhammad Haseeb UI Rasool, Vinay Kumar Gadamidi, et al. 2022. "The impact of misinformation on the COVID-19 pandemic." *AIMS Public Health* 262-277.

[13] Gaurino, Stefano, Noemi Trino , Alessandro Celestini, Alessandro Chessa, and Gianni Riotta. 2020. "Characterizing networks of propaganda on twitter: a case study." *Applied Network Science.*

[14] Howard, Philip, Bharath Ganesh, and Dimitra Liotsiou. 2019. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* University of Oxford.

[15] Howard, Philip, Samuel Woolley, and Ryan Calo. 2018. "Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration." *Journal of Inofrmation Technology and Politics* 81-93.

[16] Lasswell, Harold. 1938. *Propaganda Technique in the World War.* New York: Peter Smith.

[17] Marigliano, Rebecca, Lynnette Hui Xian Ng, and Kathleen Carley. 2024. "Analyzing Digital Propaganda and Conflict Rhetoric: A Study on Russia's Bot-Driven Campaigns and Counter-Narratives during the Ukraine Crisis." *Social Network Analysis and Mining* 14 (1).

[18] Marino, Sara. 2024. "Refugees' Storytelling Strategies on Digital Media Platforms: How the Russia-Ukraine War Unfolded on TikTok." *Social Media + Society Sage Journals* 10 (3).

[19] Pasquetto, Irene, Gabrielle Lim, and Samantha Bradshaw. 2024. "Missinformed about misinformation: On the Polarizing Discourse on Misinformation and its Consequences for the Field." *Harvard Kennedy School Misinformation Review.*

[20] Pomerantsev, Peter. 2019. *This is Not Propaganda.* London: Faber & Faber.

[21] Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare.* New York: Farrar, Straus and Giroux.

[22] Schrijver, Peter. 2025. "Ukrainian Intelligence's Use of Telegram in Wartime." *International Journal of Intelligence and Counterintelligence* 1-27.

[23] Vosoughi, Soroush, Deb Roy, and Sinan Aral. 2018. "The Spread of True and False News Online." *Science* 359: 1146-1151. doi:https://doi.org/10.1126/science.aap9559.

[24] Yang, Kai-Cheng, Francesco Pierri, Pik-Mai Hui, David Axelrod, Christopher Torres-Lugo, John Bryden, and Fillippo Menczer. 2021. "The COVID-19 Infodemic: Twitter versus Facebook." *Big data & Society* 1-16.

[25] Zannettou, Savvas, Tristan Caulfield, Emiliano Cristofaro, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. 2019. "Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and their Influence on the Web." *Companion The 2019 Worl Wide Web Conference.*