Accelerated Innovation (AI): Sustainability for Better Humanity
21–24 May 2025
Bangkok, Thailand
make learn
TIIM
PIConf
Management, Knowledge and Learning
International Conference
Technology, Innovation and Industrial Management
Sustainable Development

Toxic Environment

Ciro Settecasi
MED.E.A – Higher Education Institution for Mediterranean, Europe and Africa, Italy
Società Italiana di Storia Militare (SISM), Italy
ciro.settecasi@gmail.com

Abstract

New Media and social networks convey ever greater flows of information, fed by videos, narratives, images, flyers and so on. Everything that manifests on the web is instantaneous and global, influencing the public's perception and behavior. Nowadays, the potential of information technology happens through social media, such as tools such as: telegram, WhatsApp, twitter, TikTok Instagram, VK (called after the Russian Facebook), Rossgram (called after the Russian Instagram), Rutube like the Russian YouTube, Odnoklassniki and Pinterest. These tools are the main manipulative channels and represent, together with cyber warfare, the cornerstone where hybrid warfare is founded. In this modern conflict, the most important action is to manage information or rather to be the masters and/or custodians of it.

Hybrid warfare refers to a strategy that blends conventional military tactics with unconventional methods, including cyber attacks, misinformation, economic pressure, and guerrilla warfare. This approach aims to exploit the vulnerabilities of an adversary, making it difficult to identify the source of the attack and respond effectively. Key characteristics of hybrid warfare include: Multi-Domain Operations; Unconventional Forces; Information and Psychological Warfare; Cyber Operations; Economic Warfare; Legal and Covert Activities.

Understanding hybrid warfare is essential for modern defense strategies, as it requires coordinated responses across military, political, and informational domains. Nations must adapt their defense and security policies to address these evolving threats effectively.

Keywords: New Social Media, Psychological Warfare, Cyber Operations, Multi-Domain Operations, Propaganda and Intoxication.

INTRODUCTION

Nowadays, in the context of the European conflict, the competition among great powers has taken the form of the spread of fake news and narratives - one of the most commonly used “hybrid” tactics by adversaries.

Indeed, in the final document of the NATO summit held in Vilnius last July, the Atlantic Alliance acknowledged that “Russia has intensified hybrid attacks against NATO countries and their partners, including activities that interfere with democratic processes, political and economic coercion, and widespread disinformation campaigns.”[1].

This awareness has gradually taken root within the European Union over the past decade. In fact, following the publication of the so-called "Gerasimov doctrine[2]" and the worsening situation in Ukraine in 2014 - with the annexation of Crimea by Russia through a referendum considered illegal by the International Community - the Council of the EU called for a stronger commitment from the External Action Service.

For this reason, a new Command in charge of Strategic Communication was established in Helsinki, becoming the first European Centre of Excellence on Hybrid Threats.

One of the most significant advancements in the fight against fake news came in 2018 with the introduction of the Code of Practice on Disinformation - the first worldwide initiative in which major industry players like Facebook, Google, Twitter, and Mozilla voluntarily agreed to adopt self-regulatory standards to combat disinformation. Other stakeholders, such as Microsoft and TikTok, also signed the agreement.

Later, during the COVID-19 pandemic, there was an overwhelming amount of unverified information, making it extremely difficult for individuals to distinguish between true and false content. The reliability of sources [3] became increasingly hard to assess.

TOXIC ENVIRONMENT

The quality of information is not only crucial for military capabilities but also represents a fundamental pillar of democracy. In today’s digital age, the variability and volume of information can significantly influence public opinion and affect the psychological well-being of a population - especially through the spread of fake news.

Misinformation has indeed become a serious threat to democratic societies. For this reason, the European Union must take active steps to defend its democratic institutions and protect its information space.

---

[1] DOCUMENTO CONCLUSIVO Summit NATO di Vilnius

[2] The Gerasimov Doctrine is a Russian military strategy developed by General Valery Gerasimov, which emphasizes the use of political, economic, and informational measures along with unconventional military operations. This doctrine is based on the idea that modern conflicts are not limited only to the use of military force, but also involve attacks on the economic and cognitive levels.

[3] European Democracy Action Plan (EDAP) disponibile online al link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:- 52020DC0790&from=EN.

The new generation faces a significant challenge in an International Community that currently lacks the strength to effectively defend democratic countries.

In response, the European Commission approved the European Democracy Action Plan (EDAP) in 2020. This plan identifies tools already developed or to be implemented to defend European democracy, and for the first time provides a comprehensive list of definitions for various related terms.

These aspects are commonly included under the term “disinformation”. In particular, the document distinguishes between misinformation - false or misleading content shared without harmful intent, though its effects can still be damaging - and disinformation, which is deliberately created and shared to cause harm.

While it may seem of secondary importance, having a shared set of definitions - something still lacking within NATO, for example - greatly facilitates the work of researchers and policymakers in developing strategies to counter the phenomenon. The 2020 document also outlines an action plan to improve coordination among EU Member States, the G7, and NATO. This coordination was further strengthened by the launch of a revision process for the Code in 2021, which was reinforced in 2022.

One of the main criticisms of both the original 2018 version and the revised document is that they are not legally binding for major social media companies. However, their cooperation in curbing fake profiles and disinformation remains essential. For example, cutting advertising revenue for disinformation campaigns is a critical step.

This was evident in one of the most elaborate and widespread disinformation operations since the beginning of the war in Ukraine: Operation Doppelgänger, which notably targeted French media starting in autumn 2022. The name, taken from the German word for “double,” was coined by the European NGO DisinfoLab. Together with other NGOs, it participated in an investigation launched by the German press in September 2022. Following these reports, Meta intervened by deleting over 1,600 accounts and 700 pages.

The operation affected all major platforms and was marked by the dissemination of false narratives portraying Ukraine as a corrupt and failed state, while simultaneously denying verified Russian war crimes, such as the Bucha massacre. To do so, clones of legitimate news websites were created to mimic credible sources - hence the name “Doppelgänger.”

But this is not the only initiative promoted by the European Union to strengthen the resilience of its Member States. Since 2015, the East StratCom Task Force of the European External Action Service has managed a debunking project called EUvsDisinfo. This website exposes prominent false narratives - particularly those promoted by the Kremlin or affiliated actors - providing facts and reliable sources for reference.

For several years, the European Digital Media Observatory (EDMO) has also been active, with significant contributions from Italian experts. EDMO brings together professionals in the field to enhance understanding of the disinformation phenomenon and develop countermeasures. These include substantial efforts in digital media literacy for European citizens.

In the NATO framework, it is also worth highlighting the work of the Strategic Communications Centre of Excellence, founded in Riga in 2014. Strategic communication encompasses more than just

countering disinformation, but that remains one of the center's core missions. It does so by developing training models to combat targeted campaigns and by analyzing narratives and counter-narrative strategies for the Allies.

One of the most elusive aspects of this threat is its multi-domain nature, as it seeks to obscure and distort both the truth and the quality of information. Internet is its most frequently and effectively used tool, enabling its spread into the cyber domain as well.

For this reason, one of the major challenges today is understanding how Artificial Intelligence (AI) can act as a force multiplier in spreading false information and generating fake evidence to support anti-Western narratives - or, conversely, how it can be harnessed as a powerful tool for defense. This is precisely what many digital platforms, such as Facebook, are currently working on in their efforts to detect and limit fake news.

Amid the overwhelming volume of data available, AI models have already proven to be valuable allies. However, at present, we cannot rely solely on digital tools to counter this evolving threat. Most likely, "analog" intelligence - human judgment and critical thinking - will remain essential to mounting an effective defense.

App Warfare

Today, Ukraine stands out as one of the world's leading countries in software development, especially in the military and civil defense sectors. Among the most notable programs is Air Alert, an app that warns users on their phones about air raids in specific locations. On the Play Store and App Store, other widely used apps include Telegram, Zello Walkie Talkie, Bridgefy, and Signal the latter being especially important for its end-to-end encryption, which guarantees complete privacy protection.

One of the most remarkable apps is GIS Art (more precisely, GIS Art for Artillery), developed by a Ukrainian officer. This tool locates enemy targets and transmits their coordinates to Ukrainian artillery units, which then select the nearest rocket launcher, drone, or mortar to identify and destroy the target. The app functions similarly to Uber, connecting a target with the nearest weapon system in real time. GIS Art provides target coordinates with an accuracy ranging from 6 to 25 meters.

Another particularly interesting App involves face-swapping technology used to inform Russian citizens about the progress of the war. It spreads awareness about the consequences of the conflict, with the goal of shifting public opinion within Russia.

Maskirovka

In Russian, the term "Maskirovka" means camouflage or deception. It refers to the Soviet doctrine of strategic misdirection, often applied in military and political contexts. Maskirovka typically unfolds in four stages:

1. **Denial** – The Russian government denies any involvement or responsibility.
2. **Narrative Control** – The focus is shifted to blame provocations and alleged aggression from Russia's enemies.
3. **Cooperation** – A declared willingness to cooperate and engage in diplomatic forums.
4. **Self-Defense** – Framing all Russian actions as defensive and justified.

Bufole.net

In the digital age, social media has revolutionized communication - but it has also facilitated the widespread dissemination of false information. In Italian, the word “bufala” (hoax) describes a form of deception that misleads the public, comparable to “being led by the nose like a buffalo.” The metaphor illustrates how false narratives can shape public thinking.

This phenomenon has created a pressing need for source and content verification. In response, a new professional figure has emerged in the digital media era: the “sbufalatore,” more widely known as a fact-checker. Since 2014, the rise of disinformation has made fact-checking an essential activity in journalism and public communication.

The website www.bufale.net has been online since 2014, offering free fact-checking responses to bufale - that is, disinformation - within the social media landscape.

Another key factor contributing to the spread of bufale is the increasing use of artificial intelligence, which has made it possible to generate fake images and videos, manipulating the thoughts and beliefs of countless internet users.

A particularly striking example is the hoax about the “miraculous” use of baking soda as a supposed cure for cancer. Tragically, this false claim led many patients to abandon legitimate, evidence-based medical treatments, with devastating consequences.

It is essential not to let the fast pace of social media influence your judgment. In all cases, news shared online must be carefully verified. Social platforms are saturated with misinformation: from completely fabricated stories to exaggerated half-truths and content that distorts reality through biased interpretations.

To avoid falling into the trap of false information, users must cross-check facts with reliable sources and be willing to spend time evaluating whether the news they read has been manipulated or taken out of context.

Dangerous truths

In other words, the strategic use of disinformation, of “grey” or “black” propaganda, is now recognized as a true weapon of war. The objective of this toxic information is to distort reality, or even more dangerously, to create a false reality - one that, quoting Noam Chomsky, functions as a form of historical engineering aimed at shaping public memory and transforming falsehoods into undisputed truths in the eyes of those who disseminate them.

Thus, we see the return of classic propaganda techniques that underpin all psychological warfare operations: The binary Us vs. Them narrative. The creation of a deceitful, inhuman enemy portrayed as monstrous and cruel.

A focus on alleged atrocities in line with the tropes of traditional atrocity propaganda. Repetition of these themes targeted especially at vulnerable groups, such as women and children.

The strategic use of symbols and myths to amplify fear and emotion, often with the aim of spreading the message to external and even global audiences.

In the current conflict, for the first time, the main actors in the flow of information are no longer traditional media. This shift had already begun during Operation Desert Storm, which is often cited as the first “media war” - a case study on the intersection of politics, warfare, and journalism. But while traditional media - TV, radio, and newspapers - once acted as the primary sources of information, they have now been surpassed by social networks.

These so-called new media are used not only to share content but also to amplify communication flows on a global scale. While it is true that television and newspapers still reach wide audiences, social media deliver an unlimited volume of information in real time to a vast, worldwide user base - making them arguably the most powerful tool in the information warfare arsenal today.

At the same time, this extraordinary synergy of communication channels reaches categories of users not necessarily engaged with new media. This interconnected network of “transmission belts” possesses the power to transform any fact - real or fabricated - into a news item that, within hours, can be perceived as reality by large portions of the population.

The infinite possibilities associated with information, disinformation, and counter-information operations on the dark web further highlight the near impossibility of censoring or suppressing information once it is online.

The only truly effective resistance lies in engaging with the same tools - black or gray propaganda - either by undermining the credibility of harmful information or by creating counter-narratives that disrupt and destabilize pre-established beliefs and perceptions.

Mark Twain once ironically remarked in response to premature reports of his death - a statement that has since become emblematic of today’s disinformation age:

"It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so."

This observation remains strikingly relevant today, as false certainties pose even greater risks than ignorance itself.

In our current era, the potential for information poisoning, often referred to as intox, has reached unprecedented levels. The widespread manipulation of news, images, and voice recordings is now made possible by technologies like deepfakes - algorithms that generate realistic video content featuring public figures apparently making false or fabricated statements.

Recent conflicts have offered stark examples of this phenomenon. One of the most notable was a deepfake video of Ukrainian President Volodymyr Zelensky, in which he appeared to urge his people to surrender and accept Russian victory. This fake message was broadcast on March 16, 2022, on the Ukrainian television channel Ukraine24, and subsequently spread across YouTube, Facebook, Telegram, and the Russian platform Vkontakte.

Conclusion

In recent years, the European conflict and the escalating rivalry among global powers have underscored the growing use of disinformation as a central weapon in so-called hybrid warfare. From coordinated fake news campaigns to the technological support provided by artificial intelligence, the manipulation of information has become a strategic tool for influence and destabilization.

Both the European Union and NATO have recognized this threat, strengthening regulatory and operational instruments to counter it. Initiatives such as the 2018 Code of Practice on Disinformation, the European Democracy Action Plan (EDAP), and concrete efforts like EUvsDisinfo and the European Digital Media Observatory (EDMO) reflect a growing institutional awareness. However, the response cannot be purely normative: the multidimensional nature of disinformation requires a transversal approach involving education, technological innovation, international coordination, and collective media literacy.

The deliberate dissemination of alternative narratives, the revival of historical techniques like Russia's maskirovka, and the use of digital platforms and social media as amplifiers of misleading content illustrate how information itself has become a battlefield. Ukraine's technological ingenuity, including the development of applications for civilian alerts and military coordination, demonstrates how innovation can be repurposed for defense and resilience.

At the same time, the rise of deepfake technologies and the ability of AI to generate realistic yet entirely fabricated content raise urgent questions about source reliability and the future of public communication. As shown by the manipulated video of President Zelensky urging surrender - broadcast on national television and shared across major platforms - the boundary between reality and fiction is increasingly blurred.

Ultimately, the fight against disinformation cannot rely solely on digital tools. It requires robust "analog" intelligence, grounded in critical thinking, digital literacy, media education, and civic responsibility. Only through an integrated, multidisciplinary effort can European democracies defend themselves against the systematic manipulation of truth and safeguard the integrity of their information space.

REFERENCES

European Commission. (2018). Code of Practice on Disinformation. Retrieved from https://digital-strategy.ec.europa.eu

European Commission. (2020). European Democracy Action Plan (EDAP). Retrieved from https://ec.europa.eu

EUvsDisinfo. (n.d.). Fighting disinformation. Retrieved from https://euvsdisinfo.eu

DisinfoLab. (2022). Operation Doppelgänger: Mapping Russia's Disinformation Ecosystem. Retrieved from https://www.disinfo.eu

NATO. (2023). Vilnius Summit Communiqué. Retrieved from https://www.nato.int

Strategic Communications Centre of Excellence. (2014). About StratCom COE. Retrieved from https://stratcomcoe.org

Twain, M. (n.d.). It ain't what you don't know that gets you into trouble. (Popularly attributed).

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe Report.

Chomsky, N. (2002). Media Control: The Spectacular Achievements of Propaganda. Seven Stories Press.