

DISINFORMATION AS A TOOL OF HYBRID WARFARE: A STRATEGIC ANALYSIS OF NATIONAL SECURITY IN THE BALKANS

Mariya HADZHIPETROVA-LACHOVA

South-West University “Neofit Rilski“, Blagoevgrad, Bulgaria
maria.hadzhipetrova@gmail.com

Abstract: Due to the rapid growth in technology, the information environment has rapidly transformed into a key avenue for hybrid threats, changing the traditional conception of national security into a perpetual state of “hybridity”. This article presents an interdisciplinary analysis of disinformation - using information science, political science, and psychology - to review its function as a strategic method in the Gray Zone. By deploying multiple tactics (conventional, irregular, cyber) simultaneously, hybrid malefactors take advantage of societal weaknesses in order to undermine democratic systems without engaging in a full-scale conflict. The special attention of this report is focused on the Balkans, where entrenched ethnic, religious, and political divisions make for a permissive environment for subversion. The author will examine how the Ukraine War and Covid-19 pandemic have acted as catalysts for increased hybrid activity through automated social bots and other technological tactics to increase impact and degrade the trust in government institutions. This report ultimately calls for a “whole-of-society” approach to building resilience against information based attacks by promoting critical digital literacy and improved levels of cooperation between the NATO and EU in order to protect regional stability given the shifting nature of these types of attacks on information systems.

Keywords: Balkans, disinformation, hybrid threats, national security, resilience

1. Introduction

The transformation of information creation and distribution in the digital age has fundamentally altered the strategic landscape of national security by introducing a constant state of hybridity. While high technology offers undeniable advantages for global connectivity, it has simultaneously empowered the deliberate dissemination of false or misleading narratives, which now function as a primary vector for hybrid threats. This phenomenon has evolved beyond traditional journalism to become a sophisticated tool for cognitive manipulation capable of destabilizing societies and undermining the very foundations of democratic processes. Within the recommended framework, hybrid warfare can be seen not as a single act of aggression, but as the synchronized use of multiple instruments of power. Specific emphasis thereby are political, economic, military, and informational, which are tailored to

exploit the specific vulnerabilities of a target state. In the current global security environment, this threat is amplified by overlapping crises, most notably the protracted geopolitical fallout from the war in Ukraine and the persistent social scars left by the COVID-19 pandemic. These events have served as catalysts for massive “infodemics” [1] that demonstrate how disinformation is now a central component of modern conflict. Hybrid actors utilize the concept of “Gray zone” [2], mainly as an envisaged space between peace and conventional war, whereby it is meant as to achieve strategic objectives without engaging in full-scale kinetic combat. Using the speed of social media and the extensive reach of automated chat bots, these actors can quickly scale up their impact to manipulate many spheres of public health, institutional trust, and electoral integrity. Current events show that the tactics used by these actors have

advanced dramatically in 2024-2025; now AI-generated deepfakes and coordinated “spear-phishing” attacks can be used to compromise both data integrity and public perception. Due to a highly fragmented ethnic, religious and political situation, the Balkan region is an ideal environment for these hybrid operations. Therefore, the manipulated messages spread through the various outlets are not just false information; however, they are strategically designed with the intent of exploiting historical and social vulnerability, provoking internal conflicts among communities, and generating increased influence by external geopolitical actors.

Disinformation acts as a catalyst for political instability by creating echo chambers and reinforcing cognitive biases, which effectively polarizes the population and hinders the ability of institutions to respond to multifaceted crises. Balkan states share a geographical proximity to the Ukraine conflict and this situation has increased the pressures related to narratives being weaponized to undermine the Euro-Atlantic integration and present international alliances as weak or divided.

Ultimately, the ambiguity inherent to hybrid threats makes attribution of these actions difficult and adds complexity to a state’s legal and military response since the actions are, in many instances, just below the threshold of traditional warfare, which makes it very difficult to identify who has conducted these actions. The ability to carry out these campaigns is often rooted in “enlargement fatigue” and a lack of media literacy which creates an environment conducive for hostile influence to exist. Therefore, identifying the interdisciplinary intersection between information science, political science, and psychology is essential when assessing the risks associated with hybrid threats and developing robust strategies for improving national resilience. The final goal of this report is to provide an analysis of these dynamics as they relate to the Balkan security architecture; which will illustrate

that only through a holistic and coordinated effort can the stability of democratic societies be guaranteed against the evolving threats of hybridity.

2. Theoretical Framework: Defining the Hybrid Threat Landscape

2.1. The Conceptual Origins of Hybridity Hybridity is now defined by the convergence of technical cyberattacks and cognitive information operations theory. Hack and leak operations are a classic example, where sensitive data is compromised through methods such as phishing and then released publicly to damage the reputation of political institutions. In this context, hacker breaches produce the “raw materials” for disinformation campaigns. The real-world consequences of these hybrid tools go beyond the psychological impact and have measurable financial and operational dimensions; for example, the attack on Tesco Bank led to the direct freezing of thousands of customer accounts and significant regulatory fines [3, 4]. The scale of these threats is so great that Lloyd’s of London estimates that a massive global cyberattack could cause economic losses of over \$53 billion (Barlyn, 2017). This confirms that modern conflict has moved into the spectrum of “hybridity” [5], where the synchronized application of cyber tools and disinformation creates a synergistic effect against which traditional defense architectures often prove unprepared.

2.2. Technological Weaponization and Vulnerability of Critical Infrastructure

The evolution of hybrid conflicts requires a rethinking of national security, as contemporary threats are not invincible, and do not require specific training of armed forces and civilian institutions [6, 7]. A central element in this process is the “weaponization” of new and emerging technologies, which changes global risks and requires attention to the critical importance of safeguarding data as artificial intelligence and big data continue to evolve [8]. The practical application of these methods includes complex preparations for conducting modern warfare, in which

disinformation is used as a strategic tool for building influence, especially in Europe [9,10]. This destabilization often targets critical energy infrastructure, where cyberattacks on power grids and physical blackouts demonstrate the vulnerability of regional systems [11, 12].

In addition to the digital space, hybrid operations also materialize through physical and legal provocations. Examples of this are the systematic jamming of GPS signals in the Baltic Sea by vessels and the instrumentalization of migration, which leads to the racialization of border management and geopolitical tensions with a special focus on Europe [13, 14, 26]. In regions such as Moldova, civil society has been facing coordinated strategies of “dismiss, distort, distract, dismay” that aim to erode democratic values [15]. This pressure, including cognitive warfare challenges, needs the strengthening of its legal frameworks and local security, while ensuring policies toward sustainability of critical services, including healthcare and seasonal safety in coastal areas [15, 22].

2.3. Psychological Mechanisms and the Diffusion of Disinformation in the Digital Environment

The concepts of echo chambers and disinformation are central to the strategic analysis of hybrid threats in the Balkans [16]. An echo chamber refers to a defined epistemic space [17] where members primarily encounter viewpoints and beliefs that reinforce their own, thereby forming a self-fulfilling cycle and pushing groups toward radicalization and extreme political postures [17]. In terms of national security, disinformation is defined as the intentional conduct of malicious actors that create deceptive narratives with specific geopolitical objectives even through social media [18], as using documentary formats or legitimate news to create strategic deception and undermine democracy.

Recent studies have been able to demonstrate how hybrid threat actors utilize social networks to propagate disinformation through fake news and the creation of automated comments [19, 20].

But this only represents the first step in executing their strategic deception. The final mechanism of success for the hybrid agent’s operation occurs when the disinformation is absorbed into popular culture and begins to circulate naturally as fortuitous by-products of the users’ belief systems [21, 22]. Ultimately, the original source and intent remain undisclosed.

3. Analysis: The Balkan Peninsula as a Hybrid Battleground

The contemporary understanding of conflict has shifted from a binary state of “peace” or “war” to a spectrum of “hybridity.” Traditional military doctrine often struggles to categorize modern threats because they deliberately blur the lines between conventional and irregular warfare. This evolution was fundamentally shaped by the realization that military force alone is often insufficient to achieve political objectives in a globalized information environment.

3.1. Regional Vulnerabilities and Historical Fragmentation

The Balkan region has been historically fragmented ethnically, religiously, and politically, making it a sensitive area for hybrid operations. As pointed out by Vasilev

[23] hybrid threats of a military-political nature exploit internal instability, building on historical trauma to provide a means for the strategic destruction of statehood through social vulnerability. In particular, Russian interests are heavily at work within the region.

Disinformation is effective within the Balkans due to the “limitations of the human mind” and cognitive distortion that affect the way people perceive reality. Vasilev [24] demonstrates how people interpret incomplete or ambiguous information through egocentrism or sociocentrism. These pathological thought patterns (e.g., “herd mentality” and prejudice) inhibit the ability to objectively analyze intelligence and enable hybrid actors to hide the truth through deception and to distort societal and

government attitudes.

Rapid advances in technology facilitate the execution of large-scale operations that affect information and cognition in such a way as to alter the perception of factual information. Vasilev [24] notes

that critical thinking is the only defense against hybrid strategies that make use of rationalization and intellectual arrogance.

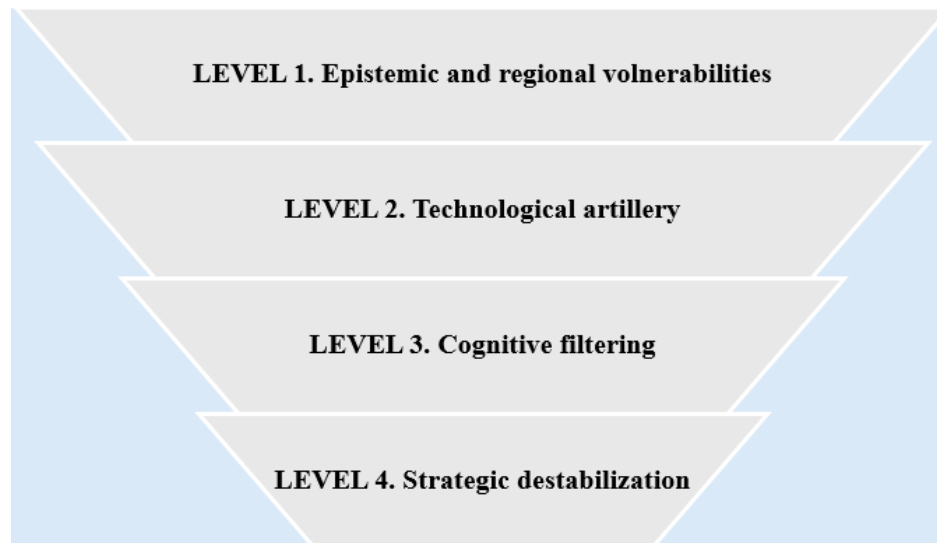


Figure 1: Integrative Funnel Model of Cognitive and Strategic impact
Source: Author's model

3.2. The War in Ukraine and Challenges Facing NATO's Southeastern Balkans as a Catalyst for Hybrid Escalation.

The geopolitical shift since the start of the war in Ukraine has intensified hybrid pressure on the Balkans, turning them into a “second front” of influence. Vasilev [23] examines how Moscow is implementing hybrid actions to undermine Euro-Atlantic integration, using disinformation as a method for “preparing and waging modern hybrid warfare”. These actions aim to create a cognitive environment in which the population questions the reliability of international alliances such as NATO and the EU, undermining the strategic sustainability of countries such as Bulgaria. The specific security problems in the Black Sea region and the Balkans are compounded by the lack of long-term strategic vision and insufficient attention from the Allies. In his analysis of Turkey and regional security, Vasilev [24] emphasizes that weak operational capabilities and low readiness to counter non-military crises make the Southeastern Flank vulnerable. The insufficient saturation with modernized weapons and the fragmented positions of the member states facilitate hybrid actors in their attempts to split the unity of the Alliance.

In conclusion, the analysis of hybrid threats to international entities and the Republic of Bulgaria requires the adaptation of conceptual approaches to security. One can insist on the development of theoretical knowledge aimed at predicting and early disclosure of hybrid impacts. Minimizing cognitive limitations and strengthening critical thinking in the intelligence community are fundamental steps for building an adequate security environment that would neutralize attempts to undermine national sovereignty in the regional and subregional context of the Balkans.

6. Conclusions

This analysis demonstrated how disinformation is not an isolated event but is a core, systematic element of the much

larger phenomena of modern hybrid warfare. Within the context of the Balkans, a region with distinct historical ethnic tensions, there exists a multidimensional threat to national security as a result of the intersection between historical ethnic tensions and high-technology manipulation. This threat operates primarily within the “Gray Zone” of operations. As the lines continue to blur between technical cyberattacks and cognitive subversion, traditional methods of responding to security threats are no longer sufficient to counter the synergistic impact of these evolving threats. The move from a reactive-defensive posture to a proactive-resilient posture requires a systematic understanding of the influence process. This is illustrated by the Funnel Model. When evaluating the vulnerabilities & technologies (Level 1 & 2) employed when countering hybridity, it is evident that securing the technical architecture from the automated “technological artillery” is a critical element of countering hybridity. In addition, national security entities must adapt to mitigate the effects of maneuvers such as spear phishing [25], which provide a gateway for more extensive campaigns. Strengthening regulations on social media to increase algorithmic transparency is essential to prevent hostile actors from scaling their influence through echo chambers [17]. The next core Level 3 & 4 (Cognitive Filtering & Strategic Impact) occurs as emphasized by Vasilev [24] in the light of “limitations of the mind” and cognitive biases are the primary targets of the adversary. Investing in critical thinking and digital literacy is a strategic necessity to empower citizens against the “Dismiss, Distort, Distract, Dismay” tactics [15].

The cross-border nature of hybrid warfare means that stability in the Balkan region is closely connected to NATO's and the European Union's collective defense mechanisms. To that end, NATO and the European Union must continually modernize their military strategies to account for the tactics observed during the

Ukraine war and ensure that the southeast flank of Europe does not become a "second front" for those who wish to establish influence. Additionally, intelligence sharing and synchronized strategic communication between NATO and the EU are critical to undercutting foreign actors' ability to portray international alliances as weak and divided. In conclusion, ensuring the Balkan region's security requires an integrated whole of society approach. This interdisciplinary approach must integrate information science, political strategy and psychology. Allocating resources to address the vulnerabilities in both our digital infrastructure and the cognitive

impacts of opportunities identified as part of the information age by focusing on how to maintain the integrity of our democratic processes will provide no less than an opportunity for securing the ongoing cooperation of both the institutional actors responsible for maintaining democratic processes as well as for securing the ongoing integrity of democratic processes. In short, the Balkans must be reconstructed to be more than just a collection of fragmented and independent theatres of operations, they must become a prosperous and stable bastion of democracy in Europe in different contexts [28].

References

- [1] Briand, S. C., Cinelli, M., Nguyen, T., Lewis, R., Prybylski, D., Valensise, C. M., Colizza, V., Tozzi, A. E., Perra, N., Baronchelli, A., Tizzoni, M., Zollo, F., Scala, A., Purnat, T., Czerniak, C., Kucharski, A. J., Tshangela, A., Zhou, L., Quattrociochi, W. Infodemics: A new challenge for public health. *Cell*, 2021; 184(25): 6010-6014. <https://doi.org/10.1016/j.cell.2021.10.031>.
- [2] Jordan, J. International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict. *Journal of Strategic Security*, 2020; 14, (1): 1-24. <https://doi.org/10.5038/1944-0472.14.1.1836>
- [3] <https://www.wired.com/story/tesco-bank-hack-fraud-customers> [cited 2026 May 24]
- [4] Financial Conduct Authority. Available from <https://www.fca.org.uk> [cited 2026 May 24]
- [5] Jackson, P., Albrecht, P. Power, Politics and Hybridity. In: Wallis, E. et al. (eds).
- [6] Hybridity on the Ground in Peacebuilding and Development: Critical Conversations ANU Press; 2018, 37–50. Available at <http://www.jstor.org/stable/j.ctvgd1g9.7>. [cited 2026 May 24]
- [7] Hoffman, F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies; 2007.
- [8] Hoffman, F. G. Hybrid Threats: Neither Omnipotent Nor Unbeatable. *Orbis*. 2010; 54 (3), 441-455.
- [9] Rickli, J.-M., Villasi, G. The Weaponization of Emerging Technologies and Their Impact on Global Risk: A Perspective from the PfPC Emerging Security Challenges Working Group. *Connections: The Quarterly Journal*. 2025; 24 (1): 91-112.
- [10] Kaczmarek, K., Karpiuk, M., Melchior, C. A Holistic Approach to Cybersecurity and Data Protection in the Age of Artificial Intelligence and Big Data. *PRAWO i WIEŻ*. 2024; 5: 103-122. Available at: <https://doi.org/10.36128/PRIW.VI50.907>. [cited 2026 May 24]
- [11] Włodyka, E. M., Kaczmarek, K. Cyber Security of Electrical Grids - A Contribution to Research. *Cybersecurity and Law*. 2024; 12(2): 260-272.

- [12] Bachmann, S. D., Gunneriusson, H. Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security. *Scientia Militaria, South African Journal of Military Studies*. 2015; 43 (1): 77 - 98.
Available at: <http://dx.doi.org/10.2139/ssrn.2506063>
- [13] Bachmann, S. D., Jones, M. Syria - A Hybrid War Case Study. *Journal of Military and Strategic Studies*. 2021: Available at: <https://ssrn.com/abstract=3939659>
- [14] Metiu, N. ,Völpel, M. Geopolitical Hybrid Threats. *Deutsche Bundesbank Discussion*. 2026; 11. Available at: <http://dx.doi.org/10.2139/ssrn.6510318>
- [15] Nistor, R. M., Stretea, A. I. Dismiss, distort, distract, dismay: the civil society in Moldova in the face of disinformation. *Civil Szemle*. 2025; 22(1): 177-194.
- [16] Kiryakova-Dineva, T., Hadzhipetrova-Lachova, M. Intercultural Management-Main Aspects and Perspectives For The Practice Of International Organizations, *Entrepreneurship*. 2017: 5 (1): 97-105.
- [17] Nguyen, C. T. Echo Chambers and Epistemic Bubbles. *Episteme*. 2020; 17 (2): 141-161.
- [18] Cinelli, M., de Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., Starnini, M. The Echo Chamber Effect on Social Media. *Proc Natl Acad Sci USA*. 2021, 18 (9): e2023301118.
- [19] Bennett, W. L., Livingston, S. The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions. *European Journal of Communication*. 2018; 33 (2): 22-139.
- [20] Anspach, N. M., Carlson, T. N. What to Believe? Social Media Commentary and Belief in Misinformation. *Political Behavior*. 2020; 42 (3): 697-718.
- [21] Baccouche, A., Ahmed, S., Sierra-Sosa, D., Elmaghraby, A. Malicious Text Identification: Deep Learning from Public Comments and Emails. *Information*. 2020; 11 (6): 312.
- [22] Achimescu, V., Chachev, P. D. Raising the Flag: Monitoring User Perceived Disinformation on Reddit. *Information*. 2021: 12 (1): 4.
- [23] Vasilev, V. Balgaria vav fokusa na hibridnite zaplahi ot Rusiya. VA G.S. Rakovski, 2024 [Василев, В. България във фокуса на хибридните заплахи от Русия. София: ВА „Г.С. Раковски“; 2024]
- [24] Vasilev, V. Ogranicheniyata na uma - faktori, opredelyashti dostovernostta na razuznavatelnia analiz. [The Limits of the Mind - Factors Determining the Credibility of Intelligence Analysis]. *Sigurnost i otbrana [Security and Defence]*. 2024; (1): 262-278.
- [25] Vasilev, V. Kritichnoto mislene - osnova za kachestven razuznavatelen analiz [Critical Thinking - The Foundation for Quality Intelligence Analysis]. *Sigurnost i otbrana [Security and Defence]*. 2024; 3 (1): 197-210.
- [26] Halevi, T., Memon, N., Nov, O. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks 2015. Available at: <http://dx.doi.org/10.2139/ssrn.2544742>
- [27] Kupreishvili, T., Okropilashvili, T. Political Alternatives of the Security Strategies. 2023; 16(3): 42-45.
- [28] Kiryakova-Dineva, T., Kitkova, M. Intercultural dialogue: a prerequisite for successful tourist adaptation. *Book of proceedings. XII International May Conference on Strategic Management IMKSM*. 2016; 593-603.