Elīna Graudiņa
Mg. sc. pol.; Rīga Stradiņš University
Mg. sc. pol.; Rīgas Stradiņa universitāte
E-mail / e-pasts: elina.graudina@rsu.lv; ORCID: 0000-0002-8878-9071

Vija Sīle
Dr. phil.; Rīga Stradiņš University
Dr. phil.; Rīgas Stradiņa universitāte
E-mail / e-pasts: vija.sile@rsu.lv; ORCID: 0000-0002-5246-3790

Mairita Satika
Mg. sc. soc.; Rīga Stradiņš University
Mg. sc. soc.; Rīgas Stradiņa universitāte
E-mail / e-pasts: mairita.satika@rsu.lv; ORCID: 0000-0002-9394-0178

Vents Sīlis
Phd. sc. soc.; Rīga Stradiņš University
Phd. sc. soc.; Rīgas Stradiņa universitāte
E-mail / e-pasts: vents.silis@rsu.lv; ORCID: 0000-0002-5482-3147

DOI: 10.35539/LTNC.2026.0063.08

The Representation of Hybrid Warfare in Latvian Public Media (*LSM.lv*): An Analysis of the Last Decade

Hibrīdkara atspoguļojums Latvijas sabiedriskajos medijos (*LSM.lv*): pēdējās desmitgades analīze

Keywords:
hybrid warfare,
public media,
disinformation,
democracy,
values,
hybrid threats,
cybersecurity

Atslēgvārdi:
hibrīdkarš,
sabiedriskie mediji,
dezinformācija,
demokrātija,
vērtības,
hibrīddraudi,
kiberdrošība

Summary The term "hybrid war" entered the Latvian public discourse in 2015, after Russia annexed the Crimean Peninsula, which belonged to Ukraine. This fact confirms that hybrid warfare is a form of conflict that poses a real challenge to the West's traditional value system. Since 2015, the topic of hybrid warfare has become a constant focus of public media research. Over the past decade, hybrid warfare has become multifaceted, assuming increasingly diverse forms of expression. One of the forms of hybrid warfare is the redefinition of values, which pertains to the understanding of democracy.

The study examined the information space of Latvia's public media, conducting a thematic analysis of content related to the concept of hybrid warfare, which included 93 publications on *LSM.lv* over the past decade. The polymorphic nature of hybrid warfare poses a challenge in defining the boundary between truth and disinformation. The complex process of democratization of political systems in Eastern Europe and Latvia over the past decade has been influenced by a range of factors, among which hybrid warfare is becoming increasingly relevant – both as a phenomenon and as a topic of theoretical discourse. Since 2007, a number of books have been published that have become iconic, as well as countless articles offering a multifaceted analysis of military and informational dimensions of hybrid warfare, taking into account the unmistakable slowdown, stagnation, or even authoritarian tendencies in the functioning of democratic institutions.

Kopsavilkums Jēdziens "hibrīdkarš" Latvijas sabiedriskajā medijā ienāca 2015. gadā, kad Krievija anektēja Ukrainai piederošo Krimas pussalu. Šis fakts ir apliecinājums, ka hibrīdkarš ir konflikta veids, kas ir reāls izaicinājums Rietumu tradicionālajai vērtību sistēmai. Kopš 2015. gada hibrīdkara tēma ir kļuvusi par konstantu sabiedriskā medija pētniecības lauku. Pēdējā desmitgadē hibrīdkarš ir kļuvis daudzšķautņains, veidojot arvien jaunas izpausmes formas. Viena no hibrīdkara izpausmes formām ir vērtību pārdefinēšana, kas attiecas uz demokrātijas izpratni.

Pētījumā tika veikta hibrīdkara jēdziena satura tematiskā analīze Latvijas sabiedriskā medija informācijas telpā, aptverot 93 *LSM.lv* publikācijas. Hibrīdkara polimorfiskā forma ir izaicinājums patiesības un dezinformācijas robežu noteikšanai. Pēdējās desmitgades komplicēto politiskās sistēmas demokratizācijas procesu Austrumeiropā un arī Latvijā ietekmē virkne faktoru, kuru vidū aizvien aktuālāks kļūst hibrīdkarš – kā parādība un kā teorētiskā diskursa tēma. Kopš 2007. gada ir publicēta virkne grāmatu, kas kļuvušas ikoniskas, tāpat arī neskaitāmi raksti, kuros tiek piedāvāta daudzpusīga dažādu militāru un informatīvu hibrīdparādību analīze, ņemot vērā nepārprotamo demokrātizācijas procesa palēninājumu, sastingumu vai pat autoritārisma tendences demokrātisko institūciju darbībā.

Democracy in the Context of Hybrid Warfare

Democratization in Europe from the late 20th century into the 21st has been a multidimensional process. It influences not only prospects for economic growth but also the consolidation of democratic values and the stability of state institutions. Crucially, it cannot be regarded as irreversible. While economic development provides a necessary foundation for democracy, it is not in itself sufficient to secure democratic consolidation (Huntington 1993).

Political sociologist Larry Diamond observed in the *Journal of Democracy* (2015) that the global expansion of freedom and democracy, which reached its high point between 1974 and 2005 according to Freedom House data, has experienced regression since 2006 (Diamond 2015). The most recent Freedom House report (2024) underlines the persistence of this trend, noting a decline in individual freedoms for the 19th consecutive year (Freedom House 2025).

Additional evidence comes from *The Economist*'s annual Democracy Index, which evaluates regimes across five dimensions: electoral process and pluralism, government functioning, political participation, political culture, and civil liberties. Countries are then categorized as "full democracies," "flawed democracies," "hybrid regimes," or "authoritarian regimes " (Hoey 2025). The 2024 index revealed that in 130 of 167 countries assessed, levels of democracy either deteriorated or remained static (Hoey 2025). States in the so-called "gray zone" – those identified as hybrid regimes – are especially vulnerable, oscillating between pressures toward democratization and authoritarian retrenchment (Hoey 2025). This reflects a broader slowdown in the democratization process worldwide.

Against this backdrop, the concept of *hybrid warfare* has assumed increasing importance. Since the first attempts to define it in 2007, consensus on a comprehensive definition has proved elusive. Analysts emphasize that hybrid warfare straddles both international and domestic arenas, incorporates a diversity of actors, and employs a wide spectrum of methods – from conventional force to irregular tactics and disinformation campaigns. Its indeterminate character complicates both theoretical analysis and policy response, particularly in fragile democracies where institutional resilience is already under strain. The aim of this study is to examine how the concept of hybrid warfare has been represented in Latvian public media during the period from 2014 to 2024.

The Development of Interpretations of the Concept of Hybrid Warfare

F. G. Hoffman's seminal 2007 study *Conflict in the 21st Century: The Rise of Hybrid Wars* articulated the polymorphic nature of hybrid warfare. Hoffman defined hybrid warfare as encompassing a spectrum of conflict types, combining conventional military capabilities with a variety of unconventional tactics and formations. These range from terrorism, mass violence, and coercion to criminal activity directed against civilian populations. As he noted, "Hybrid warfare encompasses a range of different types of warfare, including conventional capabilities, irregular tactics and formations, acts of terror, including mass violence and coercion, as well as criminal disorder " (Hoffman 2007).

Hoffman's framework also underscores two defining features: the multiplicity of actors involved and the erosion of traditional boundaries between war and peace, and between combatants and civilians. This blurring extends beyond military operations to encompass the political sphere, including electoral manipulation, the fomenting of tensions between governments and societies, and the exertion of political and economic pressure.

Subsequent scholarship, particularly following Russia's annexation of Crimea and intervention in Ukraine in 2014, has placed greater emphasis on the military dimension of hybrid warfare. Analysts have examined the interplay between regular armed forces and irregular formations, including partisan groups and terrorist organizations. The events of 2014 also prompted renewed attention to the writings of General Valery Gerasimov, Chief of the Russian General Staff, whose 2013 article on modern conflict was retrospectively associated with Russian operations in Ukraine. Although often mischaracterized as a formal doctrine, "the Gerasimov Doctrine" became a shorthand for describing Russia's integration of military and non-military tools in hybrid conflict. The prominence of hybrid warfare in international discourse was reinforced at the NATO summit in Wales in September 2014, where it was explicitly linked to Russian aggression. Yet this expansion of the term's usage has contributed to its conceptual ambiguity. Despite its prevalence in both political rhetoric and public debate, a comprehensive and widely accepted definition remains absent. This lack of conceptual precision hinders the analytical utility of the term in both academic research and policy formulation, complicating efforts to develop coherent responses to the evolving character of contemporary warfare (Käihkö 2021: 116).

Hoffman's definition remains the most widely cited and, to date, the most comprehensive articulation of hybrid warfare. Yet a fully developed, broad definition that captures the concept's polymorphic character has not emerged. One reason is that the phenomenon itself continues to evolve. Initially, the term was applied to describe the combination of conventional armed forces with special forces. Hoffman

emphasized the fusion of regular and irregular means and methods (Käihkö 2021: 117). However, Russia's occupation of Crimea in 2014, achieved largely without direct lethal force, demonstrated novel tactics and forms of warfare not previously witnessed, giving renewed salience to the "hybrid" label. Following the annexation, considerable attention was directed toward the writings of General Valery Gerasimov. According to the reading of Russia's so-called "Gerasimov Doctrine", non-military measures can be deployed to destabilize a previously stable society, thereby justifying external intervention. The outcome is a "gray zone" conflict below the threshold of declared war, in which strategic non-military tools play a more decisive role than conventional armed force (Käihkö 2021:117).

Many elements associated with hybrid warfare echo earlier debates on "fourth-generation warfare," a contested concept that emerged in the 1990s. Its central premise was that advances in information technology had enabled non-state actors to erode states' willingness to fight by targeting decision-makers and the public through globalized, networked media and the internet. This broadened the scope of conflict to encompass cultural, social, legal, psychological, and moral dimensions, reducing the relative importance of military force (Wither 2016:78).

Similar parallels can be drawn with the theory of "unrestricted warfare" articulated by two People's Liberation Army colonels, Qiao Liang and Wang Xiangsui, in their 1999 book *Unrestricted Warfare*. Their argument was that states such as the People's Republic of China could offset adversaries' technological superiority by employing a wide range of military and non-military instruments. In their words, "the first rule of unlimited warfare is that there are no rules, and nothing is forbidden." The tactics outlined included cyberattacks, manipulation of financial markets and banking systems (i.e., financial warfare), terrorism, and disinformation. For Qiao and Wang, globalization and the rise of information technologies had irreversibly transformed the character of conflict, producing what they termed the "concept of new weapons " (Wither 2016: 78).

The breadth of hybrid threats has since been mapped in greater detail. In her article *Countering Hybrid Threats: Problematic Aspects in the European Region*, Eglė Štareikė draws on a framework developed by Bajarūnas and Keršanskas, which identifies the principal elements of hybrid threats (Štareike 2024: 230). These include: propaganda and disinformation; manipulation of mass media; cyberattacks; espionage; psychological operations; subversive activity; the politicization of culture, language, and religion; energy leverage; interference in elections; the mobilization of criminal groups; and the combined use of covert and overt military and paramilitary forces. According to Štareikė, they also extend to economic, financial, and social pressure, the exploitation of national or regional vulnerabilities, and the pursuit of objectives

through ambiguity and deniability. Nuclear blackmail is cited as a possible escalatory tool once hybrid operations have secured initial gains. The complexity of these threats is compounded by the broader stagnation of democratization, highlighted in the studies of Freedom House and *The Economist*. Both stress that particular attention should be directed toward states and regions at risk of democratic backsliding, where hybrid threats may exert the greatest pressure. The pillars of democracy identified by *The Economist*, i.e., electoral integrity, effective governance, political participation, political culture, and civil liberties, highlight the areas most exposed to such pressures. Strengthening these foundations is vital for enhancing democratic resilience, safeguarding the rule of law, and resisting authoritarian encroachment. Yet globally, the risks to democracy remain acute, as shrinking civic space and hybrid threats continue to erode the scope for genuine democratic governance (Štareike 2024: 230).

Legitimacy has been identified as one of the targets for undermining democracy, because citizens, by casting their votes in elections, demonstrate their trust in a democratic state. It is the citizens' right to uphold democratic values on the path to the nation's growth and development. Democracy is founded on political trust and social cohesion, which ensure the continuity of democracy. In today's climate of hybrid warfare and hybrid threats, the process of establishing the legitimacy of a trusted authority increasingly reflects the fragility and vulnerability of democracy during elections. The fragility of democracy is directly linked to increasing and heightened competition, emotions, and the "visibility" of political forces in the information sphere, which is turning into a competitive arena (Iarovyi 2025: 15). In this arena, political polarization intensifies, with disinformation serving as a tool during elections. It is considered the main driving force behind polarization, leading to the fragmentation of society. The election platform is used to polarize society through its existing narratives, widening the divide between different segments of society.

Disinformation campaigns – whether foreign or domestic – exploit these identifiable divisions and societal fragility to spread content that discredits political opponents, casts doubt on the integrity or fairness of the electoral process, or stoke identity-based grievances (Iarovyi 2025: 15). In the long term, public trust in the fundamental principles of democracy is gradually declining. Social media plays a significant role in this cyclical process, as content creators frame the information that enters the media landscape. From a theoretical perspective, the structuration theory developed by British sociologist Anthony Giddens draws attention to the duality of structure and agency, in which institutions and norms shape human behavior, while everyday practices simultaneously reproduce or transform those structures.

> This lens shows that resilience to disinformation is built not only through formal strategies – laws, policies, regulation – but also through informal practices of communication and interpretation (Iarovyi 2025: 16).

Structuration theory in the information space reflects a duality, as it highlights top-down interventions (such as platform policies) and bottom-up practices (such as user agency) that shape the information space. Social media, driven by various interests, can fragment information content, framing the public sphere, increasing societal polarization, and gradually eroding the legitimacy of democracy. Consequently, it can be concluded that Giddens' theory reflects the role of social media – they are structuring agents whose actions reflect and transform the digital public sphere. The specific power of social media stems from its hybrid position: embedded within macro-level systems – such as platforms and regulations – it operates through meso-level infrastructures, such as the media and NGOs, and directly influences micro-level perceptions. In this way, social media is attributed with a hitherto undefined ability to set the agenda, shape existing social norms, and amplify public reactions to various sensitive topics or issues (Iarovyi 2025). It can be concluded that even in a situation where the government establishes a legal framework for the media space to promote public awareness, openness, and transparency, the media, as structuring agents, shape public values, perceptions, and attitudes in both the political and social spheres by filling the information space.

When analyzing the past decade as a time of crisis, it is evident that disinformation campaigns targeting democratization processes, electoral practices, and public trust in government undermine public discourse, which is considered the epistemological foundation of democratic legitimacy. During this period, reliable information functions as a stabilizing force/power. In peacetime, freedom of speech is the cornerstone of liberal democracy, even in cases where it may create instability or threats in the information space (Iarovyi 2025). However, contemporary hybridity may challenge this position, as safeguarding the long-term existence of democracy requires a reassessment of the multifaceted nature of existing challenges. European Centre of Excellence for Countering Hybrid Threats in Helsinki defines hybrid threats as follows:

> Coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means; Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international); Activities aimed at influencing different forms of decision-making at local (regional), state, or institutional level, and designed to further and/or fulfil the agents' strategic goals while undermining and /or hurting targets (Hybrid CoE 2019: 10).

It can be concluded that the explanation of hybrid threats provided by the aforementioned definitions can influence disinformation campaigns, interference in the electoral process, the spread of conspiracy theories, manipulation aimed at dividing ethnic, religious, cultural, and other social groups – including various diasporas – as

well as cyberattacks, and increasing the risk of political and economic corruption, the infiltration of agents of influence into society, media control, the influence of the media landscape, as well as economic sanctions, covert and parliamentary activities, airspace violations, military exercises, arms proliferation, attacks on critical infrastructure, etc. (Ellingsen 2024). Based on the above, the fragility of elections in a democratic society undermines the integrity and fairness of election outcomes, a phenomenon referred to as "election interference." In her article "Hybrid threats as a threat to democracy ", researcher Tanja Ellingsen lists and provides a detailed analysis of 12 cases in Europe and the U.S. where electoral democracy has been compromised, involving clear instances of the distortion of factual information, cyberattacks, the use of propaganda, email leaks, "hacking" of politicians' private accounts, attacks on various social and ethnic groups, etc. It should be noted that the researcher points out that, according to the Oxford Internet Institute, the spread of propaganda and political disinformation was observed in 81 countries in 2020 alone (Ellingsen 2024:43). It is particularly emphasized that interference in the electoral process is multifaceted and complex, ranging from hacking/cyberattacks, bribery, pressure/intimidation, false claims, bots, pages, and videos, to playing on diasporic ethnic or religious identities, nurturing ethnic and religious differences, or issues regarding migration, climate, vaccines, gender, and sexuality, the EU/NATO, etc. The application of these tactics is facilitated by fundamental democratic values – freedom of speech, minority rights, religious freedom, pluralism, and a free and independent press, which directly shapes the information landscape in society. Although freedom of speech is one of the fundamental values of democracy, in the context of existing hybrid threats, it provides representatives of other political regimes with a space for disinformation to spread, thereby undermining democratic values. The Nordic countries have recognized the existing issues and identified the risks. The researcher emphasizes that disinformation and fake news have, overall, contributed to a toxic information environment in which it is becoming increasingly difficult for individuals to distinguish facts from fiction and malicious lies, thereby fostering a general distrust of the media landscape (Ellingsen 2024: 44). The media landscape as a whole has become one of the most fragile aspects of democracy, where the future of democratic legitimacy is potentially challenged through the electoral process. The multifaceted process of election interference employs tactics that erode the public's political trust in democracy. According to statistics published by the OECD, in 2021 only 49% of people living in OECD countries trusted their national governments (Ellingsen 2024: 46).

A critically thinking and educated society, as well as strengthening the information space with verified and truthful information, is one of the most pressing

and important mechanisms for safeguarding democracy. Strengthening the legal sphere is also crucial, by combating the spread of disinformation through cooperation between the political and economic spheres. Equally important is the security of the media sphere; its strengthening enables independent, high-quality journalism to provide accurate information. Journalists and the media play a decisive role in ensuring the integrity of democracy (Ellingsen 2024: 46). In the sustainability of the state, the media ensure the protection of the truthfulness of information by pointing out real and potential threats. This article examines public media, which play this special role in providing reliable information and fostering critical thinking. The role of the media in a democratic society is to inform the public and critically evaluate not only political processes but also the decisions made, thereby promoting media literacy. The public benefit of such information is the ability to influence government structures, but in the context of hybrid warfare, such opportunities are narrowed. The fact that media freedom in the EU is threatened by disinformation is clearly demonstrated by the European Commission's strategic decisions, which are reflected over a ten-year period. A type of content analysis – thematic analysis – is used, as it most clearly illustrates the current issues and the context of the real threat to democracy.

Hybrid Threats as Security Challenges: The European Commission's Strategic Responses (2016–2024)

From 2016 onwards, an increasing number of institutions became engaged in assessing the security environment in Europe. In 2017, the European Commission (EC) published a report on the necessity of addressing hybrid threats. The report, *Joint Report to the European Parliament and the Council on the Implementation of the Common Framework for Countering Hybrid Threats – The European Union's Response* (European Commission 2017), frames hybrid threats as a security challenge unprecedented in the history of the EU. The term encompasses cyberattacks, disinformation campaigns, and media manipulation, all of which target fundamental European values, particularly freedom and democracy.

The 2017 EC report outlined an action plan to counter hybrid threats and to enhance the security and resilience of the EU, its Member States, and its partners. The plan set out a structured set of measures, including the identification of hybrid threats, improvement of situational awareness, the building of resilience, protection of critical infrastructure, promotion of common EU values, and the prevention of radicalization (European Commission 2017). Subsequent reports have continued to

focus on threat mitigation and prevention, reflecting the evolving nature of hybrid threats. In parallel, a decision was made to establish the European Centre for Countering Hybrid Threats, inaugurated in Finland in April 2017. Then ten EU Member States (Estonia, Finland, France, Germany, Latvia, Lithuania, Poland, Spain, Sweden, and the United Kingdom), together with Norway and the United States, actively participate in the Centre, while both the European Union and NATO provide institutional support. (European Commission 2017) By 2018, countering hybrid threats had become a core area of EU–NATO cooperation, reflecting recognition that the combined resources and capabilities of both organizations enhance the capacity of Member States and allies to prevent, deter, and respond to such threats (European Commission 2018).

Between 2016 and 2024, the evolution of hybrid threats in Europe can be traced through the European Commission's annual reports and related publications. Official EU assessments and policy documents reveal how such threats have developed over time, exploiting vulnerabilities in democratic institutions and critical infrastructure, while simultaneously prompting the European Union and its Member States to strengthen resilience and safeguard fundamental values.

2016: Events since April 2016 indicate that hybrid threats were still frequently assessed in isolation. Nevertheless, there was a *growing recognition and understanding* within the European Union of *the hybrid nature of some activities observed* and the need for a coordinated response. (European Commission 2017)

2017: Hybrid threats became less immediately visible when aimed at *influencing public opinion through disinformation campaigns and media manipulation*. These efforts sought to undermine fundamental European values, including human dignity, freedom, and democracy. (European Commission 2017) The systematic dissemination of fake news on social media emerged as a prominent tool to discredit governments, institutions, and electoral processes, creating societal confusion and eroding trust in democratic structures. At this stage, fake news was mostly spread on online platforms.

2018: Strengthening *societal resilience and protecting critical infrastructure* such as transport, communications, energy, space, and financial systems became a priority. Collaboration with NGOs was established to monitor terrorist groups and intermediaries. (European Commission 2018) The increasing frequency of *cybersecurity* incidents highlighted the necessity of *political-level coordination*, including measures to identify sources of terrorist financing and to prevent money laundering. The Commission also prioritized the removal of illegal online content and the prevention of violent radicalization, both online and offline. A code of conduct to combat illegal hate speech online was agreed with major technology platforms, including Facebook, Twitter, Google (YouTube), and Microsoft.

2019: Efforts expanded to include cybersecurity in the context of elections. Combating disinformation, enhancing election protection, and promoting cooperation in the defense industry were formally added to the EU's hybrid threat priorities (European Commission 2019).

2020: The COVID-19 pandemic was exploited by hybrid actors to manipulate the information environment, including disinformation, election interference, and cyberattacks. State and non-state actors sought to undermine EU values through financial and economic pressure, cyber espionage, and targeted disruption of public trust (European Commission 2020). The European Union established a dedicated group to counter intelligence-related activities, including *election-related hacking, malicious operations on social media platforms, state-sponsored cyber capabilities, cyber espionage, and the dissemination of disinformation*. In addition, a specific tool was developed to combat misinformation and disinformation across digital and traditional media channels. *Cyberattacks* targeting European institutions and attempts to *undermine their leadership* had been documented, while disinformation in the context of elections had notably intensified. Concurrently, there was a rise in both direct and indirect financial support and economic pressure exerted on political actors, alongside disruptive activities undertaken by civil society, further complicating the EU's security environment (European Commission 2020).

2021: The EU budget was allocated to support projects aimed at enhancing resilience to hybrid threats across critical sectors, including energy, space, water supply, health, transport, communications, and finance (European Commission 2021). The 2021 report shows that in September 2020 the Commission adopted a proposal for a screening regulation, designed to improve the management of mixed migration flows by ensuring the rapid identification of migrants' identities and any potential security risks. This measure also sought to strengthen the structured approach to customs risk management, enhance the effectiveness of controls, and mitigate both financial and non-financial risks to the EU and its citizens, while maintaining the competitiveness of legitimate businesses. In November 2020, the European Commission reached a political agreement on a proposal for a new export control regulation, significantly enhancing the EU's capacity to address security risks within strategic supply chains. The regulation also referenced a range of crises (health, political, economic, and environmental) as well as hybrid threats that may disrupt the functioning of critical systems, including food supply chains. At the same time, traditional Public-Private Partnership (PPP) cooperation in the field of cybersecurity had become increasingly challenging. The COVID-19 health crisis had additionally been exploited through specific hybrid methods, highlighting the evolving and multifaceted nature of contemporary security threats (European Commission 2021).

2022: Although the responsibility for countering hybrid threats continued to rest primarily with Member States, the European Union played a complementary role by supporting coordination, enhancing situational awareness and resilience, cooperating with like-minded countries and organizations, and ensuring joint response capabilities in the event of hybrid campaigns. (European Commission 2022) Hybrid actors sought to disrupt, divide, and redefine European security architecture, challenging the international rules-based order. The EU faced increasingly frequent cyberattacks targeting critical infrastructure, alongside foreign information manipulation and interference aimed at undermining the foundations of democracy. Russian state-owned media and affiliated actors further contributed to this trend by spreading narratives and war propaganda for economic gain (European Commission 2022). The Commission also addressed operational requirements for threat detection equipment and explosives precursors used in public spaces. Radicalization and violent extremism acquired an increasingly prominent digital and cyber dimension, as terrorist groups exploited information and communication technologies to plan and execute attacks. This evolving threat landscape underscored the EU's need to prevent terrorists from exploiting emerging technologies (European Commission 2022).

2023: Hybrid tactics continued to be employed by states and non-governmental actors against democracies, targeting fundamental values, dividing societies, and undermining political decision-making. In Europe, this trend was exacerbated by Russia's continued aggression against Ukraine in 2022 and 2023, alongside hybrid campaigns directed at the EU and its partners, aiming to weaken their unity and solidarity with Ukraine. Foreign information manipulation and interference (FIMI), together with cyberattacks, remained among the most prevalent forms of hybrid influence. Additionally, the strategic use of energy as a coercive tool and acts of sabotage, such as those targeting the Nord Stream gas pipelines, highlighted the urgent need to strengthen the resilience of critical infrastructure across the EU (European Commission 2023).

2024: The direct and indirect cross-border consequences of hybrid threats were evident not only in Russia's ongoing aggression against Ukraine but also in the emerging conflict between Hamas and Israel. In light of the forthcoming elections across Europe, a series of measures were implemented during the reporting period to enhance democratic and electoral resilience. In May 2024, Member States achieved notable progress in establishing an EU rapid response unit for hybrid threats through the formal adoption of operational guidelines. Over the same period, engagement with NATO was intensified, and new structured dialogues were initiated on issues relating to space, climate and security, as well as on emerging

and disruptive technologies – areas recognized as critical for the effective prevention and mitigation of hybrid threats.

To summarize, over the past decade, the European Union has developed a progressively comprehensive and multi-layered strategy to address hybrid threats, reflecting both the evolving complexity of such threats and the need for coordinated action across Member States and international partners. The strategy integrates measures to strengthen societal resilience, safeguard critical infrastructure across sectors including energy, transport, health, communications, space, and finance, and protect democratic institutions and processes from disinformation, election interference, and cyberattacks. It emphasizes enhanced situational awareness, intelligence-sharing, and cooperation with like-minded countries, NGOs, and technology platforms, alongside the development of specialized regulatory frameworks, screening mechanisms, and export control measures to mitigate financial, economic, and strategic vulnerabilities. The EU has also institutionalized rapid response capabilities, including the establishment of a dedicated hybrid threat unit and structured dialogues on emerging and disruptive technologies, space, climate, and security. Central to this approach is the recognition that hybrid threats operate across military, political, economic, informational, and technological domains, often exploiting crises and societal vulnerabilities to undermine fundamental European values. The strategy reflects a shift from reactive, *ad hoc* measures to proactive, integrated, and multi-level responses designed to enhance democratic resilience, protect critical infrastructure, and uphold the rules-based international order in the face of increasingly sophisticated and cross-border hybrid challenges.

Manifestations of Hybrid Warfare in Latvia

In 2025, Latvia has experienced a marked escalation of hybrid threats, encompassing sabotage of critical infrastructure, cyberattacks on municipalities, arson, vandalism, GPS jamming, the militarization of migration, and direct military intimidation. Such pressures are most acute in the Baltic states, alongside Poland and Germany, which are identified as being at the highest risk (Industrial Cyber 2025). While Latvia is not directly involved in armed conflict, its position as an external border of the European Union renders it especially vulnerable to the full spectrum of hybrid tactics.

As early as 2014, Jānis Bērziņš, a researcher at the National Defense Academy of Latvia's Centre for Security and Strategic Research, highlighted this emerging phenomenon in his article *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. He described a "new generation" of warfare that can be implemented only under conditions in which a favorable environment has been

established. According to Bērziņš, Russia can execute strategic actions based on specific phases of this warfare. Within the Latvian context, he observed that the first phase of this strategy is already being pursued through non-military asymmetric tactics, such as the broadcasting of Russian propaganda channels, the granting of Russian citizenship to Latvian non-citizens, pseudo-civic rights movements, and the activities of pro-Russian political parties. This approach represents an opportunistic strategy that, if successful, could facilitate the implementation of subsequent phases of this new form of warfare. Bērziņš emphasizes that the creation of conducive conditions is largely dependent on Latvia's own policies and actions (Bērziņš 2014). His conclusions raise critical questions regarding the future political agenda for national security, including the potential need to strengthen the media space as part of Latvia's broader security strategy.

The events of 2014 prompted a reassessment of security policy, not only with respect to the EU's eastern border but also at the level of the European Union as a whole. This issue was addressed at a conference held in Riga in February 2015. The EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, emphasized the importance of collective action, stating: "It is important to come together and unite, not only militarily, but also on a broader scale" (Krops 2015). Security policy thus became a pressing item on the European Union's agenda, with member states being urged to explore avenues for cooperation in order to address growing threats from external actors. At the same time, commenting on Mogherini's call for mutual cooperation, Žanete Ozoliņa, Professor of Political Science at the University of Latvia, expressed skepticism, saying, "Europe is too diverse to be able to agree on a single defense minister in the face of the current threats" (Sprūds et al. 2016).

Although the diversity of the European Union presents a factor that may hinder the development of a unified strategy, it is important to note that there is a growing institutional awareness that the threat of hybrid warfare must be examined at both international and local levels. One example of such research was conducted by the NATO Strategic Communications Centre of Excellence (NATO StratCom COE) in collaboration with the Latvian Institute of International Affairs and Riga Stradiņš University. The study, entitled *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*, aimed to analyze organized pro-Russian trolling in online media and assess its impact on public opinion in Latvia (Sprūds et al. 2016).

By examining the comments sections of various social media platforms, the study provided detailed insights into the dynamics of public discourse and highlighted the vulnerability of society to disinformation. One of the key conclusions drawn was the necessity of internet safety campaigns to mitigate such risks (Sprūds et al. 2016).

In 2021, the Academic Publishing House of the University of Latvia published a book on security policy in Latvia, titled *Latvian Residents' Subjective Perception of Security: Impact on Security Policy-Making*. The research reflected in this publication offers a comprehensive evaluation of factors that directly and indirectly influence individuals' living conditions from a security perspective (Struberga et al. 2021). Notably, the study gave special attention to hybrid threats, recognizing them as a highly debated issue within security research, as well as in the political, media, and public spheres (Struberga et al. 2021). Researchers Struberga and Ceple emphasized the significance of hybrid threats, defining them as: "hostile, coordinated actions by state and non-state actors that involve two or more threats simultaneously and are aimed at causing harm to the target country by influencing decision-making at the local, regional, national, or international institutional level" (Struberga et al. 2021).

This definition underscores the multifaceted nature of hybrid threats, which can manifest in political, economic, and informational domains, and can be applied with varying degrees of intensity. It is crucial to recognize that the combination of different types of threats can give rise to new forms of hybrid threats (Struberga et al. 2021). Moreover, the inherent unpredictability and variability of hybrid threats suggest that they may represent an increasingly pervasive security challenge at the state level. It follows, therefore, that merely identifying hybrid threats within the context of hybrid warfare is insufficient; it is equally imperative to advance the development and strengthening of international legal frameworks, thereby facilitating mechanisms for the timely mitigation and neutralization of such security threats.

In this context, it is worth noting the work of Valērijs Bodnieks, a researcher at the National Defence Academy of Latvia, who, in an article published in May 2023 entitled *Defensive Lawfare and Deterrence: Analysis of Latvia's Approach to Legal Bases in the Context of Hybrid Warfare (2014–2022)*, emphasizes that Western society is founded on legality, democracy, respect for human rights, and international law. The principal mechanism for individual and collective self-defense is enshrined in Article 51 of the UN Charter, with each state adapting international legal regulations, including the laws and customs of war and human rights frameworks, to the national context for deterrence purposes (Bodnieks 2023: 57). Following the events of 2014 and the occupation of Crimea, discussions regarding hybrid warfare intensified, highlighting the disruption of previously well-understood, law-based international order. Bodnieks identifies the organized flows of refugees from Russia and Belarus as a clear instance of legal warfare targeting Latvia, Lithuania, and Poland, primarily manifesting as violations of human rights. Equally significant is Russia's comprehensive use of hybrid warfare against Ukraine, employing military and non-mil-

itary means, covert operations, and armed groups with the long-term objective of undermining international principles and the authority of international law. Today, Russia asserts a self-proclaimed right to interfere with and challenge the existing international order, exerting both destructive and non-destructive influence over targeted states (Bodnieks 2023: 58). In the Latvian context, Russia seeks to influence security through a variety of measures, including propaganda, psychological operations, cyber activities, support for agents of influence, and operations in border regions (Bodnieks 2023: 59). In response to these threats, both legal and informational measures are essential to strengthen Latvia's information space and mitigate the impact of hybrid warfare on society.

Currently, there is no precise definition of hybrid warfare in Latvian legislation or political discourse. The Latvian National Security Concept, adopted on 28 September 2023, addresses only one element of hybrid warfare (cybersecurity), which is considered in detail through the *Cybersecurity Strategy 2023–2026* (Government of Latvia 2020) and the *National Cybersecurity Law* (Government of Latvia 2022). The development of these instruments can be understood in the context of the EU's *Security Union Strategy*, in which cybersecurity is integrated into one of four strategic pillars. The first pillar addresses the future security environment, encompassing the protection and resilience of critical infrastructure, cybersecurity, and the safeguarding of public and social spaces. The second pillar focuses on responses to emerging threats, including cybercrime, modern law enforcement, the removal of illegal online content, and hybrid threats. The third pillar concerns the protection of European citizens against terrorism and organized crime, further subdivided into areas such as illegal drugs, child sexual exploitation, arms smuggling, and 5G security. The final pillar seeks to establish a robust security ecosystem, encompassing mutual cooperation, information sharing, strong external borders, strengthened research and innovation, and the promotion of skills and individual awareness (European Commission 2020). Collectively, this framework demonstrates that the EU's common security strategy addresses an increasingly broad range of issues that may directly influence the future of the Union.

Although cyber security receives the greatest attention within Latvia's political arena, research also provides analyses of hybrid warfare specific to Latvia. For instance, the Latvian Institute of Foreign Affairs' 2025 publication, *Hybrid War Thinking Hobbles Europe's Response to Russian Sabotage* (Wilde 2025), together with NATO's Strategic Communications Centre of Excellence study *The Context of Russia's Information Influence* (Ahonen et al. 2024), examine the impact of hybrid warfare on an ethnically divided society. Ethnic divisions are considered a potentially conducive environment for the implementation of hybrid threats, making this a particularly

salient and pressing issue in Latvia's political discourse (Bērziņa 2026, this issue; Griķe, Raubiško 2026, this issue).

Taken together, the Latvian experience illustrates both the persistence and the adaptability of hybrid warfare as a security challenge. From the early recognition of Russian asymmetric tactics in 2014 to the pronounced escalation of hybrid threats in 2025, the discourse has shifted from tentative conceptualization to urgent policy debate. Yet the absence of a precise legal definition in Latvian or European frameworks underscores the enduring difficulty of operationalizing a comprehensive response. What emerges instead is a layered approach: legal and informational measures at the national level, paralleled by broader EU strategies aimed at resilience and collective security. Latvia's case highlights not only the vulnerabilities inherent to small states on the Union's external border, but also the ways in which hybrid warfare exploits social, political, and technological divides. The challenge ahead lies in bridging the gap between conceptual recognition and effective deterrence, while ensuring that the defense of security does not come at the expense of the democratic values it seeks to protect.

Reflection of Hybrid Warfare in Latvian Public Media: Analysis of the Last Decade

Latvian public media is an electronic media outlet whose overall strategic goal is to strengthen Latvia's democratic system and freedom of speech (Government of Latvia 2021). As stipulated by law, public electronic media encourage the participation of Latvian society in political, social, and cultural processes, strengthen national security, and adhere to the fundamental principles of quality journalism. The study examined publicly available articles on the topic of "hybrid warfare" published on the *LSM.lv* public news portal over the last decade to observe the dynamics and quality of publications. The portal was selected due to its high traffic and significance in informing the Latvian public. According to a study conducted by Gemius Audience in April 2025, *LSM.lv* ranked fifth among the "most visited websites," recording 664,064 visits, despite experiencing a decline of 32,000 users compared to 2024 (Gemius 2025). This indicates that Latvian public media maintains a sufficiently large audience, thereby providing substantial scope for informing and educating the public.

The analysis considered the *Law on Public Electronic Media and its Management, Latvian Public Media: Code of Conduct and Ethics*, and *Latvian Public Media: Editorial Guidelines*. Article 2 of the law stipulates that the overall strategic objective of public electronic media is to strengthen Latvia's democratic system, freedom of speech,

and residents' sense of belonging, as well as to preserve the Latvian language and national culture in accordance with the Constitution and relevant legislation (Government of Latvia 2018). The Code of Conduct clearly states that employees must perform their duties in alignment with core public media values, namely independence, reliability, and human dignity. These values inform both the day-to-day operations of the media and the content it produces (SEPLP 2025).

Despite academic research indicating a growing understanding of hybrid warfare, disinformation has notably increased, particularly during election periods. This underscores the importance of further exploring public media's contribution to informing citizens about hybrid warfare. Given that the European Commission has developed recommendations and mechanisms to enhance public resilience against hybrid threats, the role of public media in explaining these concepts becomes especially critical. The situation is detailed in the European Commission's annual reports from 2016 to 2024. The study conceptually analyses the contribution of the national public media portal to informing the public about hybrid warfare (or hybrid threats), including the forms in which such threats manifest and the political actors involved in their implementation.

The publications from the decade under review are dominated by several types of information, which are presented quantitatively in Table No .1.

Table 1. Types of information in the "Hybrid War" section on *LSM.lv*

Year	News	Inter-view	Scientific confe-rence	Political confe-rence	Scientific research	Expert opinion	Resolu-tions	Other
2015	–	3	1	1	6	3	–	–
2016	6	2	–	1	1	1	2	–
2017	4	2	–	–	1	–	–	1
2018	1	2	–	–	1	1	–	–
2019	1	2	–	–	–	–	–	1
2020	–	–	–	–	–	–	–	–
2021	2	6	–	–	–	3	–	1
2022	2	2	–	–	–	–	–	–
2023	7	3	–	–	–	3	–	1
2024	2	3	1	–	–	5	–	2

Source: (Table created by the authors using data from the study "The Representation of Hybrid Warfare in Latvian Public Media (*LSM.lv*): An Analysis of the Last Decade.")

Among the types of information that quantitatively predominate over the others, three genres stand out: news and interviews (in equal numbers), and expert opinions. Some publications include both news and interviews. Notably, in 2014, the *LSM.lv* news portal did not publish a single article on the topic of "hybrid warfare," highlighting the evolution of public attention to this issue over the subsequent decade.

In 2015, *LSM.lv* made an initial attempt to explain the concept of hybrid warfare, though coverage remained superficial and failed to address the essential elements characteristic of such warfare. During this year, a total of sixteen articles were published. Several recurring themes can be identified in these publications:

1. Pessimism among political scientists regarding the feasibility of joint action by EU states against hybrid warfare, highlighting a tension between the creation of security institutions on the one hand and the contradictory views of Latvia's political leadership and other political scientists on the other.
2. A lack of comprehensive explanation of the concept of "hybrid warfare" and its manifestations. Coverage focused primarily on the activities of the so-called "little green men" in Crimea, without addressing the broader strategic and non-military dimensions.

In 2016, *LSM.lv* published eleven articles on the topic of hybrid warfare. At the beginning of the year, coverage primarily focused on the non-military components of hybrid warfare. Several key themes emerge from the reporting:

1. Emphasis was placed on the informational dimension as a potential countermeasure, specifically the strategy of "ignoring" disinformation. Security experts, however, expressed skepticism regarding the effectiveness of this approach. By mid-year, the discourse shifted toward calls for more proactive counteraction.
2. Informational propaganda, manifesting as aggressive communication from Russia, was identified as a core non-military component of hybrid warfare.
3. *LSM.lv* introduced its "troll diary," analyzing comments on articles across various news portals. The diary highlighted how hybrid warfare methods engage civilians in the conflict by providing opportunities to comment on commercial media, thereby expanding the informational theater of conflict into the public sphere.
4. The concepts of hybrid warfare and hybrid threats appeared for the first time in the reporting, explicitly linking them to the terminology adopted in the European Commission's reports, where "hybrid threats" became the dominant concept.
5. Despite the number of publications, there remained no clear or consistent definition of hybrid warfare or hybrid threats within the media coverage.
6. Within the framework of EU–NATO cooperation, agreement was reached on forty aspects of collaboration addressing hybrid threats and cybersecurity, signaling growing institutional recognition of these issues.
7. Finally, the Minister of Foreign Affairs confirmed the applicability of NATO Article 5 in situations of hybrid warfare, underlining the relevance of collective defense mechanisms in responding to hybrid threats.

Overall, the reporting in 2016 reflects a nascent but evolving understanding of hybrid warfare in Latvian public media, moving from an initial emphasis on non-military components toward recognition of institutional and international frameworks for countering hybrid threats.

In 2017, *LSM.lv* published eight articles addressing the topic of hybrid warfare. The coverage primarily emphasized the role of disinformation, aligning with the European Commission's focus on the issue. The portal also published polarizing content designed to generate tension and discord within society. Notably, hybrid threats began to acquire an official status within the Latvian media space. However, no articles linked hybrid warfare explicitly to cyber operations; instead, *LSM.lv* maintained separate sections for hybrid threats and cybersecurity, which may have led to a perception among readers that the two topics are unconnected.

In 2018, reporting on hybrid warfare decreased markedly, with only a single article covering the US Senate elections under this topic. In contrast, the portal published two articles on hybrid threats and 23 articles on cybersecurity, signaling a growing editorial focus on digital security rather than the broader conceptualization of hybrid warfare.

In 2019, *LSM.lv* published two articles on hybrid warfare, ten on hybrid threats, and sixteen on cybersecurity. Within these publications, the media introduced the term "hybrid attack," highlighting Finland's initiative to train EU ministers (across foreign affairs, internal affairs, and related portfolios) on appropriate responses. Additionally, disinformation disseminated via social networks, often based on anonymous reports concerning banking activities, was noted as a continuing concern.

By 2020, the term hybrid warfare did not appear in *LSM.lv* publications. Coverage instead comprised fourteen articles on cybersecurity and two articles on hybrid threats. This shift reflects an increasing media focus on digital vulnerabilities and cyber resilience, rather than on hybrid warfare as a multidimensional concept encompassing both military and non-military components.

In 2021, *LSM.lv* publications incorporated all three key concepts: hybrid warfare (seven articles), hybrid threats (six articles), and cybersecurity (thirty-five articles). Articles addressing hybrid warfare primarily focused on migration-related issues. Belarusian propaganda highlighting the inhumane conditions of illegal migrants was widely reported, alongside information that more than 4,000 migrants (predominantly from Iraq and Syria) had crossed the Belarus–Lithuania border, an operation openly orchestrated by Belarusian leader Alexander Lukashenko. The coverage noted the polarizing effects of migration on political parties in Sweden and Germany, while also emphasizing the intensification of hybrid aggression against Lithuania via illegal migration flows during the COVID-19 pandemic. Publications revealed highly

divergent public opinions on illegal migration, reflecting growing societal polarization on this issue. The European Union's commitment to strengthening its external borders was also highlighted.

In 2022, coverage reflected the increasing diversity of hybrid warfare manifestations. *LSM.lv* published three articles on hybrid warfare, six on hybrid security, and thirty-eight on cybersecurity. The public was informed about potential Russian hybrid attacks against Ukraine, although the start of Russia's conventional war in Ukraine was not discussed in the context of hybrid warfare. Migration issues at the Latvian–Belarusian border continued to be covered, with an emphasis on humanitarian considerations in the treatment of illegal migrants.

In 2023, *LSM.lv* published thirteen articles on hybrid warfare, fourteen on hybrid threats, and twenty-four on cybersecurity, with all publications relating to illegal migration as a manifestation of hybrid warfare. Coverage included reports on hybrid warfare operations in Moldova, notably protests against President Maia Sandu in response to the country's NATO accession ambitions. The head of the Latvian Constitutional Protection Bureau conveyed a public view suggesting that "we have overestimated Russia's capabilities in hybrid threats."

The arrival of the Russian mercenary group Wagner in Belarus was reported to increase risks at the Latvian–Belarusian border, with migrants being deployed as instruments of hybrid warfare against the European Union. Border Guard Chief Guntis Pujāts confirmed that Latvia had become a target country for hybrid warfare owing to the intensification of illegal migration. Analysts at the US-based Institute for the Study of War (ISW) indicated that Russia was using hybrid tactics to artificially generate a migration crisis on the Finnish border. The publications also highlighted signs of societal polarization resulting from migration pressures, with Jussi Lasila, senior researcher at the Finnish Institute of International Affairs, noting the increasing division of public opinion. Statements from the Finnish Foreign Minister further reinforced the hybrid threat perspective, asserting that "our NATO allies and our friends in the European Union clearly understand that this is a hybrid attack and has nothing to do with normal migration or seeking asylum " (Šukurovs 2023).

In 2024, *LSM.lv* published twelve articles on hybrid warfare, seven on hybrid threats, and thirty-four on cybersecurity, reflecting a broadening of public discourse on the various forms of hybrid warfare. Information from the Ministry of the Interior highlighted the potential use of hybrid warfare against Latvia in the form of provocations. The concept of hybrid warfare was increasingly understood in a comprehensive sense, extending beyond conventional security threats and cyberattacks to include attacks on societal values and human consciousness. These tactics sought to exacerbate societal polarization using sensitive issues such as

religion, sex, ethnic relations, and nationalism, whereby even a minor spark could trigger tension and outbreaks of violence (Grūbe, 2024).

Public reporting also documented instances of Russian sabotage, fires, and violent attacks by illegal migrants on border guards in Poland. Polish Foreign Minister Radosław Sikorski noted that Russian and Belarusian services were effectively controlling the situation on Poland's eastern border, instructing migrants on how to target Polish soldiers and border guards (Plūme 2024). Warnings were also issued regarding efforts to promote chaos and sabotage in other European states.

End of the year publications emphasized the necessity of enhancing security and implementing countermeasures in the digital environment, particularly in response to growing cyber threats. Among the state-initiated countermeasures, particular emphasis was placed on the legal right to restrict border violators from totalitarian regimes in exercising asylum rights.

Table 2. The content framework of the "Hybrid War" section on *LSM.lv*

Year	Info	Cyberattacks	Social polarization	Critical infrastruc.	Economic security	Political security	Social values	Border security	Migration	Internal security	Definition	Countermeasures
2015	8	–	–	–	–	–	1	–	–	–	4	6
2016	6	–	–	1	1	2	1		1		1	8
2017	3	–	3	–	–	–	3	–	–	–	1	3
2018	1	1	–	–	–	1	–	–	–	–	–	–
2019	3	–	–	–	–	–	–	–	–		1	3
2020	–	–	–	–	–	–	–	–	–	–	–	–
2021	1	1	2	–	–	–	–	2	11	3	1	8
2022	–	–	–	–	–	–	–	2	2	–	2	1
2023	1	–	1	–	–	–	–	10	8	–	5	8
2024	–	1	–	1	–	–	1	5	4	3	2	6

Source: Table created by the authors using data from the study "The Representation of Hybrid Warfare in Latvian Public Media (*LSM.lv*): An Analysis of the Last Decade."

Given that the understanding of the concept of hybrid warfare/hybrid threats has evolved over a ten-year period, a shift in the discourse from abstract concepts

to more concrete terms has been observed. Initially, 23 publications provided information solely on the fact of hybrid warfare as such. A thematic content analysis shows that a significant number of publications begin with those on social values (6), followed by publications on border security (19). From 2021 onward, the topic of migration enters the publications, as a noticeable increase in illegal migration has been observed in practice from 2021 to 2024; in total, this amounts to 26 publications. Unfortunately, there is no correlation between publications on the rise in migration and those addressing internal security issues: only 3 publications in 2021 and 3 publications in 2024. Despite the fact that the concept of hybrid warfare is still being refined in terms of content, a stable trend is observable – the number of publications addressing countermeasures to prevent hybrid warfare/hybrid threats is increasing (42 publications). Countermeasure publications play a crucial role:

> If, in the process, democratic ideals are compromised, then democracy may be as well (Kruks, Skulte 2022: 202).

The year 2025 is notable for the merger of *LSM.lv* with *Latvijas Televīzija* (Latvian Television) and *Latvijas Radio* (Latvian Radio), forming a unified Latvian public media platform. Publications reviewed from this year demonstrate an increase in analytical depth and a focus on the practical utility of information for the public. Coverage in the context of hybrid warfare included twenty-two articles on hybrid warfare, five on hybrid threats, and ten on cybersecurity.

Several key themes emerge from the 2025 coverage. Due to the vulnerability of critical infrastructure, discussions increasingly emphasized limiting access to sensitive information. Rihards Bambals, the former Director of the Strategic Communications Coordination Department at the State Chancellery, highlighted that information warfare constitutes a core component of Russia's broader war strategy. According to Bambals, state-funded public media can counter this strategy through three pillars: firstly, by improving communication between the state and citizens to reduce disinformation; secondly, by ensuring an independent and secure media environment; and thirdly, by strengthening media literacy and public resilience (Grūbe 2025). Resilience, in this context, encompasses the ability to critically evaluate sources, verify headlines, and engage with media content responsibly.

The concept of hybrid warfare was further expanded to include analysis of sensitive narrative topics, such as health and economic issues, targeting specific social groups through manipulative tools, including deepfakes, trolls, and bots. Minister of the Interior Rihards Kozlovskis described the situation as "a real phase of sabotage and diversion," noting that 2024 marked the outbreak of hybrid warfare (Šņore 2025). NATO's response was critiqued for underestimating the integration of hybrid warfare into conventional military operations (Arnicāns 2025).

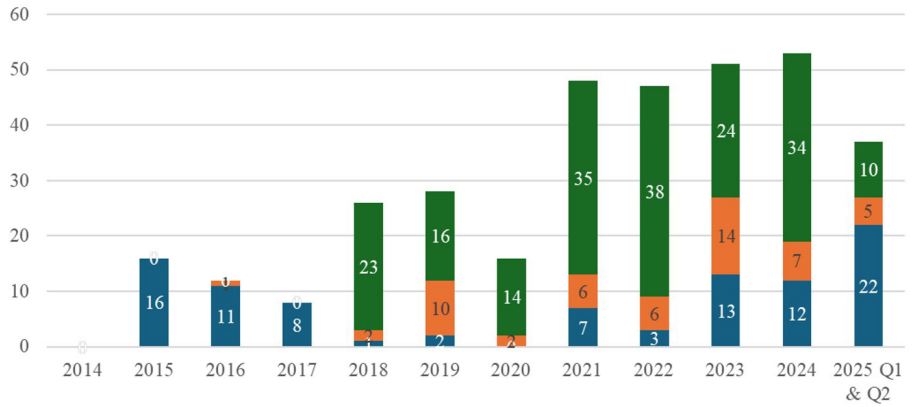

Figure 1. Evolution of *LSM.lv* reporting on hybrid warfare, hybrid threats, and cybersecurity, 2014–2025

Coverage also reflected the growing emphasis on restricting migration, with proposals for tighter controls over the residence of third-country nationals. Publications introduced the concept of "disposable agents," recruited via social media to conduct cyberattacks, arson, vandalism, sabotage, and the dissemination of disinformation across Europe (Nagla 2025). The Czech intelligence service reported the recruitment of migrants for surveillance activities, including filming military bases, Ukrainian support centers, and logistics hubs. A new psychological mechanism of hybrid warfare was also identified, wherein disinformation actors exploit social networks to establish romantic relationships as a means of luring targets, as exemplified by a case in Bulgaria.

Results

The topic of "hybrid warfare" was examined by analyzing publications on the Latvian public media portal *LSM.lv*, where content is published in Latvian, Russian, and English. Given that Latvian is the only official language of the Republic of Latvia, as confirmed in the preamble to the Constitution, this study focused on content published in Latvian. The volume of analyzed material did not allow for a comparative review of content published in Russian and English, which will be examined in the next phase of the study.

In total, 93 publications were reviewed during the period from January 1, 2015, to July 21, 2025. The main unit of analysis was the term "hybrid war," although the related concepts of "hybrid threats" and "cyber threats" were also listed but not analyzed in greater detail. It should be noted that 2020 – the year dominated by the COVID-19 pandemic – was the only year in which the term "hybrid war" did not

appear in the publications; instead, fourteen articles on cybersecurity and two on hybrid threats were published.

Following the 2025 merger of *LSM.lv* with *Latvijas Televīzija* and *Latvijas Radio*, both the presentation and the analytical depth of publications increased significantly. The number of articles specifically addressing hybrid warfare also reached its highest level by 21 July 2025, reflecting a strengthened editorial focus and heightened public engagement with the topic.

Conclusions

With global indices recording democratic backsliding, hybrid warfare has become a central tool of authoritarian influence, blending conventional and unconventional means across political, economic, informational, and military domains. Exemplified by Russia's tactics in Crimea, such threats exploit technological interconnectivity and weak institutions, exposing vulnerable states and underscoring the need to strengthen democratic resilience and the rule of law.

The European Union has increasingly positioned itself as both a guarantor of democratic resilience and a target of hybrid threats. EU mechanisms such as the Rule of Law framework, annual monitoring reports, and coordinated sanctions regimes represent attempts to safeguard member states from democratic backsliding and external interference. Yet, as *LSM.lv* reporting has highlighted in recent years, Latvia and other frontline states remain acutely exposed to disinformation campaigns and information warfare orchestrated by Russia. These challenges underscore that European democratization is not only an internal process of institutional consolidation but also an ongoing struggle to protect democratic space against external authoritarian influence. The EU's capacity to respond collectively to these pressures will be decisive in determining whether the continent's democracies strengthen or erode in the decades ahead.

The comparative analysis of European Commission policy documents and Latvian media coverage reveals a gradual convergence in how hybrid threats are conceptualized and addressed. At the European level, policy has developed from initial recognition in 2016 to a comprehensive resilience-oriented framework by 2024, embedding legal, technological, and cooperative mechanisms in close alignment with NATO and other partners. At the national level, Latvian public media, particularly *LSM.lv*, has evolved from superficial reporting toward more sophisticated, multi-dimensional analysis. Coverage increasingly integrates the perspectives of television and radio, producing a coherent national narrative that balances public awareness with sober recognition of risks. Especially since 2025, editorial attention has intensified, situating hybrid threats within broader concerns about democratic resilience, societal cohesion, and critical infrastructure.

Taken together, the policy trajectory of the European Commission and the evolving media discourse in Latvia are mutually reinforcing. Both underscore resilience not only as a technical or military imperative but as a central element in safeguarding democratic institutions and values. This dual movement – from institutional frameworks to public communication – demonstrates how hybrid threats are being mainstreamed into both strategic governance and societal understanding.

Bibliography

Books and Reports

Bērziņa, Ilze (2026, this issue). Language and Minority Issues, Border Security as Human Rights Challenges. *Letonica*, No. 63, pp. 58–81. https://doi.org/10.35539/LTNC.2026.0063.04

Bērziņš, Jānis (2014). *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy. Policy Paper No. 2.* National Defense Academy of Latvia, Centre for Security and Strategic Research.

Bodnieks, Valerijs (2023). Defensive Lawfare and Deterrence: Analysis of Latvia's Approach to Legal Bases in the Context of Hybrid Warfare (2014–2022). *Security & Defence Quarterly*, No. 42(2), pp. 55–67. http://doi.org/10.35467/sdq/163435

Diamond, Larry (2015). Facing Up to the Democratic Recession. *Journal of Democracy*, No. 26(1), pp. 141–155.

Eisen, Norman; Katz, Jonathan (eds.) (2025). *Democracy Playbook 2025: Seven Pillars to Defend Democracy in 2025 and Beyond*. Washington, DC: Brookings Institution.

Ellingsen, Tanja (2024). Hybrid Threats as a Threat to Democracy. Soft and Smart Tactics and Three Dimensions of Democracy. Borch, Odd Jarl; Heier, Tormod (eds.). *Preparing for Hybrid Threats to Security. Collaborative Preparedness and Response*. Routledge, pp. 36-51. https://doi.org/10.4324/9781032617916-4

Griķe, Anna E.; Raubiško, Ieva. "Weapons" of the "Hybrid War": Treatment of Irregular Migration in the Latvian Discourse of National Security. *Letonica*, No. 63, pp. 110–134. https://doi.org/10.35539/LTNC.2026.0063.07

Hoey, Joan (ed.) (2025). *Democracy Index 2024: What's Wrong with Representative Democracy?* London: Economist Intelligence Unit.

Hoffman, Frank G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, VA: Potomac Institute for Policy Studies.

Huntington, Samuel P. (1993). *The Third Wave: Democratization in the Late Twentieth Century.* Norman: University of Oklahoma Press.

Iarovyi, Dmytro (2025). Disinformation and Democracy. Mildner, Stormy-Annika; McIntyre, Alyssa; Zimmer, Niklas (eds.). *Hybrid Realities: Disinformation, Influencers, and the Defense of Democracy in Central and Eastern Europe*. Berlin, Aspen Institute Deutschland.

Käihkö, Ilmari (2021). The Evolution of Hybrid War: Implications for Strategy and the Military Profession. *The US Army War College Quarterly: Parameters*, No. 51(3), pp. 115–127. https://doi.org/10.55540/0031-1723.3084

Kruks, Sergejs; Skulte, Ilva (2022). The Perils of Defence in an Information War: Media, Minorities, and the Treat Next Door. Chakars, Janis; Ekmanis, Indra (eds.). *Information Wars in Baltic States. Russia's Long Shadow*. Palgrave Macmillan, pp. 187–203. https://doi.org/10.1007/978-3-030-99987-2_10

Sprūds, Andris; Rožukalne, Anda; Sedlenieks, Klāvs; Daugulis, Mārtiņš; Potjomkina, Diāna; Tölgyesi, Beatrix; Bruge, Ilvija (2016). *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*. Riga: NATO StratCom COE. Available: https://stratcomcoe.org/publications/internet-trolling-as-a-hybrid-warfare-tool-the-case-of-latvia/160 [Accessed 09.03.2025].

Struberga, Sigita; Ceple, Ruta (2021). Hibrīddraudi. Ozoliņa, Žaneta; Reinholde, Iveta; Struberga, Sigita (red.) *Latvijas iedzīvotāju subjektīvā drošības uztvere: ietekme uz drošības politikas veidošanu*. Rīga: LU Akadēmiskais apgāds, pp. 166–197. https://doi.org/10.22364/liesdu.07

Štareikė, Eglė (2024). Countering Hybrid Threats: Problematic Aspects in European Regions. *Public Security and Public Order*, No. 36. https://doi.org/10.13165/PSPO-24-36-17

Wither, James K. (2016). Making Sense of Hybrid Warfare. *Connections*, No. 15(2), pp. 73–87. http://dx.doi.org/10.11610/Connections.15.2.06

Institutional and Legal Sources

European Commission (2017). *Kopīgs ziņojums Eiropas Parlamentam un Padomei par to, kā tiek īstenots Kopīgais regulējums hibrīddraudu apkarošanai – Eiropas Savienības reakcija* [Joint Communication on Resilience, Deterrence and Defense: Building Strong Security]. COM(2017) 30 final. 19.07. Available: https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:-52017JC0030 [Accessed 21.07.2025].

European Commission (2018). *Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018*. COM(2018)14 final. 13.06. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0014&from=EN [Accessed 21 July 2025].

European Commission (2019). *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.* SWD(2019) 200 final. 17.06. Available: https://defence-industry-space.ec.europa.eu/system/files/2023-07/SWD%282019%29%20200%202%20final.pdf [Accessed 17.06.2019].

European Commission (2020). *Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.* 24.07. Available: https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2020)153&lang=en [Accessed 24.07.2020].

European Commission (2021). F*ifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.* Hybrid Threats Annual Progress Report (JSWD), 23.06. Available: https://defence-industry-space.ec.europa.eu/system/files/2023-07/JSWD%20Hybrid%20threats%20APR%2023062021.pdf [Accessed 23.06.2021].

European Commission (2022). *Sixth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats.* SWD(2022) 308 final. 16.09. Available: https://defence-industry-space.ec.europa.eu/system/files/2023-07/SWD_2022_308_6_EN_document_travail_service_conjoint_part1_v5.pdf [Accessed 16.09.2022].

European Commission (2023). *EU Defence Industry and Hybrid Threats Portal.* Available: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en [Accessed 14.09.2023].

Government of Latvia (2021). *Sabiedrisko elektronisko plašsaziņas līdzekļu un to pārvaldības likums* [Law on Public Electronic Media and Their Management]. Available: https://likumi.lv/ta/id/319096-sabiedrisko-elektronisko-plassazinas-lidzeklu-un-to-parvaldibas-likums [Accessed 25.03.2025].

Government of Latvia (2020). *Par Nacionālās drošības koncepcijas apstiprināšanu* [On the Approval of the National Security Concept]. Available: https://likumi.lv/ta/id/345911-par-nacionalas-drosibas-koncepcijas-apstiprinasanu [Accessed 04. 05.2025].

Government of Latvia (2022). *Nacionālās kiberdrošības likums* [National Cyber Security Law]. Available: https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums [Accessed 17.04.2025].

Government of Latvia (1922, with amendments). *Latvijas Republikas Satversme* [Constitution of the Republic of Latvia]. Available: https://likumi.lv/ta/id/57980-latvijas-republikas-satversme [Accessed 18.04.2025].

Hybrid COE (2019). Countering disinformation: News media and legal resilience. *Hybrid CoE Papers.* Available: https://www.hybridcoe.fi/publications/hybrid-coe-paper-1-countering-disinformation-news-media-and-legal-resilience/ [Accessed 12.04.2025].

Online Articles and Media

Ahonen, Anneli; Bilal, Arsalan; Gjørv, Gunhild Hoogensen; Jurāns, Juris; Kragh, Martin; Krūmiņš, Kārlis Kristofers; Lange-Ionatamishvili, Elīna, Liubinavičius, Balys, Mikulski, Kamil; Mölder, Holger; Ólafsson, Jon Gunnar; Ómarsdóttir, Silja Bara; Sazonov, Vladimir; Serritzlev, Jeanette. *Russia's Information Influence Operations in the Nordic-Baltic Region.* Riga: NATO Strategic Communications Centre of Excellence. Available: https://stratcomcoe.org/publications/russias-information-influence-operations-in-the-nordic-baltic-region/314 [Accessed 17.03.2025].

Arnicāns, Matīss (2025). Krievijas "ēnu karš" Eiropā [Russia's shadow war in Europe]. *LSM.lv*, 12.03. Available: https://www.lsm.lv/raksts/zinas/arzemes/12.03.2025-krievijas-enu-kars-eiropa.a591246 [Accessed 21.03.2025].

Gemius (2025). gemiusAudience aprīlī apmeklētāko vietņu TOP 20 [gemiusAudience: April Top 20 most visited websites in Latvia]. *Gemius*, 09.05. Available: https://gemius.com/lv/gemiusaudience-aprili-apmekletako-vietnu-top-20/ [Accessed 19.05.2025].

Grūbe, Gints (2024). Hibrīdkarš ir arī karš par vērtībām un prātiem. Saruna ar sociologi Aiju Zobenu [Hybrid war is also a war of values and minds: a conversation with sociologist Aija Zobena]. *LSM.lv*, 07.04. Available: https://www.lsm.lv/raksts/dzive--stils/sarunas/07.04.2024-hibridkars-ir-ari-kars-par-vertibam-un-pratiem-saruna-ar-sociologi-aiju-zobenu.a549005 [Accessed 01.03.2025].

Grūbe, Gints (2025). Komunikācijas pētnieks: Informatīvais karš ir daļa no Krievijas kara vešanas stratēģijas [Communications researcher: information warfare is part of Russia's war strategy]. *LSM.lv*, 20.02. Available: https://www.lsm.lv/raksts/dzive--stils/sarunas/20.02.2025-komunikacijas-petnieks-informativais-kars-ir-dala-no-krievijas-kara-vesanas-strategijas.a587836 [Accessed: 11.04.2025].

Industrial Cyber (2025). Social engineering becomes strategic threat as OT sector faces phishing, deepfakes, and AI deception risks. *Industrial Cyber*, 17.08. Available: https://industrialcyber.co/features/social-engineering-becomes-strategic-threat-as-ot-sector-faces-phishing-deepfakes-and-ai-deception-risks/ [Accessed 17.02.2026].

Kairis, Krišs (2023). Satversmes aizsardzības biroja vadītājs: Esam pārvērtējuši Krievijas spējas hibrīdapdraudējumā [Head of the Constitution Protection Bureau: we have overestimated Russia's capabilities in hybrid warfare]. *LSM.lv*, 28.02. Available: https://www.lsm.lv/raksts/zinas/latvija/satversmes-aizsardzibas-biroja-vaditajs-esam-parvertejusi-krievijas-spejas-hibridapdraudejuma.a498607 [Accessed 08.02.2025].

Krops, Jānis (2015). Hibrīdkarš – jauns izaicinājums, pret kuru stratēģijas vēl nav [Hybrid warfare – a new challenge for which there are no strategies yet]. *LSM.lv*, 23.02. Available: https://www.lsm.lv/raksts/zinas/latvija/hibridkars-jauns-izaicinajums-pret-kuru-strategijas-vel-nav.a118975 [Accessed: 07.01.2025].

Nagla, Ilze (2025). Krievija mēģina vairot paniku Eiropā ar "vienreizlietojamo" aģentu hibrīduzbrukumiem [Russia attempts to spread panic in Europe with disposable agent hybrid attacks]. *LSM.lv*, 07.06. Available: https://www.lsm.lv/raksts/zinas/arzemes/07.06.2025-krievija-megina-vairot-paniku-eiropa-ar-vienreizlietojamo-agentu-hibriduzbrukumiem.a601970 [Accessed 11.07.2025].

Plūme, Rihards (2024). Polija apsver iespēju slēgt robežšķērsošanas punktus ar Baltkrieviju [Poland considers closing border crossing points with Belarus]. *LSM.lv*, 23.06. Available: https://www.lsm.lv/raksts/zinas/arzemes/23.06.2024-polija-apsver-iespeju-slegt-robezskersosanas-punktus-ar-baltkrieviju.a559103 [Accessed 17.03.2025].

Reire, Gunda (2015). Kas ir hibrīdkarš? Uzbrukuma mērķis ir ikviens cilvēks [What is hybrid warfare? The target of the attack is any person]. *LV portāls*, 07.04. Available: https://lvportals.lv/viedokli/270138-kas-ir-hibridkars-gunda-reire-uzbrukuma-merkis-ir-ikviens-cilveks-2015 [Accessed 22.01.2025].

Šņore, Inga (2025). Krievijas iebrukums Ukrainā: Arī Rietumvalstīm pamatīgi jāsargā sava infrastruktūra [Russia's invasion of Ukraine: Western countries must also thoroughly protect their infrastructure]. *LSM.lv*, 23.02. Available: https://www.lsm.lv/raksts/zinas/latvija/23.02.2025-krievijas-iebrukums-ukraina-ari-rietumvalstim-pamatigi-jasarga-sava-infrastruktura.a588948 [Accessed 24.01.2025].

Štareike, Eglė (2024). Countering Hybrid Threats: Problematic Aspects in European Regions. *Public Security and Public Order*, No 36, p. 228–240. https://doi.org/10.13165/PSPO-24-36-17

Šukurovs, Rustams (2023). Somijas ārlietu ministre: Austrumu robežas slēgšana ir pietiekami spēcīgs signāls Maskavai [Finnish Foreign Minister: Closing the eastern border is a strong enough signal to Moscow]. *LSM.lv*, 29.11. Available: https://www.lsm.lv/raksts/zinas/arzemes/29.11.2023-somijas-arlietu-ministre-austrumu-robezas-slegsana-ir-pietiekami-specigs-signals-maskavai.a533556 [Accessed 11.02. 2025].

Wilde, Gavin (2025). Hybrid war thinking hobbles Europe's response to Russian sabotage. Latvian Institute of International Affairs. Available: https://liia.lv/en/opinions/hybrid-war-thinking-hobbles-europes-response-to-russian-sabotage-1367 [Accessed 01.05.2025].