RUSSIAN HYBRID THREATS WITHIN THE EU MEMBER STATES

*Major (ret) Sînziana IANCU, Ph.D**

Abstract: *Contemporary conflict extends beyond conventional warfare, integrating cyber, informational, cognitive, economic, and space dimensions into an evolving ecosystem of hybrid threats. The boundary between war and peace is becoming increasingly blurred, as both state and non-state actors employ influence operations, disinformation campaigns, and cyberattacks to disrupt decision-making processes and target critical infrastructure. Recent conflicts have demonstrated the strategic importance of digital infrastructures, communication networks, and satellite systems in maintaining national and international security.*

The rapid development of emerging technologies, such as artificial intelligence, the Internet of Things, and quantum computing, creates both new opportunities and significant strategic vulnerabilities. In this context, resilience has become a central objective, requiring close cooperation among government institutions, the private sector, academia, and civil society. Strengthening cybersecurity, protecting critical infrastructure, reducing technological dependencies, and enhancing international cooperation are considered essential measures for safeguarding democratic societies against hybrid threats.

Keywords: *hybrid warfare, cybersecurity, artificial intelligence, resilience, critical infrastructure.*

DOI 10.56082/annalsarscimilit.2026.2.129

I. Introduction

Contemporary warfare can no longer be understood solely through the lens of conventional military confrontation; rather, it requires the simultaneous integration of cyber, informational, cognitive, economic and space dimensions within an evolving ecosystem of hybrid threats.

The traditional boundary between war and peace is becoming increasingly blurred. State and non-state actors employ hybrid instruments to shape perceptions, exploit vulnerabilities within democratic societies and influence decision-making processes without crossing the threshold of a formally declared armed conflict. In this context, cyberspace has been defined as an "invisible battlefield," where digital infrastructure, communication networks and the information environment simultaneously serve as targets, weapons and vectors of strategic influence.

* corresponding member of the Academy of National Security Sciences, Minister Counselor in the Ministry of Foreign Affairs, Romania, email: iancu_sanziana@yahoo.com.

Nearly every contemporary conflict develops its own cyber dimension and cyber operations are employed not only for espionage and strategic pre-positioning, but also for sabotage, coercion, information influence and attacks against critical infrastructure. **The lessons drawn from the war in Ukraine constitute a key reference point for understanding how energy infrastructure, satellite communications, logistics systems and command-and-control networks can become priority targets for hostile actors.**

Particular emphasis has been placed on the relationship between emerging technologies and the transformation of hybrid conflict. Artificial intelligence, the Internet of Things (IoT), quantum computing and XR/Metaverse technologies are viewed not only as instruments of technological progress, but also as significant source of strategic vulnerability. Artificial intelligence substantially accelerates the development of influence operations, the generation of manipulative content, the automation of phishing attacks and the creation of adaptive malware. At the same time, quantum technologies introduce the risk of "***harvest now, decrypt later***" campaigns, in which encrypted data are collected today with the intention of decrypting them in the future.

With regard to the cognitive dimension of conflict, the information environment has become one of the primary arenas of strategic confrontation. Disinformation campaigns and Foreign Information Manipulation and Interference (FIMI) operations aim to manipulate public perceptions, polarize societies and undermine trust in democratic institutions. In this regard, it has been observed that artificial intelligence enables the personalization and amplification of manipulative messages at an unprecedented speed and scale, transforming information operations into a process that is significantly more difficult to detect and attribute.

At the same time, outer space is increasingly emerging as a new domain of hybrid competition. **Orbital infrastructure and satellite systems are often described as the "invisible backbone" of the global economy and security, as they support communications, navigation, financial systems, military operations and modern critical infrastructure**. In this context, cyberattacks and interference targeting space-based systems are considered capable of generating major strategic effects on contemporary societies.

Since the earliest doctrines of warfare, it has been recognized that attack is often easier than defense. Today, this principle is even more evident in the cyber and space domains, particularly due to the challenges associated with attribution, which facilitate operations conducted below the threshold of conventional armed conflict. **The concept of "plausible deniability" has become one of the defining characteristics of modern hybrid warfare, with hostile actors frequently employing proxy**

structures, hacktivist groups or private companies to conceal their direct involvement.

From an operational and doctrinal perspective, increasing emphasis has been placed on the role of international cooperation and Euro-Atlantic structures in strengthening cyber resilience. Equally important are multinational exercises, cooperation mechanisms and doctrinal initiatives designed to integrate cyber capabilities into modern operational planning. Cyberspace is now recognized as a distinct operational domain alongside the land, air, maritime and space domains, while information security is regarded as an essential component of collective security. Within this broader context, initiatives such as the **Foreign Information Manipulation and Interference Information Sharing and Analysis Center (FIMI-ISAC)** have gained increasing relevance. This international network is dedicated to protecting democratic societies against information manipulation and foreign interference. Such initiatives facilitate information sharing, the development of a common situational awareness picture, and the coordination of responses among governments, civil society, academia, and the private sector in the face of increasingly sophisticated influence operations.

Discussions on national resilience have also highlighted the importance of cooperation between governments and the private sector in protecting critical infrastructure. In most Western countries, digital and energy infrastructure is primarily operated by private companies, making interinstitutional cooperation and information sharing fundamental prerequisites for effective cyber defense. In this regard, Nordic resilience models provide relevant examples of how a security culture can be integrated across society through trust, cooperation and continuous preparedness.

At the same time, the use of diplomatic instruments in response to external cyber threats represents an important component of a broader defensive strategy. Public attribution of cyberattacks, sanctions and international cooperation are additional tools capable of limiting the freedom of action of hostile actors and contributing to the deterrence of hybrid operations.

Vulnerabilities generated by technological dependencies and global supply chains remain a critical topic of discussion at both the regional and global levels, particularly in the current context of a significant intensification of hybrid threats, driven by the ongoing war in the region as well as other conflicts with far-reaching, cascading effects. Growing concerns are frequently raised regarding the widespread use of digital equipment and components manufactured by external actors, as well as the risks associated with *firmware updates*, the collection of operational data and persistent access to critical networks. Consequently, supply chain

security and the reduction of strategic dependencies have been identified as essential priorities for democratic states.

Hybrid warfare systematically exploits the gap between the pace of technological development and the ability of democratic institutions to adapt. Hostile actors operate within a "grey zone" characterized by legal ambiguity, attribution challenges and institutional fragmentation, taking advantage of limited interoperability and delays in decision-making processes.

In this context, the concept of resilience is defined in a broader sense, extending beyond its strictly technical or military dimensions. Resilience encompasses the capacity of societies to absorb shocks, maintain institutional functionality and rapidly recover following hybrid attacks. This perspective reflects a "whole-of-society" approach based on sustained cooperation among state institutions, the private sector, academia, and civil society.

Technology is fundamentally reshaping the nature of contemporary conflict, while digital infrastructure, the information environment and the cognitive dimension have become central components of international security. In a strategic environment characterized by continuous competition, hybrid attacks and rapid technological acceleration, the protection of democratic resilience and collective security increasingly depends on swift institutional adaptation, the development of a robust security culture, and the strengthening of international cooperation.

II. Techniques, Tactics and Procedures of Hybrid Threats Employed by the Russian Federation

Today, we are witnessing an escalating confrontation between strategies aimed at preserving national identity and increasingly aggressive external factors that challenge the order and stability of the security environment. These developments are taking place against the backdrop of persistent and adaptive hybrid activities conducted by the Russian Federation against Western democratic societies. Russia is increasingly relying on ***single-use agents***, criminal networks, and non-state actors to carry out operations characterized by a high degree of plausible deniability abroad. According to several authors, more than 100 individuals involved in activities associated with Russian influence or destabilization operations in Western countries were identified over the past year, the majority of whom had criminal records. Furthermore, more than 600 Russian operatives have been expelled from pro-Western European states since 2018[1].

[1] Kacper Rekawek et al, *Russia's Crime–Terror Nexus Criminality as a Tool of Hybrid Warfare in Europe*, September 2025, available at https://www.globsec.org/sites/-default/files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%-20Tool_0.pdf, accessed on 30h of May, 2026, p. 06.

Russia promotes what has been described as a "ghost–gangster nexus," in which state security actors function as extensions of criminal elites ("ghosts"), who, in turn, subcontract tasks to "gangsters" or entities operating outside the formal control of the state.[2]

The Russian Federation has already recruited thousands of convicted criminals to support its war effort in Ukraine. Evidence suggests that similar methods are being applied to hybrid operations across Europe. Prisons, both within Russian Federation and abroad, provide a pool of recruits connected to organized crime and accustomed to violence. This reflects practices previously employed by groups such as Islamic State (ISIS), which viewed prison systems as reservoirs of potential operatives for political violence[3].

Moscow often begins by recruiting low-level offenders—such as thieves, drug traffickers, or heavily indebted individuals—whose initial roles are limited to low-level activities. However, repeated recruitment can encourage these actors to form more structured criminal groups. Over time, such groups may evolve into organized networks that serve Moscow's interests in a more systematic manner, reinforcing the broader "ghost–gangster nexus" and potentially enabling more sophisticated or lethal operations[4].

Looking retrospectively, German security authorities recorded 320 suspected sabotage attempts in 2025 alone. Clear attribution, however, remains challenging, as perpetrators are rarely identified[5].

Regarding the geographical distribution of incidents, more than one-quarter of all newly identified incidents (11 cases between July 2025 and February 2026, relative to the period from February 2022 to February 2026) occurred in Poland, which had already been the most frequently targeted country. With a total of 31 incidents, Poland now stands out even more clearly as the principal hotspot of Russian activity[6]. Significant increases were also observed in France, which recorded five new cases and now accounts for a total of 20 incidents between 2022 and 2026, making it the second most affected country. Lithuania and Germany each recorded 15 incidents, followed by the United Kingdom with 12 and Estonia with 11.

This distribution strongly suggests that support for Ukraine is the most significant factor shaping target selection. Some of Ukraine's most prominent supporters, including Poland, France, Germany, and the United

[2] *Ibidem*, p. 13.
[3] *Ibidem*, p.4.
[4] *Ibidem*, p. 31.
[5] Julian Lanchès, Kacper Rekawek, *More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited*, 23rd Feb. 2026, available at https://icct.nl/publication/more-same-russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited, accessed on 30th of May, 2026.
[6] *Ibidem*.

Kingdom, collectively account for more than half of all identified incidents. In addition, the Baltic states, which are derogatorily referred to by Russian Federation as part of a broader "near abroad," represent nearly one-fifth of all recorded cases.

Examples of such cases include [7]:

*** September 2025:** Eleven Serbian nationals were arrested in Serbia. They had previously traveled across Europe, often in different configurations and were linked to several incidents aimed at inciting ethnic and racial polarization. These activities included splashing green paint on Jewish sites in and around Paris, placing skeletons bearing inscriptions near the Brandenburg Gate, distributing stickers containing genocidal messages throughout the greater Paris area, and leaving severed pig heads in front of mosques in and around the city. French authorities linked these activities to foreign interference conducted on behalf of a hostile state actor, namely the Russian Federation[8].

*** October 2025:** Romanian and Polish authorities, acting jointly, disrupted plots involving the shipment of explosives through Poland and Romania to Ukraine. Specifically, the plan allegedly involved sending two incendiary parcels through Nova Poshta, a Ukrainian courier service operating between EU member states and Ukraine. The devices were reportedly intended to ignite and destroy the company's facility in central Bucharest. An Ukrainian citizen, Vitalij S., was arrested in Poland, while Romanian authorities detained two additional unnamed Ukrainian nationals[9].

*** October 2025:** Four Russian men between the ages of 26 and 38 from Dagestan were arrested in France on suspicion of plotting to assassinate Russian dissident Vladimir Osechkin, founder of the human rights organization *Gulagu.net*. The suspects had reportedly traveled earlier in 2025 to Osechkin's residence in France to conduct surveillance activities. One of the individuals also held French citizenship[10].

*** November 2025:** French authorities arrested three individuals as part of an investigation into a Franco-Russian association suspected of disseminating Kremlin propaganda and collecting intelligence on behalf of the Russian Federation. A 40-year-old Russian national was captured on municipal surveillance footage posting pro-Russian posters on the Arc de Triomphe and subsequently reporting to the head of the association (*SOS Donbass*)[11].

[7] *Ibidem*.
[8] *Ibidem.*
[9] *Ibidem.*
[10] *Ibidem.*
[11] *Ibidem.*

*** November 2025:** Three Ukrainian nationals sabotaged railway tracks in eastern Poland with the alleged intention of derailing trains, one of them reportedly remaining in close proximity to the destroyed section of track. The perpetrators had allegedly entered Poland specifically to carry out the attack before later returning to Belarus. According to available information, one of the individuals had maintained a longstanding relationship with Russian intelligence services and had previously been involved in a failed explosives attack against a factory in Ukraine[12].

This trend reflects Moscow's preference for the use of intermediaries and proxy structures, which enable the Russian state to conceal its direct involvement while simultaneously exploiting vulnerabilities within target populations. Of the 131 identified perpetrators, 62% committed multiple attacks, and 89% operated in groups of at least two individuals. Approximately 93% of the perpetrators were male, with an average age of 30, originating from post-Soviet states and primarily motivated by financial compensation[13]. Only 58% of the perpetrators were aware that their activities were directed by Russian services, while 27% had prior criminal records or involvement in illicit activities[14].

The general population thus often becomes an indirect instrument of hybrid operations without being aware of the underlying strategic objectives driving their actions. In other words, individuals do not necessarily realize that the outcomes of their actions are being leveraged by the Russian Federation, as third-party proxy elements are used to obscure attribution and intent. By exploiting social divisions, online influence ecosystems and local intermediaries, Russian actors aim to amplify polarization and erode trust in democratic institutions. Recent incidents involving drone incursions near airports and critical infrastructure further illustrate the increasingly visible and aggressive behavior attributed to the Russian Federation, as well as the fact that no state is immune to such challenges.

Regarding Russian strategic communication, it has become significantly more explicit and coercive. In contrast to earlier periods characterized by ambiguity and indirect signaling, Russian actors have recently begun publishing lists of potential future targets. This evolution suggests a gradual normalization of intimidation practices within the hybrid spectrum. In this context, fundamental questions arise regarding the definition of strategic "red lines" and the risk of accepting hostile hybrid activities as part of a so-called "new normal" – so, in other words – "*this is*

---

[12] *Ibidem.*

[13] Kacper Rekawek et al, *Russia's Crime–Terror Nexus Criminality as a Tool of Hybrid Warfare in Europe*, September 2025, available at https://www.globsec.org/sites/default/-files/2025-10/Russia%20Crime%20Terror%20Nexus_Criminality%20as%20a%20Tool-_0.pdf, p. 23, accessed on 30h of May 2026.

[14] *Ibidem,* p. 24.

the new normal, but don't get used to it", with the implication that continued efforts are required to develop strategies to mitigate these increasingly direct threats emanating from the Russian Federation. Although tactics, techniques, and procedures (TTPs) remain largely consistent, the scale and visibility of these operations have increased significantly.

II. 1. Russian Hybrid threats in the electoral domain

The Russian Federation's attempts to influence the political process in Moldova (including the 2024 presidential elections and the 2025 parliamentary elections) make it a potential testing ground for future Russian electoral interference operations in other European states. Such campaigns are likely planned in advance, typically at least six months prior to elections, requiring substantial financial resources, logistical preparation, influence networks, and coordinated information operations.

In this regard, a preliminary phase, occurring approximately six to twelve months in advance, may involve the identification of societal vulnerabilities and the construction of digital and proxy infrastructure, supported by significant funding and complex cyber operations. Three to six months prior to elections, influence operations may intensify, activating coordinated networks such as bots, troll farms and proxy media channels in order to polarize the electorate. The final phase, occurring in the last weeks before voting, may involve highly aggressive messaging campaigns, including delegitimizing narratives and so-called Black Swan-type disruptive events.

The presidential elections of October - November 2024 and the referendum on EU accession in Moldova revealed a significant escalation of FIMI operations conducted by the Russian Federation in the country, as these activities intensified in response to Moldova's pro-European trajectory[15]. In the months preceding the elections, Russian Federation employed a complex, multi-layered and adaptive FIMI infrastructure. These operations strategically combined existing capabilities with newly developed assets in order to manipulate public opinion, destabilize the electoral process, and undermine the EU enlargement process in the region[16].

[15] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 29 in chapter "Exposing the architecture of FIMI operations: a network analysis of influence operations", March 2025, available at https://www.eeas.-europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?, accessed on 26 of May 2026.
[16] *Ibidem*.

Therefore, maintaining continuous vigilance is essential, as is ensuring sustained funding for countermeasures at national and European levels, alongside the development of credible deterrence mechanisms.

Several examples of disinformation in this area include[17]:

*** Estonia:** During elections, a false claim spread on social media suggesting that voters should bring their own pens to polling stations because the provided ones were "erasable" and could alter votes[18];

*** France:** Prior to presidential elections, extremist groups disseminated anti-vaccination and anti-COVID-19 restriction narratives, promoting conspiracy theories designed to erode trust in public institutions[19];

*** Germany:** In Germany, far-right groups propagated narratives about electoral fraud, imported from U.S.-based election denial movements, in an effort to undermine democratic processes[20];

*** Slovakia:** Disinformation campaigns in Slovakia included AI-generated audio clips in which political leaders appeared to discuss electoral manipulation. These materials were widely circulated before being debunked[21];

*** Spain:** During the 2023 elections, false narratives circulated regarding foreign interference and electoral fraud, including claims that EU officials were campaigning for specific candidates[22].

Although the impact of disinformation varies across countries, the rapid dissemination of this phenomenon, its technological evolution, including speed, scale and transnational reach, its perceived harmlessness by segments of society and its relatively low funding requirements represent significant challenges not only to electoral processes but to democracies more broadly[23].

In 2024, the Russian Federation employed these manipulative tactics particularly in the context of European elections, where pro-Kremlin organizations attempted to target voters in EU member states with narratives undermining support for Ukraine. Additional notable elements include smear campaigns against prominent European political leaders through corruption allegations, as well as attempts to fuel protests, encourage voter

---

[17] Igor Soroceanu, *Dezinformarea în campaniile electorale*, 02nd of May, 2025, available at https://revista.universuljuridic.ro/dezinformarea-in-campaniile-electorale/, accessed on 30th of May, 2026.

[18] *Ibidem.*

[19] *Ibidem.*

[20] *Ibidem.*

[21] *Ibidem.*

[22] *Ibidem.*

[23] *Ibidem.*

abstention, and foster distrust in European institutions[24]. Nevertheless, the European Union and its Member States have actively monitored these interference attempts and countered false claims through exposure and awareness campaigns. The EUvsDisinfo platform has published extensive analyses exposing Foreign Information Manipulation and Interference (FIMI) operations targeting electoral processes[25]. Furthermore, Russian FIMI campaigns have also sought to exploit specific local vulnerabilities across political, social, and technological domains, deploying highly tailored and targeted content, particularly in contexts where the Russian Federation aims to advance its foreign policy and security interests[26]. In 2024, the Russian Federation also attempted to interfere in democratic processes in Moldova, targeting both the presidential elections and the referendum on EU accession.

Overall, the role of the Russian Federation as a FIMI actor reflects its perception of the information space as a domain of warfare. By using a combination of state and non-state actors, Russia has developed a multi-layered strategy aimed at shaping global narratives in support of Moscow's geopolitical objectives[27]. Focusing on long-term influence rather than isolated incidents, the Russian Federation continues to exploit vulnerabilities in the global information landscape, making its FIMI tactics a significant security concern for the EU[28]. The full-scale invasion of Ukraine launched by the Russian Federation on 24 February 2022 has highlighted the wide spectrum of information manipulation tactics employed by this state actor.

- ***Four key elements have defined Russian FIMI operations***[29]: * **First**, the simultaneous use of covert and overt channels, abandoning earlier discretion and making influence efforts more visible; * **Second**, Russian official channels and state-controlled media have

[24] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 12 in chapter "FIMI trends and findings in 2024", subchapter "Russia as a FIMI threat actor in 2024", March 2025, available at https://www.eeas.europa.eu/sites/-default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?, accessed on 26 May 2026.

[25] *Ibidem.*

[26] *Ibidem.*

[27] *Ibidem.*

[28] *Ibidem.*

[29] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 29 in chapter "Exposing the architecture of FIMI operations: a network analysis of influence operations", March 2025, available at https://www.eeas.europa.-eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?, accessed on 26 May 2026.

intensified their role, increasing their presence and promoting more aggressive narratives targeting Moldova; * **Third**, the Russian FIMI infrastructure previously deployed against Ukraine has been repurposed to target Moldova, adapting networks and narratives to a new interference front; * **Fourth**, a network of newly established local channels has functioned as a backbone for content distribution, ensuring resonance and credibility among local audiences while enabling broader amplification across the media space.

Russian influence operations are coordinated through a complex ecosystem that includes cryptocurrencies, local oligarchs, influencers, bloggers, hooligan groups, and even religious structures[30].

II.2. Russian Hybrid threats in the religious domain

In many cases, activities associated with the Russian Orthodox Church have been observed, with its influence allegedly being deliberately expanded in certain states as part of broader strategic influence campaigns.

Such examples have been identified across Northern Europe, including the following cases:

* **Sweden**[31]: In the city of Västerås (approximately 100 km west of Stockholm), authorities shut down a structure associated with the Russian Orthodox Church amid suspicions of espionage-related activities. Swedish authorities also exposed nuns from the "Saint Elisabeth" Monastery in Belarus, suspected of collaborating with Russian military intelligence services. According to the investigation, they operated for years across EU countries under the cover of religious activities, raised funds through the sale of religious goods and, allegedly, transferred them to support the Russian military effort. They also visited temporarily occupied territories in Ukraine. In winter 2025, they reportedly traveled to Sweden to continue their activities. At the time, Archpriest Andrei Lemeshonok publicly referred to his monastery as a "combat unit" in the war against Ukraine[32]. This case illustrates how the Russian Federation allegedly uses the Russian Orthodox Church as an instrument of hybrid influence. Under the cover of religious activity, such networks are accused of collecting intelligence, disseminating pro-Russian propaganda, legitimizing aggression against

[30] *Ibidem*.

[31] Roméo Langlois et. al., *Exclusive investigation: Is the Russian Orthodox Church in Sweden a platform for espionage?*, 07th of April, 2025, available at https://www.-france24.com/en/tv-shows/reporters/20250704-exclusive-investigation-is-the-russian-orthodox-church-in-sweden-a-platform-for-espionage, accessed on 26 May 2026.

[32] Center for countering disinformation, *In Sweden nuns were exposed for spying for Russian intelligence*, 19th of January, 2026, available at https://cpd.gov.ua/en/international-threats-en/europe/in-sweden-nuns-were-exposed-for-spying-for-russian-intelligence/, accessed on 26th of May, 2026.

Ukraine and building influence networks within Western societies[33]. Additional concerns have been raised regarding the **sensitive location** of the church, situated near an international airport, a major water treatment facility, and advanced energy companies in Västerås, a city of approximately 130,000 inhabitants located 100 km west of Stockholm[34].

*** Norway[35]:** Several religious entities in Norway are located near strategically significant sites. Although the Norwegian Police Security Service (PST) has not publicly detailed individual cases, independent analyses indicate a notable geographic pattern of Russian Orthodox churches and chapels aligned with the Moscow Patriarchate, often situated near military, industrial, or governmental infrastructure[36]: *****Oslo - The parish "Saint Princess Olga," operating since 2003, is located in the central district within walking distance of the Norwegian Parliament (Stortinget), Statistics Norway (SSB), several ministries and at least seven foreign embassies; * Bryne - The "Saint Martyr Irene" church, built in 2014, is located within an area hosting high-tech manufacturing firms specializing in metal processing, robotics and semiconductor components, including *Nordic Steel AS* (650 metres distance from the church) and *IXYS Norway* (approx.. 586 metres distance from the church); * Kirkenes - The "Saint Tryphon of Pechenga" parish, established in 2015 near the Russian border, is located close (5 km) to the Sør-Varanger garrison and municipal and consular facilities; * Vardø - An Orthodox chapel under construction, since 2017, is located near the GLOBUS radar installation, a strategic intelligence asset; * Trondheim - The parish of "Saint Anna of Novgorod", established in 2008, is located approximately one kilometer from several defense-related facilities, including a submarine bunker, an air force academy, and other military installations. It is also situated near the city's naval port and in proximity to the consulates of several NATO member states, including Finland, Poland, Denmark and the Netherlands. Such a location could potentially provide a particularly observant "parishioner" with ample opportunities to monitor military activity and movements.

Within the Norwegian context, this pattern closely mirrors the experience observed in Sweden, where places of worship affiliated with the Moscow Patriarchate have been established in areas of strategic

[33] *Ibidem*.

[34] Charlie Duxbury, *New Russian church raises suspicions in Swedish town*, 11th November, 2024, available at https://www.politico.eu/article/new-russian-orthodox-church-suspicion-sweden-town-vasteras/, accessed on 26th of May, 2026.

[35] Nordic Defence Review, *Russian Orthodox Churches in Europe: Espionage Outposts Under the Guise of Faith*, s.a., available at https://nordicdefencereview.com/russian-orthodox-churches-in-europe-espionage-outposts-under-the-guise-of-faith/, accessed on 30th of May, 2026.

[36] *Ibidem*, accessed on 26th of May, 2026.

significance. It is also noteworthy that several Russian religious figures active in Norway, including Father Khukhtamyaki and others, maintain direct ties with Patriarch Kirill and have broadly aligned themselves with Moscow's political positions[37].

*** Finland[38]: *** Turku **-** In August 2022, authorities closed a Russian Orthodox parish, citing national security concerns in the context of the Russian Federation's invasion of Ukraine. The parish was located near the Pansio naval base, the Port of Turku and regional administrative institutions, as well as in proximity to the Russian consulate; ***** Helsinki - The "Saint Nicholas the Wonderworker" parish, active since 1938, is located near multiple military and governmental facilities, while another smaller chapel in eastern Helsinki is situated near the Vuosaari commercial port and a major power plant.

*** Netherlands[39]: *** Hague - The Russian Orthodox monastery "Saint John the Baptist," operating since 1972, came under increased scrutiny after the invasion of Ukraine, as it was located near numerous government and defense-related facilities. Approximately 29 government offices were identified in its vicinity, including the European Defence Technology Associations headquarters and a Dutch Army facility. The monastery was closed in December 2022 amid growing security concerns; ***** Rotterdam - The "Saint Alexander Nevsky" church, established in 2004 with the involvement of Russian construction companies and consecrated by Patriarch Kirill, is located near critical infrastructure, including government institutions, maritime logistics facilities and energy-related industrial sites.

*** Czech Republic[40]:** Prague - The historic Cathedral of Saints Cyril and Methodius received significant restoration funding from Gazprom Neft, a Russian state-owned energy company, raising concerns among legislators regarding potential influence operations; ***** Moravian region - The Orthodox Cathedral of "St. Gorazd in Olomouc" is located relatively close to the site of the 2014 Vrbětice ammunition depot explosions, an incident attributed to Russian intelligence operatives; ***** Vrbětice - A small Orthodox chapel exists within the broader regional environment of the same incident, prompting discussions among investigators regarding possible links between religious infrastructure and intelligence activities.

*** Bulgaria[41]:** In 2022, Bulgarian authorities expelled three priests of the Russian Orthodox Church (two Belarusian nationals and one Russian national) on national security grounds.

---

[37] *Ibidem*.
[38] *Ibidem*, accessed on 30th of May, 2026.
[39] *Ibidem.*
[40] *Ibidem.*
[41] *Ibidem.*

*** Estonia[42]:** The Estonian government recently refused to renew the residence permit of the leader of the local Orthodox Church affiliated with Moscow, citing security risks linked to explicit justification of the Russian Federation's war and potential ties to Moscow-based religious services.

At the pan-European level, institutions have begun to respond more decisively. In October 2024, the Council of Europe went as far as to characterize the Russian Orthodox Church as an instrument of Kremlin influence, within a resolution that also sanctioned Russian propagandists.[43]

*** Latvia:** The Latvian authorities have adopted strict legislative and economic measures to limit Russian influence, including restrictions on land ownership by Russian nationals and expanded sanctions against proxy networks and intermediaries.

The current confrontation with the Russian Federation should not be interpreted as a temporary anomaly, but rather as an expression of how the Kremlin perceives the international order and the balance of power. From this perspective, expectations of a rapid normalization of relations with the Russian Federation are considered unrealistic in the short to medium term.

III. Takeaways

The analysis of the evolution of contemporary conflict demonstrates that hybrid warfare has become one of the primary manifestations of strategic competition among states, extending far beyond the traditional framework of conventional military confrontation. Cyber, informational, cognitive and space dimensions are now integrated into a complex ecosystem of threats that exploit the technological, institutional and societal vulnerabilities of democratic states. In this context, digital infrastructure, satellite systems and the information environment have acquired a strategic significance comparable to that of the traditional operational domains, while the ability to adapt to emerging forms of conflict has become an essential prerequisite for maintaining both national and collective security.

The cases examined illustrate that the Russian Federation employs a broad range of hybrid techniques, tactics and procedures (TTPs), relying on proxy actors, criminal networks, influence operations and information manipulation campaigns. These activities are designed to erode trust in democratic institutions, amplify societal polarization and disrupt decision-making processes, including during electoral periods. Furthermore, the use of seemingly non-political structures, including religious organizations and entities associated with them, highlights the multidimensional and adaptive nature of Moscow's influence strategies. The difficulty of attributing responsibility and the systematic use of the concept of *plausible deniability*

[42] *Ibidem.*
[43] *Ibidem.*

enable such operations to be conducted below the threshold of conventional armed conflict, significantly complicating the response of targeted states.

In the face of these challenges, strengthening societal resilience must go beyond strictly military or technical approaches and embrace an integrated *whole-of-society* perspective. Cooperation among state institutions, the private sector, academia and civil society, together with the development of a strong security culture, the protection of critical infrastructure and the enhancement of international cooperation, constitute fundamental elements for countering hybrid threats. At the same time, recent experiences demonstrate that strategic vigilance, continuous adaptation and the development of effective deterrence mechanisms will remain essential in a security environment characterized by persistent competition, rapid technological acceleration and the increasingly aggressive use of hybrid instruments of influence and destabilization.

BIBLIOGRAFY

3rd EEAS REPORT ON FOREIGN INFORMATION MANIPULATION AND INTERFERENCE THREATS, *Cementing the foundations of Russia FIMI infrastructure in Moldova: the opportunistic use of events*, p. 29 in chapter "Exposing the architecture of FIMI operations: a network analysis of influence operations", March 2025, available at https://www.eeas.europa.eu/sites/default/-files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf?;

CENTER FOR COUNTERING DISINFORMATION, *In Sweden nuns were exposed for spying for Russian intelligence*, 19th of January, 2026, available at https://cpd.gov.ua/en/international-threats-en/-europe/in-sweden-nuns-were-exposed-for-spying-for-russian-intelligence/;

DUXBURY C., *New Russian church raises suspicions in Swedish town*, 11th November, 2024, available at https://www.politico.eu/-article/new-russian-orthodox-church-suspicion-sweden-town-vasteras/;

SOROCEANU I., *Dezinformarea în campaniile electorale*, 02nd of May, 2025, available at https://revista.universuljuridic.ro/-dezinformarea-in-campaniile-electorale/;

LANCHÈS J., REKAWEK K., *More of the Same. Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare Revisited*, 23rd Feb. 2026, available at https://icct.nl/publication/more-same-

russias-crime-terror-nexus-criminality-tool-hybrid-warfare-revisited;

REKAWEK K., LANCHÈS J., ZOTOVA., BOWSER D., *Russia's Crime–Terror Nexus Criminality as a Tool of Hybrid Warfare in Europe*, September 2025, available at https://www.globsec.org/-sites/default/files/2025-10/Russia%20Crime%20Terror%20-Nexus_Criminality%20as%20a%20Tool_0.pdf;

NORDIC DEFENCE REVIEW, *Russian Orthodox Churches in Europe: Espionage Outposts Under the Guise of Faith*, s.a., available at https://nordicdefencereview.com/russian-orthodox-churches-in-europe-espionage-outposts-under-the-guise-of-faith/;

LANGLOIS R., NORDSTROM L., SEIBT S., CHABOUR K., France 24, Exclusive investigation: Is the Russian Orthodox Church in Sweden a platform for espionage? available at https://www.-france24.com/en/tv-shows/reporters/20250704-exclusive-investigation-is-the-russian-orthodox-church-in-sweden-a-platform-for-espionage.