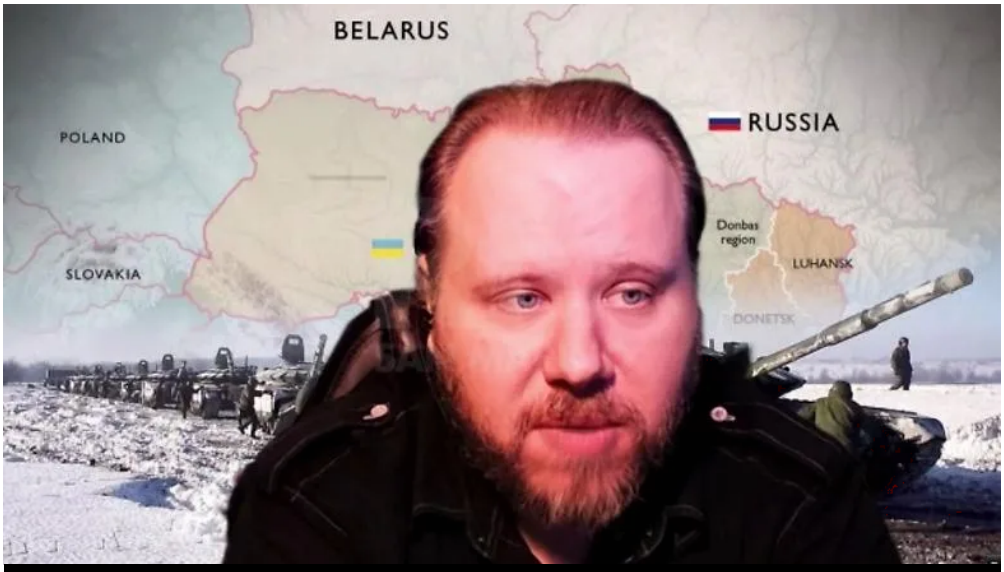
Moscow's Hybrid War Uses Italian Pro-Russians

Published on 29/12/2025

The war in Ukraine, reaching the **1,394th day** by the end of December 2025, continues to claim victims and unfold not only in the trenches but also in the “gray zone” of hybrid warfare: cyberattacks, disinformation, sabotage, and low-attribution actions used to test European democracies. This is what emerges from the **interview of Il Dubbio with Mirko Campochiari** , CEO and founder of Parabellum, an Italian think tank that conducts OSINT analysis and maps the Ukrainian front.



Moscow's Hybrid War Uses Italian Pro-Russians

The Front: Cities, Drones, and Attrition Choices

On the ground, Campochiari highlights the centrality of **urban agglomerations** in Donbass: defending them means protecting the “backbone” of systems and defensive lines in a narrow sector of tens of kilometers. In parallel, he notes how a majority of actions now occur with **drones**, making positions in open fields more vulnerable compared to urban contexts.

In this framework, he cites examples of “non-linear” tactics and decisions: in **Kupiansk**, he speaks of small group infiltrations to create chaos among Russian forces; in **Siversk**, he highlights a case where Ukrainians prioritized conserving forces over staunch defense, signaling a possible strategic adaptation to preserve manpower.

Russian Losses: Why Numbers Matter (and How They Are Estimated)

One of the most delicate points remains the human toll. Campochiari disputes the Ukrainian estimate of **1.2 million dead and wounded** as “unreliable” and points to the work of Mediazona (with BBC Russian and volunteers) as more credible, maintaining a verified nominal list and using statistical methods to estimate the overall impact.

In this area, European press has also highlighted the existence of estimates based on confirmed names, though noting that the real total may be higher due to the limitations of public sources and the difficulty of fully accounting for losses and injuries.

Campochiari then links the “sustainability” of Russian recruitment to economic dynamics and incentives: he describes an increase in economic offers over time, signs of stabilization, and a recent decline, along with the greater appeal of **drone units** because they allow for “remote” combat. Added to this, in his account, is a “structural” element: pressures on regional administrators to meet recruitment quotas, with practices ranging from incentives to social coercion.

The Polymarket–ISW Case: When a Map Becomes a Weapon

The interview sheds light on another front: that of **trust** in public sources and information infrastructures. Campochiari reconstructs a case linked to **Polymarket**, a “prediction market” platform with bets on military outcomes, whose resolution relies (in many markets) on maps like those of the **Institute for the Study of War (ISW)**.

According to the cited reconstruction, on the night of **November 15, 2025**, an update temporarily showed **Myrnohrad** as under Russian control, coinciding with the closure of a bet; the edit then “disappeared” and a correction was issued. ISW spoke of an **unauthorized modification**. Beyond the single episode, the lesson is clear: even a “technical” artifact like a map can become a target, as it influences reputations, narratives, and even money flows.

What Is “Hybrid Warfare” (and Why Europe Feels It)

In the operational definition recalled by institutional documents and analyses, the hybrid threat combines different tools — **cyber**, **disinformation, economic and social pressure, sabotage** — exploiting ambiguity, deniability, and long timelines.

A non-paper circulated in the Defense sector, citing the Annual Report of the **DIS**, lists typical examples of this “gray zone”: **fake news**, targeted infrastructures, **cut cables**, sabotage, and interference in democratic processes. At the EU level, reports on hostile information insist on one point: state actors and influence networks have built digital ecosystems to manipulate the European information space, fueling polarization and distrust.

On the cyber side, the picture is consistent: sector analyses describe an environment where phishing, vulnerability exploitation, and DDoS remain significant vectors often associated with

“hybrid” and political pressure campaigns.

Moscow's Hybrid War Uses Italian Pro-Russians

Drones, Airports, Sabotage, Cyberattacks: “Testing” the Political Response

Campochiari summarizes it this way: cyberattacks, fake news, drones, and online recruitment of “expendable agents” would be **indirect ways** to “test” the political response of European countries and, if the reaction is timid, **raise the stakes**.

In the same months, the European debate has focused precisely on this dynamic: episodes related to drones, alarms, and temporary shutdowns of sensitive infrastructures are interpreted as high-impact, low-attribution signals capable of producing immediate costs (economic and political) without openly crossing the threshold of conflict.

On the digital front, recent journalistic reconstructions have linked pro-Russian groups to DDoS actions and disruption campaigns against public services and businesses, aiming to create disruptions, amplify social anxiety, and demonstrate vulnerabilities. In this type of operation, even a temporary interruption can be worth more than the technical damage: it is a political message.

“The Italian Megaphone” and the Pro-Russian Galaxy: Theses and Risks

It is in the reading of the Italian context that Campochiari uses the harshest words: he claims that Italy is, for historical and cultural reasons, a **“megaphone”** of Kremlin propaganda, with figures (including academic and professional) ready to relay narratives favorable to Moscow or rewrite recent history.

He does not speak only of ideological convictions: he describes a “pattern” of coordinated content relaunch (“one brings up a news item and others follow”), and adds that part of the pro-Russian ecosystem would actually be bonded by **anti-EU, anti-USA, or conspiracy/novax identities**, rather than a real interest in Russia. In this light, propaganda is not a monolith, but an opportunistic network that exploits every available fracture.

Here the stakes are democratic resilience: **hybrid warfare works when it manages to turn pre-existing social fractures into permanent polarization, eroding trust in institutions and media.**

The Fault Line: National Security and Freedom of Information

If **the military front** is made of drones and artillery, the **hybrid one passes through maps, platforms, digital infrastructures, and especially through the vulnerability of open societies where propaganda can disguise itself as “competent opinion”**. The point is not only to recognize disinformation but to understand when an internal ecosystem becomes, willingly or not, a multiplier of external pressure.

Sources Used:

- **Il Dubbio**, interview by Emilio Minervini with Mirko Campochiari (Parabellum), “Moscow's Hybrid War Uses Italian Pro-Russians”, December 27, 2025
- Materials and public content from the think tank **Parabellum** (OSINT analysis and map)
- **Mediazona** (with contributions and collaboration from **BBC Russian** and volunteers), estimates based on verified names and statistical methods
- **Institute for the Study of War (ISW)**, communications and updates related to the Myrnohrad case and map update methods

- **ENISA**, “Threat Landscape” (recent editions), overview of major cyber threat vectors and trends
- **EEAS / EUvsDisinfo**, reports on interference and manipulation campaigns in the European information space
- **Annual DIS Report** and Italian documents on hybrid threats and disinformation
- International journalistic reconstructions (e.g., **AP**, **Reuters**) on cyberattacks, sabotage, and “hybrid” dynamics in Europe (2024–2025)

News link: https://www.ildubbio.news/news/interviste/48354/voto-si-al-referendum-perche-e-una-riforma-che-completa-la-costituzione.html