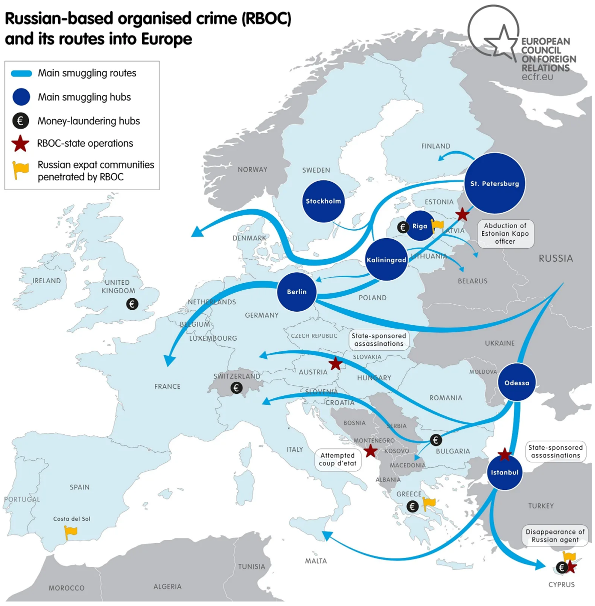

Russian Secret Services and Organized Crime

Published on 16/12/2025

In the last twenty years, the line between Russian state apparatuses (particularly the FSB and, externally, the GRU) and organized crime groups has progressively blurred: mafias and criminal networks are not only independent economic entities but become useful tools for clandestine operations, sanction evasion, cyberattacks, and actions of intimidation or physical elimination of targets. This "operational coexistence" allows the state to achieve direct action with a high degree of deniability and reduced political costs.

Methods of Use (Tactics and Mechanisms)

1. **Assassinations and “contract killings”**: secret services and actors linked to hybrid warfare use killers and crime professionals to target dissidents, political opponents, or individuals deemed dangerous. The use of underworld executors reduces the risk of immediately tracing the action back to the state.

2. **Proxies for sabotage and clandestine actions ("shadow alliance" model)**: criminal networks in Europe and the ex-Soviet area have been used as proxies for acts of sabotage, arson, political cyberattacks, and disinformation campaigns. Europol and other reports indicate a growing integration between crime and operational capabilities aimed at destabilizing infrastructures and institutions.
3. **Cybercrime and "cyber proxies"**: criminal groups offer ransomware-as-a-service, botnets, and digital money laundering services; these tools are employed for operations serving strategic interests (economic espionage, information gathering, economic damage). The use of cybercriminals gives the state incremental offensive capabilities without the direct use of official military resources.
4. **Sanction evasion and international-scale money laundering**: organized crime networks and shell companies are used to move capital, purchase assets (real estate, media), and hide flows intended to evade international sanctions, support unofficial state projects, or finance influence networks. International counter-operations have led to seizures and arrests in multiple countries.
5. **Recruitment and training of fighters or action teams**: crime figures are sometimes recruited for security tasks, bodyguarding, or employed as irregular militias in conflict areas (e.g., Ukraine), creating links between mercenarism, crime, and military politics.

Russian Secret Services and Organized Crime

Russian Secret Services and Organized Crime

Why This Convergence Benefits the Kremlin

- **Deniability and operational anonymity**: using non-state actors allows for plausibly deniable actions.
- **Reduced political costs**: actions attributed to "criminals" attract fewer immediate diplomatic sanctions compared to operations undeniably attributable to the state.
- **Capabilities and know-how**: criminal networks offer access to clandestine infrastructures, alternative financial channels, IT specialists, and flexible action forces.

Impact on European States and Civil Societies

The state-crime cooperation complicates investigative and judicial activities: actions are masked through complex transnational structures, cryptocurrencies, and front men, making it difficult to trace funding and prove state origin. Additionally, the presence of “criminal proxies” increases internal security risks — from cyberattacks to systemic corruption — and undermines trust in institutions. Examples and reported cases

- Money laundering operations and networks that enabled the purchase of assets in Europe have been dismantled in major international investigations (cross-border operations coordinated by the United Kingdom, U.S. Treasury, and European authorities).
- Reports from think tanks and institutes (Global Initiative, New Lines Institute, GLOBSEC, ICCT) document how the war in Ukraine has accelerated the fusion between state objectives and criminal capabilities, with uses in espionage, sabotage, and opaque economic operations.

Analysts recommend integrated approaches: greater international cooperation between intelligence, law enforcement, and financial authorities; cryptocurrency tracking tools; stricter anti-money laundering laws; rapid information sharing and critical infrastructure resilience plans. Additionally, public policies are needed to reduce the legal and financial space in which these networks operate.

Conclusion

The use of organized crime by parts of the Russian state is a documented, multifaceted, and growing phenomenon in recent years: it combines traditional tools (contract killings, illicit trafficking) with modern capabilities (cybercrime, transnational money laundering, use of AI/digital tools for proxy operations). Countering it requires multi-level efforts, legal, technical, and diplomatic, along with continuous monitoring of evolving methods.

Main Sources (Selection — English & Italian)

- Mark Galeotti, *Gangsters at war: Russia's use of organized crime as an instrument of statecraft*. Global Initiative / GI-TOC (Nov 2024).
- New Lines Institute, *How Russia Uses Organized Crime for Espionage* (Jul 22, 2025).
- GLOBSEC, *Russian Organised Crime and Links to Hybrid War in Europe* (report, 2025).

- Europol, *EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025* / related reports on the use of criminal networks for sabotage.
- ICCT, *Russia’s Crime–Terror Nexus: Criminality as a Tool of Hybrid Warfare* (2025).
- AP / investigations on money laundering networks and international dismantling (e.g., UK/NCA operations).
- Financial Times / articles on AI, crime, and proxy attacks (Europol findings).
- ECFR, *How the Kremlin uses Russia*'*s criminal networks in Europe* (historical analysis and context).

News link: https://globalinitiative.net/analysis/gangsters-at-war-russias-use-of-organized-crime-as-an-instrument-of-statecraft/