



Servizi Segreti Russi e Criminalità Organizzata

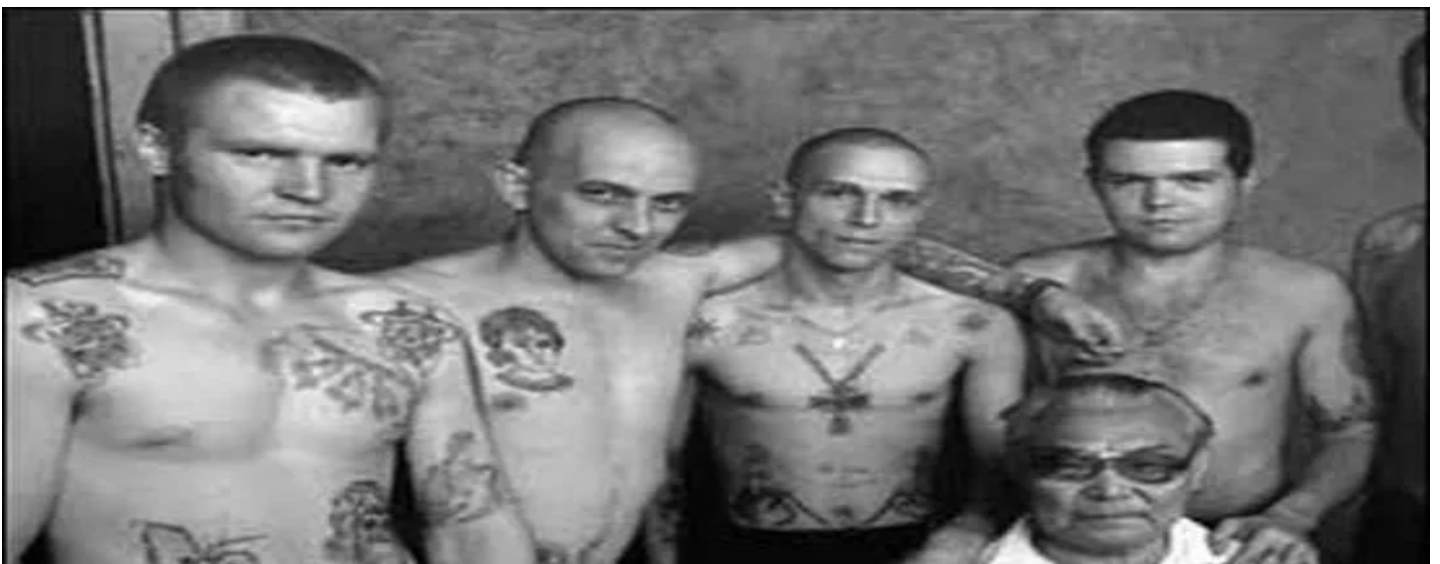
Pubblicato il 16/12/2025

Negli ultimi vent'anni il confine tra apparati dello Stato russo (in particolare FSB e, in ambito esterno, GRU) e gruppi della criminalità organizzata si è progressivamente sfumato: mafie e reti criminali non sono solo soggetti economici indipendenti, ma diventano strumenti utili per operazioni clandestine, evasione sanzioni, attacchi informatici e azioni di intimidazione o eliminazione fisica di bersagli. Questa «convivenza operativa» permette allo Stato di ottenere azione diretta con un elevato grado di negabilità e con ridotti costi politici.

Modalità d'impiego (tattiche e meccanismi)

1. **Assassini e “contract killings”:** servizi segreti e attori legati alla guerra ibrida si servono di killer e professionisti del crimine per colpire dissidenti, avversari politici o persone ritenute pericolose. L'uso di esecutori legati alla malavita riduce il rischio di ricondurre immediatamente l'azione allo Stato.

2. **Proxies per sabotaggi e azioni clandestine (modello “shadow alliance”):** reti criminali in Europa e nell’area ex-sovietica sono state utilizzate come proxy per atti di sabotaggio, incendio doloso, attacchi informatici politici e campagne di disinformazione. Europol e altri report indicano una crescente integrazione tra criminalità e capacità operative finalizzate a destabilizzare infrastrutture e istituzioni.
3. **Crimine informatico e “cyber proxies”:** gruppi criminali offrono ransomware-as-a-service, botnet e servizi di riciclaggio di denaro digitale; questi strumenti sono impiegati per operazioni che servono interessi strategici (spionaggio economico, raccolta informazioni, danneggiamento economico). L’uso di criminali informatici dà allo Stato capacità offensive incrementali senza l’impiego diretto di risorse militari ufficiali.
4. **Evasione di sanzioni e riciclaggio su scala internazionale:** network di criminalità organizzata e società di comodo sono impiegati per spostare capitali, acquistare beni (immobili, media) e nascondere flussi destinati a eludere sanzioni internazionali, sostenere progetti statali non ufficiali o finanziare reti di influenza. Operazioni internazionali di contrasto hanno portato a sequestri e arresti in più Paesi.
5. **Reclutamento e addestramento di combattenti o squadre di azione:** esponenti della criminalità sono talvolta reclutati per compiti di sicurezza, bodyguarding, o impiegati come milizie irregolari nelle aree di conflitto (es. Ucraina), creando legami tra mercenarismo, criminalità e politica militare.



Servizi Segreti Russi e Criminalità Organizzata

Perché questa convergenza conviene al Cremlino

- **Negabilità e anonimato operativo:** usare attori non statali permette di compiere azioni plausibilmente negabili.
- **Costi politici ridotti:** azioni attribuite a “criminali” attirano meno sanzioni diplomatiche immediate rispetto a operazioni attribuibili senza dubbio allo Stato.
- **Capacità e know-how:** reti criminali offrono accesso a infrastrutture clandestine, canali finanziari alternativi, specialisti informatici e a forza d'azione flessibile.

Impatto sugli Stati europei e sulle società civili

La cooperazione Stato-criminalità complica l'attività investigativa e giudiziaria: le azioni vengono mascherate attraverso strutture transnazionali complesse, criptovalute e prestanome, rendendo difficile la tracciabilità dei finanziamenti e la prova dell'origine statale. Inoltre, la presenza di “proxy criminali” aumenta i rischi per la sicurezza interna — dagli attacchi informatici alla corruzione sistemica — e mina la fiducia nelle istituzioni. Esempi e casi riportati

- Operazioni di riciclaggio e reti che hanno permesso l'acquisto di beni in Europa sono state smantellate in importanti inchieste internazionali (operazioni transfrontaliere coordinate dal Regno Unito, U.S. Treasury e autorità europee).
- Rapporti di think-tank e istituti (Global Initiative, New Lines Institute, GLOBSEC, ICCT) documentano come la guerra in Ucraina abbia accelerato la fusione tra obiettivi statali e capacità criminali, con impieghi in spionaggio, sabotaggio e operazioni economiche opache.

Gli analisti raccomandano approcci integrati: maggiore cooperazione internazionale tra intelligence, forze dell'ordine e autorità finanziarie; strumenti di tracciamento delle criptovalute; leggi anti-riciclaggio più stringenti; condivisione rapida di informazioni e piani di resilienza delle infrastrutture critiche. Inoltre, servono politiche pubbliche che riducano lo spazio legale e finanziario in cui queste reti operano.

Conclusione

L'uso della criminalità organizzata da parte di parti dello Stato russo è un fenomeno documentato, multifaccettato e in crescita negli ultimi anni: combina strumenti tradizionali (omicidi su commissione, traffici illeciti) con capacità moderne (cybercrime, riciclaggio transnazionale, uso di AI/strumenti digitali per operazioni proxy). Contrastarlo richiede sforzi

multilivello, legali, tecnici e diplomatici, oltre a un continuo monitoraggio dei metodi in evoluzione.

Fonti principali (selezione — inglese & italiano)

- 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* / reportage correlati su uso di reti criminali per sabotaggi.
- ICCT, *Russia's Crime-Terror Nexus: Criminality as a Tool of Hybrid Warfare* (2025).
- AP / inchieste su reti di riciclaggio e smantellamenti internazionali (es. operazioni UK/NCA).
- Financial Times / articoli su AI, criminalità e attacchi proxy (rilevazioni Europol).
- ECFR, *How the Kremlin uses Russia's criminal networks in Europe* (analisi storica e contesto).

Link notizia: <https://globalinitiative.net/analysis/gangsters-at-war-russias-use-of-organized-crime-as-an-instrument-of-statecraft/>