NICOLA CRISTADORO

LUCI E OMBRE DELL'INTELLIGENCE MILITARE RUSSA NEL CONFLITTO RUSSO-UCRAINO (PERIODO 2022-2026)

RESEARCH PAPER

ISTITUTO GINO GERMANI

SCIENZE SOCIALI E STUDI STRATEGICI

LUCI E OMBRE DELL'INTELLIGENCE MILITARE RUSSA NEL CONFLITTO RUSSO–UCRAINO (PERIODO 2022-2026)

Nicola Cristadoro

RESEARCH PAPER

Novembre 2026

ISTITUTO GINO GERMANI
DI SCIENZE SOCIALI E STUDI STRATEGICI

www.istitutogermani.org

L'Istituto Gino Germani di Scienze Sociali e Studi Strategici, un think tank senza fini di lucro costituito nel 1981, ha la missione di difendere e rinnovare la democrazia liberale e la società aperta.
L'Istituto promuove e pubblica studi e analisi sulle sfide alla sicurezza e alla stabilità dell'Occidente, della comunità euro-atlantica e dell'Italia. Inoltre, l'Istituto ha lo scopo di elevare la consapevolezza dei decisori politici e dell'opinione pubblica circa le minacce interne ed esterne alla democrazia liberale e ai suoi valori. In particolare, il think tank approfondisce temi quali: regimi e ideologie autoritari e totalitari, terrorismo e violenza politica, estremismi di destra e di sinistra, criminalità organizzata transnazionale, corruzione politica, movimenti nazional-populisti illiberali, disinformazione e manipolazione delle percezioni, minacce cibernetiche, ingerenza e influenza da parte di potenze straniere autocratiche con finalità di destabilizzazione delle democrazie, il ruolo dell'intelligence e della counter-intelligence nella tutela degli Stati democratici.

Il Gen. **Nicola Cristadoro** è un Ufficiale dei Bersaglieri. Ha frequentato il 166° Corso dell'Accademia Militare di Modena ed è laureato in Scienze Politiche presso l'Università degli Studi di Milano, Scienze Strategiche presso l'Università degli Studi di Torino ed in Scienze Internazionali e Diplomatiche all'Università degli Studi di Trieste. Per molti anni ha lavorato nel settore dell'Intelligence e Sicurezza, approfondendo studi in materia di terrorismo e, in ambito più strettamente militare, focalizzando il proprio lavoro sulla dottrina e sull'organizzazione delle Forze Armate Russe. È esperto, inoltre, in materia di Information Operations e PsyOps. Ha pubblicato numerosi articoli sulla "Rivista Militare", "Rassegna dell'Esercito", "Informazioni della Difesa", "Rivista Italiana Difesa" (RID), "Difesa Online", "Analisi Difesa", "Limes", "Domino". È socio della Società Italiana di Storia Militare ed ha pubblicato sulla Nuova Antologia Militare, curata dalla stessa. È autore di diversi libri prevalentemente orientati allo studio delle realtà politico-militari di Russia e Cina. Ha svolto diverse collaborazioni con le facoltà di Scienze Politiche delle Università di Torino, Perugia, Trieste, Milano, con l'Istituto per gli Studi di Politica Internazionale (ISPI) di Milano, con lo United Nations Interregional Crime and Justice Research Institute (UNICRI) di Torino, con la Youth Atlantic Treaty Association (YATA) Piemonte.

Le opinioni espresse sono strettamente personali
e non riflettono necessariamente le posizioni dell'Istituto Gino Germani.

© 2026 ISTITUTO GINO GERMANI DI SCIENZE SOCILAI E STUDI STRATEGICI
ISBN: 979-12-98570-795
Via del Commercio 4 – 00015 Monterotondo (RM)
Tel. 06-84969914

fondazionegermani@gmail.com
info@istitutogermani.org
wwwistitutogermani.org

Sommario

Premessa 5

1. Analisi dottrinale **7**

2. Gli errori russi nelle valutazioni strategiche e operative dell'intelligence **9**

3. Il ruolo della *humint* nell' "operazione militare speciale" **11**

4. *Imint* e *targeting*. L'impiego degli *Unmanned Aerial Systems* (UAS) **22**

5. La ricognizione con il fuoco e il movimento **36**

6. Le intercettazioni attraverso la guerra elettronica (EW) e la *signal intelligence (sigint)* a livello tattico **39**

7. Miglioramenti nell'analisi intelligence **44**

8. Integrazione dell'intelligence nel Complesso di Ricognizione e Attacco (RUK) **46**

9. Misure di *opsec* e di counterintelligence russe **49**

10. Il reparto speciale *Centro 795* ***53***

11. Conclusioni **55**

Bibliografia e sitografia *57*

Elenco degli acronimi *73*

Premessa

Tra febbraio 2022 e giugno 2026, la Direzione generale per le informazioni militari (GRU), cioè l'intelligence militare russa, ha attraversato un drammatico ciclo di iniziali fallimenti strategici, ristrutturazioni interne e un cambio di rotta verso operazioni asimmetriche aggressive in tutta Europa.

Nell'evoluzione dell'intelligence militare russa riferita al periodo indicato possiamo individuare tre fasi.

- **Fase 1**, riconducibile al 2022. In questa fase sono ravvisabili gravi errori di valutazione da parte del GRU, ma anche del Servizio di sicurezza federale (FSB) . Le due agenzie hanno drasticamente sottovalutato la resistenza delle Forze armate ucraine e hanno falsamente assicurato al Cremlino che Kiev sarebbe caduta entro pochi giorni. Questo fallimento strutturale ha portato a configurazioni di comando scoordinate, catastrofiche strozzature logistiche e ingenti e inaspettate perdite iniziali.

- **Fase 2**, riconducibile all'arco temporale tra il 2023 e il 2025. In tale periodo emergono una forma di adattamento tecnico con l'attribuzione di un ruolo importante alla guerra elettronica sulla linea del fronte. A seguito delle battute d'arresto iniziali, l'*intelligence* militare russa ha modernizzato le sue tattiche sul campo. Il GRU (ma anche le forze ucraine) ha virato verso il *targeting* algoritmico ad alta velocità[1], utilizzando ampiamente droni da ricognizione assistiti dall'intelligenza artificiale (IA) e integrando la guerra elettronica (EW) per localizzare le posizioni dell'artiglieria ucraina. Ha anche consolidato le strutture di comando e controllo (C2) per centralizzare i dati operativi, sebbene la persistenza di compartimenti stagni sistemici abbia continuamente ostacolato un'ottimale sincronizzazione degli attacchi a lungo raggio.

---

[1] J.-J. Hwang, *Reassessing Biddle's Modern System: data-linked kill chains, advanced algorithms, and the evolution of combined arms warfare in the Russo-Ukrainian war*, Taylor&Francis, 12/05/2026, https://www.tandfonline.com/doi/full/10.1080/14702436.2026.2672089?scroll=top&needAccess=true#abstract.

- **Fase 3** (fine 2025-giugno 2026), in cui il Cremlino si concentra sullo sviluppo di operazioni asimmetriche e ibride nel territorio europeo. Mentre i progressi sul fronte in Ucraina si arrestavano in una estenuante guerra di logoramento, culminata nelle perdite territoriali nette russe nella primavera del 2026, il GRU ha intensificato le sue operazioni esterne. L'*intelligence* russa ha sistematicamente ampliato la guerra di nuova generazione in tutta Europa. Secondo le valutazioni della difesa europea, ciò includeva sabotaggi mirati contro infrastrutture critiche, intrusioni informatiche e minacce dirette ai cavi di comunicazione sottomarini per costringere le potenze occidentali a interrompere il supporto a Kiev[2].

Indicatore strategico	**Situazione al febbraio 2022**	**Situazione al giugno 2026**
Obiettivo primario dell' intelligence	Rapida decapitazione della *leadership* ucraina.	Monitoraggio delle perdite e azioni ibride (sabotaggi) sul territorio europeo.
Perdite stimate	Basse aspettative di partenza.	Tra 1.000.000 e 1.200.000 vittime totali (fino a 500.000 morti).
Operazioni con droni e attività ISR	Ricognizione tattica frammentata.	Picco record di oltre 8.000 droni lanciati mensilmente[3].
Guadagno territoriale	Espansione fulminea attraverso la *blitzkrieg*.	Perdite nette minime; controllo limitato a circa il 12% dell'Ucraina[4].

Tabella comparativa del conflitto russo-ucraino (febbraio 2022 – giugno 2026)

[2] Congessional Research Service, Russian Hybrid Warfare Activities in Europe: Considerations for Congress, 11/08/2026.

[3] https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-may-13-2026.

[4] https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-may-20-2026.

Al mese di giugno 2026, mentre il GRU riusciva a colmare le sue lacune strutturali nell'*intelligence* sul campo di battaglia e nella ricognizione basata sull'uso massiccio di droni, il suo obiettivo si è evoluto da supporto ad una forza di invasione localizzata alla gestione di una vasta e pericolosa campagna ibrida progettata per destabilizzare la sicurezza europea.

1. Analisi dottrinale

Lo scopo principale dell'intelligence militare è quello di fornire supporto alla comprensione del contesto operativo, proteggendo al tempo stesso tutte le informazioni relative alla propria organizzazione. In sostanza, si tratta di conoscere le caratteristiche dell'area delle operazioni, inquadrare l'organizzazione militare e dell'apparato bellico avversario, individuarne le vulnerabilità e i punti di forza, formulare delle ipotesi sulle probabili azioni che il nemico può svolgere e suggerire quali possano essere gli obiettivi più remunerativi da colpire per inibire le suddette operazioni. Tale logica è patrimonio condiviso di tutti gli addetti all'intelligence militare, dunque anche a quelli delle forze armate russe.

Sebbene dalle fonti aperte sia possibile ricavare una visione limitata delle operazioni di intelligence russe, è ragionevole concludere che la gestione russa della funzione operativa dell'intelligence sia stata piuttosto incostante. La Russia ha avviato le operazioni sulle basi di una valutazione intelligence imprecisa. A livello strategico, questa valutazione è stata distorta da presupposti che accompagnano la visione della *leadership* russa secondo cui l'Ucraina è un "Paese artificiale"[5] e che, pertanto, non sarebbe stata coesa di fronte a un'invasione su vasta scala. Nel contesto autoritario della Russia, questo pregiudizio ha indubbiamente influenzato l'analisi strategica dell'intelligence presentata al presidente Vladimir Putin dai suoi servizi di sicurezza. È probabile che l'errata valutazione generata da questa visione sprezzante dell'Ucraina come Paese sia stata amplificata dall'accondiscendenza o, addirittura, da una forma di sudditanza psicologica, all'interno dell'FSB e del GRU nei confronti del presidente stesso.

---

[5] B.A. Düben, *"There is no Ukraine": Fact-Checking the Kremlin's Version of Ukrainian History*, LSE, 01/07/2020. https://blogs.lse.ac.uk/lseih/2020/07/01/there-is-no-ukraine-fact-checking-the-kremlins-version-of-ukrainian-history/.

La corruzione istituzionale è stata un fattore determinante nella scarsa qualità dell'intelligence russa attraverso fonti umane (*humint*). Di conseguenza, l'individuazione degli obiettivi operativi da parte della Russia nei primi mesi dell'operazione militare è stata inefficace e non ha prodotto sull'Ucraina l'effetto devastante che la Russia desiderava. L'incapacità della humint russa di fornire informazioni utili per il *targeting* è stata ridimensionata, in larga misura, dagli adattamenti tecnologici attraverso l'impiego di veicoli aerei senza pilota (UAV) e l'adozione di procedure tecnico-tattiche (TTPs) relative al loro utilizzo. Le nuove capacità di raccolta di dati informativi acquisite dalla Russia con gli UAV sono state fondamentali per i progressi realizzati nelle TTPs operative.

Le crescenti capacità delle forze russe nella raccolta di dati tramite i droni hanno determinato un salto di qualità nella funzionalità del "Complesso di Ricognizione e Attacco" (RUK). Si tratta di una dottrina e di un sistema d'arma integrato utilizzato dalle forze armate russe. Lega strettamente e in tempo reale i dati dell'intelligence, tramite droni o aerei stratosferici, con i sistemi di artiglieria, missili tattici (come gli *Iskander* o i *Tornado-S*) e munizioni circuitanti (*ZALA Lancet*) per colpire bersagli di valore elevato (HVTs) non appena vengono individuati[6]. Il RUK rappresenta la coniugazione di intelligence, comando e controllo e risorse di fuoco che operano in modo sincronizzato per effettuare attacchi precisi, tempestivi e decisivi contro il nemico. Per decenni, si è svolto un dibattito tra gli studiosi militari russi in merito alla necessità del RUK e di come dovrebbe operare. L'invasione sembra avere offerto il contesto per un salto di qualità nella realizzazione di questo ambito sistema.

Anche il controspionaggio russo ha evidenziato aspetti contrastanti. La Russia ha iniziato l'invasione con una sicurezza operativa (*opsec*) discontinua e una sicurezza delle comunicazioni (*comsec*) pressoché inesistente. Le forze armate russe hanno apportato miglioramenti in termini di *opsec* e, in una certa misura, anche nella *comsec*, nel corso dell'invasione. Contestualmente, in diverse occasioni l'FSB non ha esitato a ricorrere a consolidate procedure brutali contro la popolazione civile per imporre la sicurezza operativa nelle aree occupate[7]. In tale quadro rientra l'attività svolta presso i cosiddetti

[6] *Russia demonstrates the Lancet-E RUK at the Dubai Airshow*, Zala, 19/11/2025. https://zala-aero.com/en/news/rossiya-demonstriruet-rabotu-ruk-lanczet-e-na-aviashou-v-dubae/.
[7] P. Sauer, *Hundreds of Ukrainians forcibly deported to Russia, say Mariupol women*, The Guardian, 22/04/2022. https://www.theguardian.com/world/2022/apr/04/hundreds-of-ukrainians-forcibly-deported-to-russia-say-mariupol-women.

"campi di filtraggio" che, di fatto, costituisce un esempio di militarizzazione dei servizi di sicurezza civili russi[8]. Sostanzialmente si tratta di campi di concentramento, utilizzati per registrare, interrogare e detenere cittadini ucraini nelle regioni occupate prima di trasferirli forzatamente in Russia.

2. Gli errori russi nelle valutazioni strategiche e operative dell'intelligence

Uno degli aspetti più sorprendenti dell'intelligence russa a seguito dell'invasione è stato il fallimento nelle previsioni riguardo alla volontà e alle capacità dell'Ucraina di difendersi. I *leader* russi ritenevano che l'invasione si sarebbe conclusa in pochi giorni, non che sarebbe durata anni. La fiducia russa era dimostrata, ad esempio, da articoli precompilati e approvati dal governo che esaltavano il successo di Putin nel ristabilire i confini del "mondo russo". Alcuni di questi articoli sono stati pubblicati *online* per errore[9]. Questa errata valutazione dell'intelligence può essere in parte attribuita ad un *bias* di conferma, ovvero all'illusione russa, sia riguardo alla propria intelligence e alle proprie capacità militari, sia riguardo alla presunta mancanza di volontà e debolezza militare ucraina[10]. Le responsabilità, tuttavia, vanno individuate in carenze dell'intelligence a diversi livelli.

Innanzitutto, a livello di vertice politico, vogliamo prendere in considerazione per la verosimiglianza l'opinione del colonnello in pensione dell'FSB Igor Girkin, molto critico nei confronti degli sforzi bellici della Russia. Girkin, già attivo nel Donbass nel 2014 per l'organizzazione di gruppi paramilitari filorussi attraverso il reclutamento di personale tra i separatisti ucraini, ha dichiarato che la *leadership* russa potrebbe non essere stata pronta ad ascoltare una valutazione onesta. Molte decisioni di alto livello in Russia, infatti,

---

[8] I. Borogan, A. Soldatov, E. Grossfeld, D. Richterova, *What impact has the war on Ukraine had on Russian security and intelligence?*, King's College London, 22/02/2023. https://www.kcl.ac.uk/what-impact-has-the-war-on-ukraine-had-on-russian-security-and-intelligence.

[9] D. Villareal, *State-Run Russian News Site Accidentally Declares Ukraine's Defeat*, Newsweek, 28/02/2022. https://www.newsweek.com/state-run-russian-news-site-accidentally-declares-ukraines-defeat-1683455.

[10] E. Cliszcz, *Russian top ex-commander says Moscow was 'unprepared' for invading Ukraine*, TVP, 03/12/2025. https://tvpworld.com/90354057/russian-ex-commander-chirkin-moscow-was-unprepared-for-ukraine-war.

sembrano essere influenzate da informazioni non veritiere elaborate dai servizi segreti, dai comandanti militari e da cattivi consiglieri e rilasciate a Putin e alla "cerchia ristretta" dei *siloviki* di cui si è circondato[11]. Una classica situazione di ossequio ai progetti del "capo", alimentata dal lui stesso, come spesso accade quando la politica vuole influenzare i risultati dell'attività di intelligence per non vedere messi in discussione i propri piani aprioristicamente concepiti. La convinzione distorta che l'Ucraina non avrebbe opposto una resistenza significativa, con grande probabilità ha influenzato agenzie come l'FSB nelle loro valutazioni di intelligence sulla situazione interna dell'Ucraina. L'accondiscendenza e la superficialità degli operatori *humint* dell'FSB e del GRU responsabili del reclutamento di informatori, insieme all'efficace controspionaggio ucraino, hanno influito sulla formazione da parte della Russia di un quadro di intelligence molto poco accurato, come vedremo successivamente quando tratteremo della *humint*.

Un altro esempio significativo riguarda l'invasione dell'*oblast'* di Kursk da parte delle forze ucraine. Sebbene l'Ucraina abbia dimostrato un'eccellente pianificazione ed un altrettanto ottimo livello di *opsec* per procedere dell'*oblast'* in territorio russo nell'agosto 2024, probabilmente la Russia ha sofferto di pregiudizi analoghi a quelli che hanno portato a sottovalutare le capacità e le intenzioni dell'Ucraina all'inizio dell'invasione[12]. È possibile che, sulla base dei costanti progressi conseguiti nel Donbass, la Russia non abbia sentito l'esigenza di destinare altrove adeguate risorse per la raccolta informativa. La Russia potrebbe semplicemente aver ritenuto di avere sotto controllo tutta la situazione relativa agli schieramenti dell'esercito ucraino. Inoltre, il fatto che la Russia avesse apparentemente perso le tracce di diverse brigate ucraine mette in evidenza alcuni problemi fondamentali con la humint e le capacità di analisi dell'intelligence russa, anche questi aspetti oggetto di una successiva disamina. Un altro problema che potrebbe aver contribuito a questa situazione è stato la lacunosa capacità di acquisizione di immagini aeree e satellitari da parte russa.

---

[11] *Igor Girkin: rebel Donbas leader turned Kremlin critic*, France 24, 28/08/2023. https://www.france24.com/en/live-news/20230829-igor-girkin-rebel-donbas-leader-turned-kremlin-critic.

[12] M. Trevelyan, A, Malenko, G. Stolyarov, *"A complete intelligence failure": how Russia looked the wrong way as Ukraine invaded*, Breakingnews, 17/08/2024. https://www.breakingnews.ie/explained/analysis-how-russia-looked-the-wrong-way-as-ukraine-invaded-1662303.html.

3. Il ruolo della *humint* nell' "operazione militare speciale"

Come abbiamo visto, l'atteggiamento sprezzante nei confronti dell'Ucraina, la corruzione tra i *leader* russi e la discutibile di onestà intellettuale hanno generato i presupposti per un approccio inadeguato all'intelligence e, di conseguenza, indotto a valutazioni errate. All'inizio dell'invasione russa dell'Ucraina nel 2022, l'intelligence di Mosca (in particolare il 5° Servizio dell'FSB) ha riscontrato gravi difficoltà nel reclutare e mantenere spie ucraine affidabili. Negli anni precedenti all'invasione il Cremlino ha speso milioni di dollari per costruire una fitta rete di collaboratori e infiltrati all'interno delle istituzioni, delle forze armate e del Servizio di sicurezza dell'Ucraina (SBU):

> *"Il mese scorso, le autorità ucraine hanno arrestato un altro ufficiale dell'SBU, Oleg Kulinich, che era stato insediato ai vertici del servizio da Bakanov, direttore dell'SBU e amico d'infanzia di Zelensky. Le accuse contro Kulinich sottolineano la pervasività delle infiltrazioni russe. Le accuse presentate dalle autorità ucraine lo descrivono come parte di una cellula di agenti dormienti gestita da Vladimir Sivkovich, ex vice capo del Consiglio di sicurezza ucraino, sanzionato dal Dipartimento del Tesoro statunitense a gennaio per aver collaborato "con una rete di agenti dei servizi segreti russi per condurre operazioni di influenza". Secondo l'atto d'accusa, due anni prima della guerra Sivkovich "affidò a Kulinich il compito" di iniziare a rubare file interni segreti dell'SBU che sarebbero stati "di interesse operativo" per i "servizi speciali della Federazione Russa". Secondo il documento, avrebbero cospirato insieme per favorire la nomina di un altro presunto agente segreto russo al controllo del dipartimento di controspionaggio dell'SBU. Tale figura, Andriy Naumov, è stata arrestata in Serbia a giugno con denaro contante e gioielli per un valore superiore a 700.000 dollari, secondo quanto riportato dalle autorità serbe[13]."*

Tuttavia , questo sistema è crollato nei primi mesi del conflitto per diverse ragioni critiche.

All'atto dell'invasione gli organi incaricati della ricerca informativa tramite fonti umane includevano informatori, osservatori e specialisti dei "gruppi di ricognizione e sabotaggio" (DRG). Uno degli sforzi prioritari su cui si è concentrata la *humint* russa è stato il reclutamento di spie in tutta l'Ucraina. In generale, la prassi prevede che funzionari del GRU e dell'FSB siano infiltrati

[13] G. Miller, C. Belton, *Russia's spies misread Ukraine and misled Kremlin as war loomed*, The Washington Post, 19/08/2022. https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/.

in Ucraina con la missione di reclutare informatori che possano riferire sull'attività delle truppe nemiche e su altri obiettivi di valore militare, in considerazione che anche strutture eminentemente civili possono essere di interesse sotto il profilo militare. A tal fine, vengono stanziati fondi per pagare informatori ed osservatori di nazionalità ucraina o, comunque, presenti sul territorio ucraino. Accanto a questi agenti, fin dalle prime fasi dell'invasione fanno la loro comparsa i DRG, piccole unità di personale, di massima inquadrato nelle unità *spetsnaz* del GRU, ma non solo, addestrate per condurre ricognizioni operative in profondità nel territorio nemico e attività di sabotaggio. Dal 2025 è stato intensificato l'impiego di queste unità per cercare di trovare una soluzione alla fase di stasi che vede l'esercito russo compiere pochi e faticosi progressi, a costi molto elevati in termini uomini, mezzi e materiali:

> *"Dalla primavera del 2025, la Russia impiega i Gruppi di Ricognizione e Sabotaggio (DRG) per individuare le falle nelle difese ucraine e i punti deboli che consentirebbero alle forze meccanizzate di penetrare. ... Le unità DRG russe sono composte da tre a dieci uomini, la maggior parte dei quali integrati in forze speciali come Spetsnaz e SSO, o in reparti specializzati come la fanteria di marina (marines). Lo scopo principale dei Gruppi di Ricognizione e Sabotaggio comprende operazioni di sabotaggio , l'apertura di varchi in settori di fortificazioni scarsamente difesi, la raccolta di informazioni e il mantenimento di settori chiave per potenziali sfondamenti[14]."*

Peculiare di queste squadre è il fatto che in diversi casi agiscano indossando vestiti civili[15] in modo da potersi muovere agevolmente oltre le linee nemiche e assolvere i compiti ricevuti riducendo al massimo i rischi. A tale proposito, non va dimenticato che nel diritto internazionale umanitario, un soldato che indossa abiti civili per ingannare il nemico e attaccarlo commette un grave illecito denominato perfidia, classificato come crimine di guerra.

Fin dalle prime settimane di guerra, l'SBU e le forze di polizia ucraine hanno avviato una durissima campagna interna di controspionaggio. La stragrande maggioranza dei collaboratori russi d'alto livello all'interno dell'apparato statale

---

[14] J. McBride, *How Small Reconnaissance Units are Playing a Critical Role in Russian Frontline Movements in 2025*, Atlas institutw for International Affairs, 19/11/2025. https://atlasinstitute.org/how-small-reconnaissance-units-are-playing-a-critical-role-in-russian-frontline-movements-in-2025/.

[15] A. MacAlpine, *Russian soldiers disguised in civilian clothes infiltrating front-line city*, The Telegraph, 13/08/2025. https://www.telegraph.co.uk/world-news/2025/08/13/russian-soldiers-disguised-civilian-clothing-infiltrating/.

o militare è stata rapidamente arrestata, neutralizzata o costretta a fuggire in Russia. Questo ha reciso i canali di comunicazione diretta e ha privato i gestori russi delle loro fonti più preziose e affidabili. Nel corso del conflitto l'SBU ha continuamente arrestato spie, sabotatori ed elementi del DRG in tutta l'Ucraina. All'inizio dell'offensiva, la maggior parte di queste attività era concentrata Kiev e dintorni, in città come Irpin, Bucha, Hostomel, Dymer, Ivankov e Baryshevka[16]. Successivamente, gli ucraini hanno scoperto queste attività anche a Odessa, Kherson, nell'*oblast'* di Sumy, Mykolaiv, nell'*oblast'* di Zaporizhzhia e persino in zone dell'Ucraina occidentale. Fin dal primo giorno dell'invasione, a Kiev sarebbero stati operativi dei sabotatori russi vestiti con uniformi ucraine, catturati o uccisi alle Forze di Difesa Territoriale ucraine[17].

Con le cautele del caso, in quanto le fonti a cui si fa riferimento sono prevalentemente ucraine, vediamo alcuni esempi delle attività di spionaggio svolto a favore delle forze di invasione nelle prime fasi della stessa. Per la tipologia dei dati richiesti alle fonti appare particolarmente rilevante la ricerca di elementi utili all'effettuazione di *targeting* che, come ha confermato lo sviluppo successivo del conflitto, è diventata la modalità di combattimento predominante sui due fronti, con il massiccio uso di droni e, da parte russa, anche missili.

All'inizio del mese di marzo 2022, è stata catturata una spia a Ivano-Frankivsk, nell'Ucraina occidentale. Secondo quanto riferito dai servizi di sicurezza ucraini

> *"Il traditore è arrivato a Ivano-Frankivsk il 22 febbraio. Si è sistemato in un motel vicino all'aeroporto. Il 23 febbraio, alla vigilia dell'attacco missilistico russo contro l'Ucraina, ha trasmesso alla Russia informazioni sull'ubicazione di una struttura militare. A seguito dell'impatto dei missili sull'aeroporto, le sue infrastrutture sono state distrutte. Dopo l'attacco all'aeroporto, l'uomo ha riferito alla Russia gli esiti dello stesso[18]."*

A Odessa, nell'estate del 2022, l'SBU ha arrestato un individuo accusato di aver fornito ai servizi segreti russi (non è specificato se il GRU o l'FSB) le posizioni

---

[16] O. Roshchina, *Saboteurs are operating in Kyiv, Russian troops are going round in circles near Kyiv - head of the Kyiv Military Administration*, Ukrainska Pravda, 17/03/2022. https://www.pravda.com.ua/eng/news/2022/03/17/7332137/.

[17] *Weapons & equipment seized from alleged Russian saboteurs in Ukraine (2022)*, ARES, 25/03/2022. https://armamentresearch.com/weapons-equipment-seized-from-alleged-russian-saboteurs-in-ukraine-2022/.

[18] R. Kravets, *Ukraine's Security Service catches man who facilitated Russian missile strike at Frankivsk Airport*, Ukrainska Pravda, 02/03/2022. https://www.pravda.com.ua/eng/news/2022/03/02/7327421/.

delle forze ucraine nei pressi della città e di aver contribuito alla designazione di obiettivi da colpire nella zona di Odessa. In riferimento alla persona arrestata, il comunicato dell'agenzia di intelligence ucraina riporta quanto segue:

"I suoi messaggi al nemico includevano:

• coordinate precise delle installazioni di difesa sulla mappa;

• descrizioni dettagliate delle condizioni delle strutture, dei materiali utilizzati per la loro costruzione, dello scopo e dell'uso da parte dei militari, del territorio circostante;

• numero di personale e attrezzature militari presenti in tali siti e i loro spostamenti;

• numero di fortificazioni attrezzate.

Gli occupanti hanno utilizzato queste informazioni per pianificare le attività dei loro gruppi di sabotaggio e condurre massicci attacchi missilistici mirati[19]*."*

Il telefono della conteneva comunicazioni compromettenti con destinatari in Russia e Bielorussia[20].

Per restare in tema, a Sumy l'SBU ha arrestato una donna accusata di aver fornito le coordinate per un attacco sulla città con droni *Shahed* nella notte del 7 settembre 2023. Si trattava di una cittadina della Federazione Russa, con un permesso di soggiorno in Ucraina, che viveva a Sumy da oltre dieci anni. Secondo l'SBU, la donna avrebbe dovuto svolgere vere e proprie attività di intelligence creando una piccola rete locale di spie, allo scopo di raccogliere dati sull'ubicazione di installazioni militari e infrastrutture critiche e sui movimenti di equipaggiamento militare, che potessero compromettere le capacità di difesa ucraine[21].

È indicativa la vicenda di Vladimir e Dmitry Mamon, due fratelli, in passato residenti a Hroza (*oblast'* di Kharkiv), che avevano iniziato a collaborare con i russi durante l'occupazione della regione e, dopo la liberazione, erano fuggiti in Russia, ma avevano continuato a mantenere contatti sociali nel villaggio per formare una rete di informatori nel territorio tornato sotto il controllo

[19] *Russian agent arrested in Odesa*, Kyiv Post, 15/08/2022. https://www.kyivpost.com/post/1745.
[20] Ibid.
[21] *Network of agents and coordinates of the deployment of Ukrainian troops: law enforcement officers detained a Russian woman in Sumy region*, MSV, 08/09/2023. https://mvs.gov.ua/en/news/mereza-agentiv-ta-koordinati-rozmishhennia-ukrayinskix-viisk-pravooxoronci-zatrimali-rosiianku-na-sumshhini.

ucraino. Secondo quanto riferito dall'SBU dopo la loro identificazione, all'inizio dell'ottobre 2023 i due uomini avrebbero iniziato a raccogliere informazioni sulla cerimonia commemorativa di un soldato ucraino deceduto a Hroza, fornendo ai russi l'orario preciso della cerimonia. In quell'occasione le forze del Cremlino lanciarono un missile *Iskander-M* sul villaggio, che causò la morte di 59 civili, nell'auspicio che fossero presenti anche i commilitoni del soldato deceduto[22].

Anche il settore di Mykolaiv è stato particolarmente interessato da queste attività di humint finalizzata al targeting. Durante i primi mesi dell'invasione, l'area della città, infatti, è stata frequentemente attaccata da missili e artiglieria delle forze russe. Per facilitare questi attacchi, i russi hanno impiegato civili ucraini come "osservatori" per rivelare la posizione di unità ucraine e altre postazioni militari. Il reclutamento si è svolto attraverso annunci su Telegram promettendo l'anonimato al personale interessato e compensi di circa 30-40 dollari per i dati forniti. Considerando la tipologia degli obiettivi colpiti dall'artiglieria russa in quella fase della guerra, si può ritenere che non sia stata fatta un'elaborazione molto accurata dei dati raccolti da parte dell'intelligence militare delle forze di invasione o che non abbia nemmeno cercato di verificare o corroborare questi dati ricevuti. D'altra parte, si può ritenere che gli informatori fossero interessati solo al denaro, o semplicemente, non fossero molto bravi a segnalare con precisione le posizioni degli obiettivi militari. Nel luglio 2022, l'SBU ha scoperto un gruppo organizzato di residenti nell'area di Mykolaiv che agivano come spie per le forze russe. Il gruppo disponeva di telefoni cellulari e computer portatili per inviare i dati al loro referente russo attraverso canali di comunicazione sicuri. In risposta a questo problema crescente, il governatore di Mykolaiv, Vitalij Kim, ha deliberato di offrire 100 dollari a tutti coloro che avessero identificato e denunciato una spia. Per contro, molti cittadini segnalarono i sospetti informatori, senza voler riscuotere il compenso[23].

---

[22] K. Katishev, *Разоблачены наводчики ракеты на село Гроза (I responsabili del puntamento del missile sono stati smascherati)*, Kommersant, 11/10/2023. https://korrespondent.net/ukraine/4630596-razoblacheny-navodchyky-rakety-na-selo-hroza.

[23] J. Kakissis, *Ukraine hunts for pro-Moscow collaborators suspected of helping Russia strike target*s, Npr, 21/09/2022. https://www.npr.org/2022/09/21/1124108146/ukraine-russia-suspected-collaborators-mykolaiv.

A quasi cinque anni dall'inizio dell'invasione, nulla è cambiato e queste attività sono proseguite in tutto il periodo della guerra, come è normale che accada. Un esempio tra tutti, un evento verificatosi ad Odessa nell'estate del 2026:

> *"Un uomo del posto avrebbe presumibilmente aiutato l'intelligence russa mappando siti di difesa e nominando obiettivi, provocando una rapida operazione di controspionaggio da parte delle autorità ucraine.…Il centro stampa dell'SBU ha affermato che l'indagine punta a un residente locale che ha attirato l'attenzione dell'FSB a causa di pubblicazioni a sostegno del regime del Cremlino e delle formazioni armate russe su canali Telegram. È stato documentato che l'agente monitorava le basi delle Forze di Difesa che la Russia intendeva colpire con attacchi missilistici e di droni. I russi erano particolarmente interessati ai centri di fuoco della difesa aerea e all'ubicazione dei depositi logistici delle Forze Armate ucraine nel sud del paese.…Secondo gli inquirenti e il controspionaggio militare, per monitorare i dati sulle installazioni militari il sospettato si spostava in auto nella zona; Dopo aver effettuato una ricognizione, trasmetteva le informazioni al funzionario nella Federazione Russa tramite un'app di messaggistica, per poi cancellare le chat.…Il criminale ha inoltre consegnato a un rappresentante dei servizi di sicurezza russi dati riguardanti un consigliere comunale e un membro della Guardia Nazionale ucraina, che conosceva personalmente, come possibili obiettivi da eliminare[24]."*

È interessante prendere in considerazione l' "effetto specchio" (*mirroring*) che ha indotto a diversi casi di valutazioni errate, basate sul presupposto che il nemico adotta il nostro lo stesso comportamento, in pratica, ragiona come noi. Nella fase iniziale dell'invasione, era convinzione dei russi che le TTPs adottate dagli Ucraini sarebbero state le medesime di quelle russe. Tale convinzione ha determinato errori significativi nel *targeting*, aggravati da una cattiva *humint*, incapace di fornire dati aggiornati e veritieri. È quanto è accaduto all'inizio di giugno 2022, quando la Russia ha attaccato l'impianto di riparazione di vagoni ferroviari Darnitsky a Kiev con un missile da crociera. Il Ministero della Difesa russo ha affermato che la struttura fosse ritenuto un deposito per carri armati T-72 forniti dall'Occidente. Un video successivo ha mostrato l'assenza di carri armati o altre attrezzature militari nell'impianto distrutto. Le forze aeree russe stavano sistematicamente prendendo di mira qualsiasi deposito ferroviario per intercettare le attrezzature militari fornite dall'Occidente, nella fase di consegna all'Ucraina[25]. A causa dell'effetto spec-

---

[24] *SBU arrested an FSB agent in Odesa for spying on Ukrainian defenses*, Mezha, 30/06/2026. https://mezha.net/eng/news/7c7210b2_sbu_arrested_an/.

[25] *Darnytskyi Car Repair Plant after Russia's missile strikes: Production shops destroyed but no tanks,* Ukrinform, 06/06/2022. https://www.ukrinform.net/rubric-ato/3500583-darnytskyi-car-repair-plant-after-russias-missile-strikes-production-shops-destroyed-but-no-tanks.html.

chio, i russi presumevano che le forze ucraine avrebbero trasportato l'equipaggiamento militare quasi esclusivamente via ferrovia, secondo gli *standard* operativi delle logistica russa.

La corruzione sistemica ha notevolmente compromesso la qualità dell'intelligence russa. Sebbene gli agenti russi siano riusciti a reclutare informatori in tutta l'Ucraina, come detto la Russia non aveva un quadro chiaro dell'atteggiamento del popolo ucraino e della sua volontà di resistere. Per giustificare gli enormi budget ricevuti dal Cremlino, i responsabili russi del reclutamento hanno sistematicamente alterato i rapporti, affermando che la popolazione ucraina avrebbe accolto i soldati russi a braccia aperte e che il governo di Zelensky sarebbe caduto in pochi giorni. Quando l'invasione è iniziata, la rete di spie pazientemente intessuta si è volatilizzata[26] o si è rivelata decisamente impreparata, non avendo alcuna reale capacità di cogliere gli eventi, influenzarli come da prassi invalsa del sistema dell'intelligence di Mosca e, soprattutto, fornire informazioni utili in uno scenario di guerra aperta. In molti casi, i reclutatori hanno presentato falsi rapporti e si sono intascati le somme da corrispondere agli agenti ucraini iscritti "a libro paga". È verosimile, altresì, che alcune spie in realtà non abbiano agito nell'interesse della causa russa, ma lo abbiano fatto solo per intascare i compensi pattuiti. E non solo, molti cittadini ucraini inizialmente considerati "simpatizzanti" o avvicinati dall'intelligence russa prima del 24 febbraio 2022 hanno cambiato radicalmente posizione di fronte all'orrore dei bombardamenti e dei massacri civili. Alcuni di coloro che erano stati reclutati hanno deciso di fare il doppio gioco, fingendo di collaborare con Mosca ma passando in realtà le informazioni cruciali all'intelligence ucraina. È il caso di Denys Kireyev, un banchiere ucraino con profondi contatti nell'FSB russo, che ha utilizzato i suoi canali per avvertire la difesa ucraina del piano russo di catturare l'aeroporto di Hostomel, contribuendo al fallimento dell'operazione pianificata dai russi per attuare la rapida occupazione di Kiev nelle prime ore del conflitto[27].

---

[26] V. Lytovchenko, *Russia tries to recruit spies among Ukrainians using blackmail*, Online.Ua, 04/04/2024. https://news.online.ua/en/russia-tries-to-recruit-spies-among-ukrainians-using-blackmail-876092/.

[27] R. Armitage, *Denys Kireyev was a Ukrainian spy hailed as a hero who saved Kyiv from Russian invaders. So why was he killed for treason?*, ABC, 02/02/2023. https://www.abc.net.au/news/2023-02-03/mystery-over-killing-ukrainian-spy-denys-kireyev/101915844.

Venuta meno la disponibilità delle fonti di elevato profilo e stante la scarsa affidabilità dei propri professionisti dell'intelligence, la Russia si è trovata impossibilitata a reclutare figure chiave della società ucraina. Questo fallimento ha costretto Mosca a cambiare completamente strategia, passando dal reclutamento ideologico o mirato a tecniche di ricatto violento e al cosiddetto *trash fishing*. L'FSB ha iniziato a contattare sistematicamente i civili ucraini i cui parenti erano stati presi in ostaggio o fatti prigionieri di guerra, minacciando di torturarli o ucciderli se i familiari non avessero accettato di spiare le posizioni militari dell'esercito ucraino[28]. Riguardo al *trash fishing*, si tratta di una procedura di reclutamento *online* utilizzata dai servizi segreti russi e, sembrerebbe, anche dal *Gruppo Wagner* (prima del suo scioglimento), per adescare persone comuni in gravi difficoltà economiche, criminali di poco conto, soggetti vulnerabili e, addirittura adolescenti ignari, tramite *social network* e *chat* criptate (specialmente *Telegram*)[29]. Lo scopo è quello di assegnare loro piccoli compiti di spionaggio - come fotografare infrastrutture registrare gli orari di transito di convogli ferroviari - o attuare dei sabotaggi che non presentino grosse difficoltà di realizzazione, in cambio di poche centinaia di dollari. Tale attività, iniziata con l'invasione, è proseguita nel corso del conflitto[30]. Questa tipologia di agenti, tuttavia, si è dimostrata altamente inaffidabile, priva di addestramento e facilmente individuabile dal controspionaggio ucraino. L'incapacità iniziale di strutturare una rete di spie solida e fedele rimane considerata dagli analisti militari uno dei più grandi errori strategici della campagna russa in Ucraina.

Un altro aspetto di non secondaria importanza riguarda la cultura russa della "*leadership* a zero difetti", per cui c'è un'enorme pressione per riferire che tutto sta andando "secondo i piani". Pertanto, anche se si ha poca fiducia nelle informazioni di intelligence, o si nutrono dubbi sulla capacità degli agenti di fornire rapporti accurati, c'è pressione per riportare ciò che il proprio superiore vuole sentirsi dire. Se il capo vuole che il quadro dell'*intelligence* mostri un'Ucraina che probabilmente capitolerà rapidamente, questo è ciò

[28] V. Lytovchenko, cit.

[29] J. Simpson, D. Gardham, *Telegram, 'trash fishing' and the Wagner Group plot to groom UK criminals for 'grey zone' attacks*, The Observer, 12/07/2025. https://observer.co.uk/news/national/article/telegram-trash-fishing-and-the-wagner-group-plot-to-groom-uk-criminals-for-grey-zone-attacks.

[30] *How Russia recruits spies through social media*, Kyiv Independent, 02/08/2026. https://www.youtube.com/watch?v=pITde5slL0A.

che gli viene comunicato, indipendentemente dal fatto che l'intelligence lo confermi o meno. Questa cultura di ossequio e deferenza nei confronti di una *leadership* poco propensa ad accettare realtà che mettono in discussione i suoi progetti determina una debole capacità di *humint*, basata su reti di informatori tutt'altro che ideali, o addirittura inesistenti. Le informazioni provenienti da fonti aperte sul Colonnello Generale Sergey Beseda, direttore del 5° Servizio dell'FSB dal 2009 a giugno 2024, sottolineano questa ambiguità:

"Il dipartimento è supervisionato da un alto ufficiale dell'FSB, Sergey Beseda, che, secondo fonti ucraine, ha iniziato la sua carriera nel KGB alla fine degli anni '70 ed è stato assegnato a incarichi all'estero, tra cui Cuba, prima di tornare a Mosca per dirigere le operazioni in Ucraina, Georgia e altre ex repubbliche sovietiche. Dopo lo scoppio delle proteste a Kiev alla fine del 2013 contro il governo filorusso di Viktor Yanukovych, Beseda si presentò nella capitale ucraina esortando Yanukovych a usare la forza letale per reprimere una rivolta che sarebbe poi passata alla storia come la Rivoluzione di Maidan, secondo quanto riferito da funzionari ucraini. Quando le proteste ebbero la meglio, Yanukovych fuggì in Russia con un gruppo di consiglieri di alto livello sospettati di aver collaborato con la filiale di Beseda negli anni successivi per riportare al potere un governo filo-russo. Quel progetto sembrò assumere una nuova urgenza nei due anni precedenti all'invasione di febbraio. Nel 2019, l'FSB ha avviato una significativa espansione della sua unità in Ucraina, un gruppo che, secondo funzionari ucraini che hanno citato intercettazioni di comunicazioni e altre informazioni di intelligence, è passato da 30 a ben 160 agenti la scorsa estate. Per attirare reclute da altri rami dell'FSB, venivano offerti bonus e alloggi gratuiti in edifici adiacenti all'accademia di addestramento dell'FSB presso Michurinsky Prospekt a Mosca, hanno riferito funzionari. Gli ufficiali appena arrivati venivano assegnati a territori in Ucraina e incaricati di stilare liste di collaboratori con cui lavorare, nonché di avversari da neutralizzare. Inizialmente, l'offensiva fu vista come un'altra iniziativa volta a "ristabilire l'influenza russa in Ucraina", ha affermato un funzionario della sicurezza di Kiev coinvolto nel monitoraggio delle operazioni dell'FSB. Ma, a posteriori, potrebbe essere stato un primo segnale che la Russia stava spostando la sua attenzione dal plasmare gli eventi in Ucraina al pianificare "la sua conquista". ... "Non ci aspettavamo... un'invasione classica in stile Seconda Guerra Mondiale con carri armati, artiglieria e fanteria", ha dichiarato un alto funzionario della sicurezza ucraina. L'Ucraina si sbagliava sulle intenzioni della Russia, ha aggiunto, ma forse nemmeno Mosca aveva previsto una guerra terrestre di tali proporzioni. "Si aspettavano che qualcuno aprisse il cancello", ha detto il funzionario. "Non si aspettavano alcuna resistenza." ... Quasi tutti i servizi segreti coinvolti nella guerra hanno commesso errori di valutazione con conseguenze significative. Le agenzie di spionaggio statunitensi avevano previsto le intenzioni di Putin, ma hanno sottovalutato la capacità dell'Ucraina di resistere all'attacco: un errore che ha contribuito all'iniziale esitazione degli Stati Uniti nell'inviare armi pesanti e sofisticate. Sembra che i servizi segreti ucraini abbiano interpretato in modo eccessivo i segnali che indicavano una scarsa preparazione delle forze russe a un combattimento

su vasta scala, ignorando gli avvertimenti occidentali di un'invasione che si era avvicinata a pochi chilometri dalla capitale. I fallimenti dell'intelligence russa in Ucraina sembrano essere di natura più sistemica: il suo lavoro è stato viziato da fonti inaffidabili, da disincentivi a rivelare verità scomode al Cremlino e da un pregiudizio endemico che rispecchiava l'atteggiamento sprezzante di Putin nei confronti del Paese. Secondo quanto riferito da alcuni funzionari, l'FSB ha alimentato questa dinamica con valutazioni formulate in modo da compiacere il Cremlino e con fonti che avevano i propri motivi – politici e finanziari – per incoraggiare un colpo di stato russo contro il governo di Kiev. ... Le conseguenze per l'FSB sono state difficili da accertare a causa dell'oscuramento delle informazioni imposto ai media russi da Putin. Le prime notizie secondo cui Beseda, responsabile della direzione dell'FSB per l'Ucraina, sarebbe stato retrocesso o addirittura incarcerato, sono accolte con scetticismo dagli ufficiali dell'intelligence statunitense e di altri paesi, i quali affermano di non aver ricevuto alcuna informazione che suggerisca che alcuno dei capi dei servizi segreti russi abbia subito tali conseguenze. "Abbiamo ottime ragioni per credere che sia ancora al suo posto", ha dichiarato un alto funzionario statunitense a proposito di Beseda. Il funzionario ha aggiunto che non vi è alcuna indicazione che il capo dell'FSB, Alexander Bortnikov, sia stato chiamato a rispondere dei fallimenti della sua agenzia. Anche un importante politico russo con stretti legami con il Cremlino e con l'FSB ha affermato in un'intervista che Beseda continua a svolgere le sue funzioni[31]."

Beseda era responsabile dell'*intelligence* sulla situazione politica in Ucraina prima che la Russia lanciasse l'invasione. Questa apparente deresponsabilizzazione per un'operazione di intelligence fallita potrebbe essere dovuta a una combinazione di riluttanza ad ammettere l'errore e a un sistema intrinsecamente corrotto, consapevole delle responsabilità a diversi livelli politico-militari, non ultima quella del Presidente Putin.

Va detto che, in verità, le attività di *humint* condotte dalla Russia cono state anche coronate da successo, come nel caso di un episodio particolarmente significativo verificatosi nel 2022 e rivelato l'anno successivo, in cui è possibile intravedere un'efficace coordinamento tra *humint* e *counterintelligence*. Nell'aprile 2023, sui *social media* ucraini è apparsa una notizia riguardante un tentativo di ucraino risalente al 2022 per reclutare piloti delle Forze aerospaziali russe (VKS), al fine di consegnare aerei delle VKS in Ucraina.

"Il Servizio di sicurezza dell'Ucraina (SBU) sta indagando sulle circostanze che hanno portato all'attacco missilistico contro l'aeroporto di Kanatove, avvenuto il 23 luglio

[31] G. Miller, K. Belton, cit.

2022. L'incidente sarebbe stato causato da un tentativo fallito di reclutare piloti e velivoli delle Forze aerospaziali russe. Secondo quanto dichiarato dall'agenzia, il piano è stato organizzato da militari ucraini senza l'approvazione dell'SBU. Alla fine di luglio 2022, i media russi hanno diffuso dettagli del complotto, sostenendo che membri dei servizi speciali ucraini avessero offerto ai piloti russi fino a 2 milioni di dollari, oltre alla garanzia di ottenere la cittadinanza di uno Stato baltico per le loro famiglie. Nel corso di questa 'operazione', condotta nonostante le obiezioni dell'SBU e senza alcun coordinamento con le autorità statali competenti, il nemico ha ottenuto informazioni sulla dislocazione del personale dell'Aeronautica militare ucraina e dei velivoli ucraini", ha spiegato l'SBU in una nota. "Tali informazioni hanno permesso all'Aeronautica russa di colpire l'aeroporto di Kanatove, nella regione di Kirovohrad". Al momento dell'attacco, l'aeroporto di riserva di Kanatove, nell'Ucraina centrale, ospitava uno squadrone di caccia Su-27 dell'Aeronautica ucraina. I bombardamenti hanno causato la morte del comandante dell'unità militare e il ferimento di 17 soldati ucraini; due caccia Su-27 sono stati distrutti e le infrastrutture della base aerea hanno subito danni[32]."

La versione riportata dai media russi è leggermente diversa, ma la sostanza non cambia:

"Venerdì, il Servizio di sicurezza dell'Ucraina (SBU) ha reso noto che un ex comandante ad interim di un'unità delle forze per le operazioni speciali ucraine è stato incriminato per abuso di potere; l'uomo, la scorsa estate, aveva tentato autonomamente – e senza alcun coordinamento – di condurre un'operazione per impadronirsi di un velivolo delle Forze aerospaziali russe, provocando di fatto una rappresaglia missilistica contro un aeroporto ucraino. Roman Chervinsky, ex comandante ad interim di un'unità delle forze per le operazioni speciali, è stato accusato di iniziative arbitrarie che hanno portato ad attacchi missilistici contro l'aeroporto di Kanatovo, nella regione di Kirovohrad, nell'estate del 2022; la notizia è stata diffusa dall'SBU tramite il proprio canale Telegram. L'ufficiale è stato incriminato per abuso di potere. Secondo quanto riferito, il piano per l'operazione speciale non era stato approvato né dall'SBU né dalla Direzione principale dell'intelligence del Ministero della Difesa: l'accusato aveva deciso di agire di propria iniziativa. Ciò ha causato la fuga di informazioni relative allo schieramento di personale militare e mezzi presso l'aeroporto di Kanatovo. A seguito dell'attacco alla struttura, il comandante dell'unità militare è rimasto ucciso e 17 militari sono rimasti feriti; inoltre, due caccia sono stati distrutti e la pista è stata danneggiata[33]."

---

[32] C. Charpentreau, *Ukraine probes failed plot to recruit Russian military pilots*, AeroTime, 21/04/2023. https://www.aerotime.aero/articles/ukraine-probes-failed-plot-to-recruit-russian-military-pilots.

[33] *Army officer in Ukraine faces charges for failed recruitment of Russian pilots*, Tass, 21/04/2023. https://tass.com/defense/1607951.

4. *Imint* e *targeting*. L'impiego degli *Unmanned Aerial Systems* (UAS)

Sebbene, prima dell'invasione la Russia utilizzasse già i droni per l'attività di ricerca e raccolta di dati informativi tramite immagini (*imint*) e, talvolta, attraverso l'intelligence delle trasmissioni (*sigint*), sembra che per l'intelligence operativa le forze armate russe intendessero affidarsi principalmente alla *humint*, come discusso in precedenza. La Russia ha dovuto confrontarsi con le efficaci TTPs ucraine di contrasto ai droni e l'efficace utilizzo degli stessi da parte delle forze di Kiev per la ricerca informativa, la sorveglianza e la ricognizione (ISR). La Russia, allora, ha compreso e sfruttato appieno il potenziale dei droni. Ha ulteriormente sviluppato lecapacità tecniche e le relative TTPs per massimizzare l'efficacia e la tempestività della raccolta di dati. Il risultato è stato un salto di qualità nella capacità delle truppe di occupazione di raccogliere e trasmettere in tempo reale dati riferiti agli obiettivi designati. Nel teatro operativo ucraino, l'impiego russo di droni ad ala fissa a corto raggio (entro i 30-40 km) è diventato un elemento centrale della dottrina tattica. Questi velivoli sono utilizzati principalmente per l'interdizione del campo di battaglia (BAI), la ricognizione tattica e gli attacchi di precisione contro i dispositivi logistici (posti comando, punti distribuzione materiali, punti di manutenzione e recupero mezzi, punti raccolta feriti), assicurati dai plotoni MTO (*Material Technical Organization*, unità logistica corrispondente alla prima linea di sostegno NATO) a sostegno diretto ai gruppi tattici, contro i convogli per gli avvicendamenti delle truppe e contro i veicoli corazzati.

Le attività di ricognizione sono svolte con UAV *Orlan-10* e *Orlan-30*, impiegati a livello tattico in un raggio d'azione tra i 10 e i 30 chilometri, sebbene abbiano una portata massima teorica superiore, soprattutto per dirigere il tiro dell'artiglieria. Il loro impiego è orientato alla sorveglianza dell'area della battaglia per tempi prolungati, alla guerra elettronica e, nel caso dell'*Orlan-30*, alla designazione laser dei bersagli per munizioni circuitanti. Gli *Orlan-10* individuano il bersaglio e trasmettono le coordinate per l'impiego dei *droni-kamikaze*. È quanto avviene con i droni Lancet, che operano quasi sempre in coordinamento con gli *Orlan*, usati per attacchi di precisione contro artiglieria, sistemi radar, contraerea e veicoli blindati ucraini[34].

[34] *War of Drones: what kind of 'kamikaze' drones Ukraine and Russia use*, Espreso, 28/07/2023. https://global.espreso.tv/war-of-drones-what-kind-of-kamikaze-drones-ukraine-and-russia-use.

All'inizio dell'invasione, le forze armate russe utilizzavano principalmente UAV *Orlan-10* per la ricognizione, forti dell'esperienza acquisita con il loro precedente impiego nel Donbass e in Siria. In Siria, in particolare, le Forze aerospaziali e probabilmente anche le Forze terrestri utilizzavano questi UAV a distanze operative già dall'autunno del 2015. Inizialmente questa pratica, però, non si è rivelata vincente nell'ambito dell'invasione. Nei primi mesi dell'operazione, gli ucraini hanno abbattuto un gran numero di questi droni utilizzando vari metodi, tra cui attacchi cinetici[35] e l'*hacking* dei sistemi di controllo dei droni[36], costringendoli ad effettuare atterraggi di emergenza. Con l'aumentare delle perdite, le forze armate russe hanno persino iniziato a requisire i droni *Orlan-10* dal Ministero delle Situazioni di Emergenza della Federazione Russa, per colmare le lacune. Successivamente, i russi si sono risolti ad integrare i droni Orlan-10 con una serie di altri droni da ricognizione come il *Forpost*[37], l'*Orion Pacer*[38], il *Merlin*[39], l'*Horizont Air S-100*[40], il *Supercam S450*[41] e persino il drone *Kartograf*[42], dotato di 12 obiettivi fotografici progettati per creare prodotti topografici. Diamo qualche cenno sulle caratteristiche di questi droni da ricognizione impiegati per affiancare o sostituire l'*Orlan-10*.

---

[35] *"Dronefall" reaches a new level - Dozens of Shaheds downed by Ukrainian Army*, Savelife.in Ua, 1/06/2025. https://savelife.in.ua/en/materials/news-en/dronefall-reaches-a-new-level-dozens-of-en/.

[36] N. Jhanjhi e al., *The Rise of GPS Spoofing Attacks on Drones in the Russia-Ukraine War*, TechRxiv, 09/07/2025. https://www.techrxiv.org/doi/full/10.36227/techrxiv.175203757.71749390/v1.

[37] *Unmanned systems forces "hunted down" a rare enemy drone "Forpost-R" over the Kursk region*, UNN, 27/07/2026. https://unn.ua/en/news/unmanned-systems-forces-hunted-down-a-rare-enemy-drone-forpost-r-over-the-kursk-region.

[38] *Russian "Inokhodets" drone destroyed in occupied Crimea*, UA.News, 04/04/2026. https://ua.news/en/war-vs-rf/v-okupovanomu-krimu-znishcheno-rosiiskii-bezpilotnik-inokhodets.

[39] V. Litnarovych, *Russia's Rare Merlin-VR Recon Drone Eliminated by Ukrainian FPV Crews*, Video, United 24, 16/01/2025. https://united24media.com/latest-news/russias-rare-merlin-vr-recon-drone-eliminated-by-ukrainian-fpv-crews-video-5144.

[40] V. Kushnikov, *For the first time, Ukrainian paratroopers have shot down a Russian Horizon S-100 drone*, Militarnyi, 20/04/2022. https://militarnyi.com/en/news/for-the-first-time-ukrainian-paratroopers-have-shot-down-a-russian-horizon-s-100-drone/.

[41] V. Kushnikov, *Ukrainian Ground Forces announced the destruction of almost 60 reconnaissance UAVs in a week*, Militarnyi, 21/07/2024. https://militarnyi.com/en/news/ukrainian-ground-forces-announced-the-destruction-of-almost-60-reconnaissance-uavs-in-a-week/.

[42] V. Kushnikov, *Ukrainian air defense shot down an enemy drone "Kartograf," which has a camera with 12 lenses*, Militarnyi, 02/09/2022. https://militarnyi.com/en/news/ukrainian-air-defense-shot-down-an-enemy-drone-kartograf-which-has-a-camera-with-12-lenses/.

- *Forpost.* Una versione prodotta su licenza russa dell'israeliano *IAI Searcher*. È un drone tattico a lungo raggio utilizzato principalmente per la sorveglianza persistente e la designazione laser dei bersagli per le bombe guidate.

- *Orion (Inokhodets)/Orion Pacer*. Un UAV di classe MALE (*Medium-Altitude Long-Endurance*), equivalente operativo del *Predator* americano o del *Bayraktar TB2* turco. Viene impiegato sia per ruoli di ISR, sia per attacchi di precisione.

- *Merlin (Merlin-VR)*. Un drone da ricognizione ad alta quota e ad alto valore tecnologico, progettato per operare in contesti di forte disturbo elettronico e sorvegliare aree sensibili.

- *Horizont Air S-100*. Un UAV ad ala rotante (elicottero senza pilota) basato sul design dell'austriaco *Schiebel Camcopter S-100*, impiegato soprattutto per la sorveglianza marittima e costiera.

- *Supercam (S100, S350)*. Una famiglia di droni ad ala fissa ad alta efficienza. Il *Supercam S100* e i modelli successivi sono ampiamente utilizzati per la fotografia aerea ad alta risoluzione, la sorveglianza video in tempo reale e la geolocalizzazione rapida dei bersagli.

- *Kartograf*. Un drone da ricognizione russo classificato, utilizzato principalmente dall'FSB)[43].

Qualche parola sull'*Orlan-30* versione migliorata dell'*Orlan-10*. Sviluppato nel 2020, ha iniziato a essere prodotto in grandi quantità nel 2023. L'*Orlan-30* può operare a una distanza di 300 km, contro i 120 km dell'*Orlan-10*. L'*Orlan-30* può anche trasportare un carico utile maggiore ed è dotato di designazione laser, utile sia per l'individuazione di obiettivi per l'artiglieria, sia per l'aviazione dotata di missili aria-terra e bombe laser guidate; questa nuova variante inoltre può fornire le coordinate esatte degli obiettivi stessi attraverso i sistemi di navigazione spaziale *Glonass*[44].

Per migliorare la qualità del proprio *targeting*, a un certo punto i russi hanno ritenuto che fosse opportuno imparare dagli ucraini, dunque osservare ed ap-

[43] *US company Iridium provides navigation for FSB drones during combat*, Ukrainska Pravda, 28/09/2023. https://www.pravda.com.ua/eng/news/2023/09/28/7421863/.
[44] *How Is Russia Using Orlan-30 UAVs to Enhance Their Artillery*, Defence Central, 27/03/2024, https://www.youtube.com/watch?v=ivlHtUw2-J8.

prendere dalle modalità adottate dagli ucraini per le attività di ricognizione con i droni nell'individuazione dei bersagli e nella condotta del fuoco. In particolare, si sono concentrati sulle procedure dell'organizzazione non governativa ucraina *Aerorozvidka* e, in questa fase di apprendimento, hanno visionato numerosi filmati didattici sui droni ucraini disponibili su *Telegram* e su *YouTube*.

Annunciata il 16 dicembre 2024 dal Ministro della Difesa Andrei Belousov[45], nel novembre 2025[46] il Cremlino ha ufficialmente reso nota l'istituzione di una nuova branca delle forze armate russe, specializzata nella guerra con veicoli a pilotaggio remoto aerei, terrestri e marittimi: le Forze dei sistemi senza pilota (VBS). Questa nuova branca comprende diversi reparti destinati a operare con i droni seguendo delle procedure standardizzate, ma non autonomamente, bensì in coordinamento con altre unità militari, nel quadro di una pianificazione unitaria. L'istituzione delle VBS è un riconoscimento formale da parte delle forze armate russe della centralità della guerra condotta con droni e sistemi autonomi nei conflitti contemporanei, così come degli sforzi di Mosca per riorganizzare l'addestramento, la struttura delle forze, lo sviluppo e la logistica relativi a questa tipologia di combattimento[47]. La Russia ha iniziato a creare unità militari di droni separate già a fine gennaio 2025[48], con il primo reggimento di droni presentato alla parata del Giorno della Vittoria di Mosca del 2025[49]. Il 12 novembre 2025 il colonnello Sergey Ishtuganov, vice capo delle VBS, ha dichiarato che la branca ha terminato la sua formazione ed è pienamente operativa[50]. Il primo aspetto che emerge con im-

---

[45] R. N. McDermott, *Russia's New Unmanned Systems Forces and the Strategic Role of DKO Weapons*, The Saratoga Foundation, 20/06/2025. https://www.saratoga-foundation.org/p/russias-new-unmanned-systems-forces.

[46] *Russia establishes Unmanned Systems Forces*, Tass, 12/11/2025. https://tass.com/defense/2042371.

[47] J. Hardie, *Russia announces plans to form Unmanned Systems Forces*, FDD's Long War Journal, 20/12/2024. https://www.longwarjournal.org/archives/2024/12/russia-announces-plans-to-form-unmanned-systems-forces.php.

[48] I. Diakonov, *Russia creates separate regiments of unmanned systems to strengthen its army – ISW,* Ukrainska Pravda, 29/01/2025. https://www.pravda.com.ua/eng/news/2025/01/29/7495735/.

[49] D. Shumlianskyi, *"Russians Completes Formation of First UAV regiment, Presents it at May 9 Parade"*, Militarnyi, 11/05/2025. https://militarnyi.com/en/news/russians-completes-formation-of-first-uav-regiment-presents-it-at-may-9-parade/.

[50] *The war of no man: Russia creates drone army 'Unmanned Systems Forces' to rival Ukraine*, The Week Magazine, 13/11/2025. https://www.theweek.in/news/defence/2025/11/13/the-war-of-no-man-russia-creates-drone-army-unmanned-systems-forces-to-rival-ukraine.html#google_vignette.

mediatezza è che la nuova branca delle forze armate russe rispecchia quella simile creata dall'Ucraina l'anno precedente, utilizzandone persino lo stesso nome. L'esercito ucraino ha dimostrato di essere un pioniere nella tecnologia dei droni, impiegando metodi innovativi per ridurre il vantaggio materiale e numerico della Russia. I droni aerei sono stati utilizzati, ad esempio, per speronare elicotteri russi o sganciare metallo fuso su posizioni terrestri, mentre i droni navali sono stati un elemento chiave nel rovesciare il predominio della Russia nel Mar Nero[51]. In ogni caso, la reazione di Kiev alla creazione delle VBS russe ha evidenziato una notevole preoccupazione[52]. Sempre Ishtuganov ha dichiarato che oltre all'impiego sul campo di battaglia, le VBS eseguono test di combattimento sia con i droni che con i sistemi di guerra elettronica[53]; quest'ultima rappresenta la principale minaccia per i droni e gli studi per migliorarne l'efficacia per le proprie unità e i sistemi di difesa nei confronti delle capacità nemiche si susseguono ininterrottamente su entrambi i fronti.

L'approvvigionamento delle componenti per l'assemblaggio dei droni è un aspetto importante per il nuovo ramo militare e va sottolineato che la Russia sta ricevendo un notevole supporto da Pechino, producendo droni interamente composti da componenti cinesi[54]. Anche l'aspetto delle risorse umane da destinare alle VBS ha una grande rilevanza e, non a caso verrebbero selezionati veterani operatori di droni in possesso di eccellenti trascorsi di combattimento, tuttavia da non impiegare più nelle fasi di assalto condotte dalle unità cui sono assegnati. Allo stato attuale questo obiettivo non è stato ancora raggiunto. Le VBS sarebbero responsabili dell'addestramento centralizzato e delle forniture per gli operatori di droni, così come dell'analisi della condotta del combattimento e della ricerca e sviluppo di nuovi sistemi, come detto, le sue unità sarebbero subordinate a varie formazioni delle forze armate. A novembre 2025, la dimensione della branca era stimata intorno ai 10.000-20.000, che vanno dagli specialisti nel lancio di droni *Shahed* a lungo

[51] Y. Taradiuk, *Russia establishes Unmanned Systems Forces, Ukraine says it's just "copying our successful approaches"*, The Kyiv Independent, 12/11/2025. https://kyivindependent.com/russia-establishes-its-unmanned-systems-forces-copying-ukraines-successful-approaches/.
[52] H. Altman, *Russia Creates New Military Branch Dedicated To Drone Warfare*, The War Zone, 13/11/2025. https://www.twz.com/news-features/russia-creates-new-military-branch-dedicated-to-drone-warfare.
[53] Ibid.
[54] N. Cristadoro, *La cooperazione russo-iraniana per la produzione di droni e il contributo della Cina*, Istituto Gino Germani, Settembre 2025.

raggio ai piloti di droni che attaccano il nemico con droni *kamikaze First Person View* (FPV)[55] in prima linea[56]. Le unità che attualmente fa no parte delle VBS sono le seguenti:

- Il Centro per le tecnologie avanzate senza pilota *Rubicon*;

- 7° Reggimento di Ricognizione-Attacco Separato di Sistemi Senza Pilota;

- 75° Reggimento Separato di Sistemi Senza Pilota;

- 77° Reggimento Separato di Sistemi Senza Pilota;

- Brigata separata di velivoli senza pilota *"GROM "Kaskad""*

- Centro per scopi speciali *Bars-Sarmat* (precedentemente Distaccamento volontario *Bars-Sarmat*).

Soffermiamoci sull'unità che può essere considerata il "traino" di tutto il progetto delle VBS: il Centro per le tecnologie avanzate senza pilota *Rubicon*, istituito nell'agosto 2024, su direttiva del Ministro della Difesa russo Andrey Belousov. L'obiettivo principale del centro era formare istruttori altamente qualificati nel campo dell'aviazione senza pilota, allo scopo di trasferire la loro competenza al personale in nuove unità militari. Inoltre, il Centro opera per preparare gli operatori di UAV da impiegare in operazioni di combattimento, sia individualmente che come parte di *team*[57]. Il centro sviluppa e sperimenta anche sistemi avanzati di droni e la loro implementazione, conduce ricerche nel campo dell'intelligenza artificiale ed esplora come può essere utilizzata nei sistemi robotici[58]. Al mese di novembre 2025 si stima che l'unità conti circa 5.000 uomini[59]. La sede di *Rubicon* sarebbe all'interno delle sale espositive del Patriot Park nell'*oblast'* di Mosca. Il comandante attuale è Sergei Zbukarev, che ha sostituito il colonnello Sergei Budnikov

---

[55] I FPV sono droni pilotati tramite un visore che trasmette in tempo reale all'operatore le immagini della telecamera di bordo.

[56] I. Volzhsky, S. Kanevskaya, *Коррупционный полк (Reggimento della corruzione)*, Novaya Gazeta Europa, 15/11/2025. https://novayagazeta.eu/articles/2025/11/15/korruptsionnyi-polk.

[57] *В Минобороны создали центр перспективных беспилотных технологий "Рубикон" (Il Ministero della Difesa ha istituito il Centro per le tecnologie avanzate senza pilota Rubicon)*, Tass, 11/10/2024. https://tass.ru/armiya-i-opk/22099195.

[58] Ibid.

[59] C. Clover, F. Deprez, *The elite Russian unit hunting Ukraine's drone warriors*, The Financial Times, 13/11/2025. https://www.ft.com/content/05ca82cc-2613-4144-a4e0-fd595246df8e.

nel corso del 2026. Le reclute vengono selezionate a Mosca prima di essere assegnate alle rispettive squadre per l'addestramento[60]. L'unità è stata inizialmente schierata nell'*oblast'* di Kursk, dove ha svolto un ruolo significativo nell'interruzione delle rotte di rifornimento ucraine, aiutando le forze russe a respingere il nemico fuori dall'area. *Rubicon* può avvalersi anche di elevate capacità di *sigint*, che le consentirebbero di localizzare e colpire i droni ucraini e i loro operatori, arrivando a distruggere in alcune aree fino al 70% delle posizioni UAV. Dal gennaio 2025, *Rubicon* ha operato nelle direzioni di Belgorod, Kypiansk, Pokrovsk, Kharkiv, Vuhledar e nel Donetsk meridionale. Dal maggio 2025, ha operato principalmente nell'oblast' di Donetsk, supportando l'offensiva russa[61]. Infine, le tipologie dei droni impiegate dall'unità:

- munizioni circuitanti *Lancet* e *Kub*;

- droni FPV normali e in fibra ottica, in particolare *VT-40* e *KVN*;

- droni da ricognizione *Orlan, SuperCam, Voron*;

- veicoli di superficie senza pilota *Shkval* (da non confondere con il siluro a supercavitazione di epoca sovietica *VA-111 Shkval*).

La componente di combattimento del distaccamento conta 245 effettivi. Il gruppo di droni FPV è composto da 106 effettivi ed è guidato dal comandante di gruppo e dal vicecomandante per le operazioni. È formato da 4 plotoni FPV, ciascuno guidato da un ufficiale. Tre di questi plotoni hanno otto squadre con tre effettivi ciascuna, mentre il quarto plotone ha sei squadre con quattro effettivi ciascuna. Ogni squadra è guidata da un sergente. È presente anche un gruppo di droni FPV ad ala fissa di 72 effettivi. Questo gruppo è composto da due plotoni con otto squadre ciascuno. Ogni squadra ha quattro effettivi. Il gruppo di ricognizione e attacco è composto da 69 effettivi, con quattro squadre di droni *S-350NJ Supercam* e quattro squadre di droni *Zala*. Ciascuna di queste squadre ha sette effettivi, tra cui piloti sia per droni ISR, sia per droni con munizioni a guida autonoma (tipicamente, una variante del *Lancet*) ed è composta da un ufficiale e due sottufficiali. Il gruppo di ricognizione aerea è composto da 35 persone, con due squadre di droni *Orlan-*

[60] E. Legalov, S. Dobrynin, M. Krutov, *Тайна "Рубикона". БПЛА-спецназ в парке "Патриот" (Il mistero di Rubicon: droni delle forze speciali al Patriot Park)*, Radio Svoboda, 17/09/2025. https://www.svoboda.org/a/tayna-rubikona-bpla-spetsnaz-v-parke-patriot-/33531165.html.

[61] ttps://lostarmour.info/tags/rubicon.

10 e sei squadre aggiuntive di droni per la sorveglianza e l'intelligence. Le squadre di *Orlan-10* sono comandate da ufficiali e sono composte da cinque persone, mentre le squadre ISR regolari sono composte da tre persone e sono comandate da sergenti. Il distaccamento dispone di un gruppo anti-droni di 29 persone, con due squadre radar, due squadre di guerra elettronica e due squadre di ricognizione radioelettronica. Sono, inoltre, presenti un plotone comunicazioni con 15 persone, un gruppo armamenti, un gruppo di manutenzione, un plotone di supporto e un gruppo di evacuazione medica.

Sotto il profilo dell'intelligence, poi, corre l'obbligo di menzionare l'OBTF *Kaskad* (Formazione Tattica Operativa da Combattimento *Kaskad*), un'unità paramilitare affiliata alle forze russe e separatiste della Repubblica Popolare di Donetsk (DNR). Trasformata in *Brigata Kaskad* nell'ottobre del 2023, successivamente è stata inquadrata nelle VBS. Si tratta di un'unità specializzata in missioni di ricognizione e ricognizione armata con droni da ricognizione e ricognizione-attacco, come i *Lancet*. La denominazione si ispira ai reparti di ricognizione e antiterrorismo *Kaskad* del KGB sovietico attivi durante la guerra in Afghanistan negli anni Ottanta. Una curiosità: l'unità è nota per accogliere nei suoi ranghi, oltre a volontari e specialisti, diversi politici di spicco russi, parlamentari della Duma di Stato (membri del partito Russia Unita) e figure di alto profilo pubblico che desiderano ottenere lo *status* di "partecipante all'operazione militare speciale", guidate da Dmitij Sablin:

> *"Il 'Kaskad' annovera tra le sue file numerosi politici e alti funzionari. Oltre a Sablin, cinque membri della Duma di Stato russa si sono uniti volontariamente al 'Kaskad': Evgenij Pervyšov, Oleg Golikov, Sergej Sokol, Dmitrij Chubezov e Oleg Kolesnikov. Vi figurano inoltre membri delle assemblee legislative delle regioni russe, due 'parlamentari' della 'Repubblica Popolare di Donetsk' e molti funzionari pubblici*[62]*."*

All'inizio di novembre 2022, l'unità *Kaskad* ha impiegato efficacemente i propri droni per l'aggiustamento del tiro di artiglieria a Pavlovka, vicino a Vuhledar. Nelle parole del comandante dell'unità, noto con il *nom de guerre* "Bely", il supporto fornito agli attacchi della 155ª e della 40ª Brigata di Fanteria di Marina delle Guardie, avrebbe contribuito in modo significativo alla conquista di Vuhledar da parte russa:

---

[62] V. Samar, V. Marchenko, *«GROM Kaskad». Who Fights against Ukraine in the First Russian Drone Brigade*, Center of Journalistic Investigations, 18/05/2024. https://investigator.org.ua/en/investigations/266753/.

"Stiamo indubbiamente combattendo contro un nemico astuto, di cui sarebbe un crimine sottovalutare le manovre tattiche. Nonostante ciò, il fuoco di controbatteria ben organizzato, unito alla ricognizione con droni e alle operazioni coordinate tra la Forza di intervento rapido Kaskad e i soldati della 155ª e della 40ª Brigata della Fanteria di marina, non ha lasciato al nemico alcuna possibilità di occupare ulteriormente Pavlovka[63]."

Nello specifico dell'attività di ricognizione finalizzata al targeting i droni *Orion* si sono rivelati efficaci nell'individuazione e nell'osservazione del tiro contro i veicoli marini senza equipaggio (USV) ucraini che operano nel Mar Nero, vicino alla Crimea.

"Il principale mezzo per contrastare i droni di superficie della Marina rimane la mitragliatrice montata su un elicottero dell'Aviazione Navale, che funge da postazione di tiro mobile. A giudicare dai numerosi video, l'elicottero deve scendere di quota per consentire al mitragliere di ingaggiare con successo un bersaglio in rapida manovra. Questo è piuttosto pericoloso, poiché il nemico ha iniziato a sperimentare il montaggio di missili antiaerei su veicoli a pilotaggio remoto. Prima o poi, un nemico astuto e spietato imparerà a intercettare gli elicotteri russi che si dirigono verso di loro. La comparsa di droni tipo Orion nel Mar Nero fa sperare che venga sviluppato un metodo altrettanto efficace, ma più sicuro, per distruggere i "branchi di lupi" delle navi incendiarie ucraine[64]."

La Marina russa, dunque, sembrerebbe aver appreso la lezione secondo cui i droni da ricognizione e attacco di medie dimensioni sono i loro strumenti migliori per monitorare le aree costiere vicino alla Crimea.

Nel 2023, i soldati ucraini hanno constatato l'improvvisa comparsa di un gran numero di droni russi, in particolare di droni da sorveglianza più piccoli e facilmente reperibili sul mercato. Allo stesso tempo, si è ridotto notevolmente il tempo di reazione e attacco delle munizioni circuitanti. Tale situazione ha destato una notevole sorpresa nelle forze ucraine, abituate a un ritardo fino a mezz'ora nelle missioni di fuoco dell'Aeronautica militare russa in seguito all'individuazione da parte dei droni. L'Aeronautica militare russa ha iniziato a utilizzare costellazioni ridondanti di droni ad alta quota, abbinati a droni da ricognizione di dimensioni minori. Questi droni, concepiti per l'osservazione, possono segnalare i bersagli ai droni d'attacco *Lancet* o all'Ae-

[63] https://t.me/s/obtf_kaskad/588.

[64] S. Marzhetsky, *Как БПЛА "Орион" может стать эффективным охотником на морские дроны (Come il drone Orion potrebbe diventare un efficace cacciatore di droni marittimi)*, AviaPort, 06/09/2024. https://www.aviaport.ru/news/kak-bpla-orion-mozhet-stat-effektivnym-okhotnikom-na-morskie-drony/.

ronautica militare russa[65], incrementando le capacità relative ai tempi di reazione e attacco e alla capacità raccolta di dati informativi.

In considerazione delle distanze tattiche così ravvicinate, i droni di entrambe le parti hanno trasformato il campo di battaglia in un ambiente praticamente in cui è impossibile nascondersi. Alcuni analisti definiscono questo fenomeno la "democratizzazione" del campo di battaglia, poiché entrambe le parti, fino alle unità più piccole, possono raccogliere informazioni utili praticamente su qualsiasi dettaglio del campo di battaglia. Rimane significativo quanto accaduto il 3 novembre 2023, quando le forze armate russe hanno impiegato un drone sopra Zarichne, nell'*oblast'* di Zaporizhzhia, a 35 km a nord della linea'di contatto e di combattimento (LCC). L'obiettivo era un raduno di artiglieri della 128ª Brigata d'Assalto da Montagna ucraina "Transcarpazia" riuniti per una cerimonia di premiazione in occasione della Giornata dell'Artiglieria. Il drone ha confermato l'obiettivo con sufficiente precisione e il risultato è stato un attacco con un missile balistico *Iskander-M*[66]. Ventotto militari sono rimasti uccisi e oltre 50 feriti. Tra i caduti figurano anche diversi ufficiali di rango elevato. Gli attacchi condotti in precedenza non avevavno mai avuto un tale livello di precisione. Questo aspetto merita alcune considerazioni. Zarichne è un villaggio situato lungo un'importante via di comunicazione, quindi si trova nella zona di attenzione della ricognizione aerea nemica. Per lungo tempo, un drone nemico ha osservato come le auto fossero concentrate nel centro del villaggio. La responsabilità della scelta del luogo e dell'ora della premiazione nel villaggio, chiaramente visibile dai droni, è stata affidata al comandante della brigata e ad altri funzionari che, insieme a lui, hanno preso le decisioni. La questione è stabilire a chi risalga la responsabilità della mancata segnalazione del volo di un drone russo. Il drone ha volato in profondità nelle retrovie a un'altitudine considerevole e un allarme radar della difesa aerea o dell'intelligence elettronica avrebbe dovuto segnalare la sua traiettoria. O non c'erano i mezzi per farlo, o non c'è stato alcun allarme da parte delle forze di difesa aerea e della guerra elettronica. L'ipotesi più grave è che l'allarme fosse stato diramato e il comando di brigata non ne abbia tenuto conto[67].

---

[65] *Russia ramps up drone production, reshaping the war in Ukraine*, You Tube, 20/08/2025. https://www.youtube.com/watch?v=sjT8GhPGBMU&t=1

[66] D.L. Sterne, *Russian missile strikes brigade in Zaporizhzhia, Ukraine says*, The Washington Post, 05/11/2023. https://www.washingtonpost.com/world/2023/11/05/russia-ukraine-128th-mountain-brigade-strike/.

[67] Y. Butusov, *Reasons and responsibility for tragedy in 128th Mountain Assault Brigade*, Censor.net, 05/11/2023.https://censor.net/en/resonance/3453741/reasons_and_responsibility_for_tragedy_in_128th_mountain_assault_brigade.

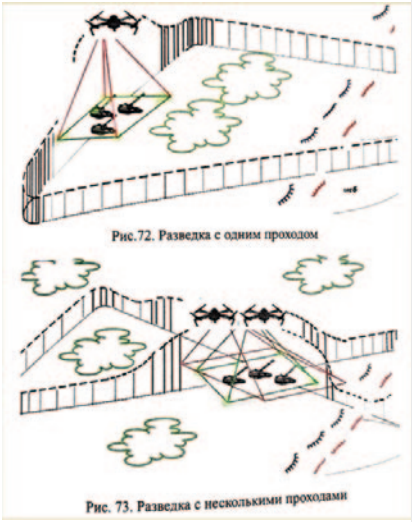


Illustrazione tratta dal manuale russo del 2022 per operatori di droni[68], che mostra gli schemi di volo per la ricognizione con droni. Le diciture indicano rispettivamente "Ricognizione con un passaggio" e "Ricognizione con più passaggi".

Oltre al miglioramento delle TTPs nell'utilizzo dei droni per scopi di intelligence, la Russia si impegna a migliorare tecnicamente i droni, aumentandone così l'utilità come strumenti di raccolta informazioni. Le forze armate russe spesso hanno modificato i droni a livello di singolo velivolo per aumentarne le capacità. Nella primavera del 2022, un militare ucraino ha mostrato un *Orlan-10* abbattuto, rimasto quasi intatto, su cui era stata montata una fotocamera Canon EOS 750D per utilizzo civile come parte dei suoi sensori. Aveva anche un tappo di plastica comune per una bottiglia d'acqua nel sistema di alimentazione[69]. In altre situazioni, le unità UAV hanno modificato i droni commerciali, regolandone le frequenze operative per contrastare le attività di guerra elettronica ucraine. Questo fenomeno evidenzia la continua

[68] *Corso di artiglieria per operatori di sistemi aerei a pilotaggio remoto (UAS)*, San Pietroburgo, 2022, p. 175.
[69] B. Bostock, *Video shows Ukrainian soldier taking apart a Russian drone and discovering its components include a plastic bottle top for a fuel cap*, Business Insider, 11/04/2022. https://www.businessinsider.com/video-ukraine-soldier-disassembles-russian-drone-reveals-unsopisticated-handiwork-2022-4.

evoluzione tattica e tecnologica nel conflitto in Ucraina, dove lo spettro elettromagnetico è diventato un vero e proprio campo di battaglia. L'adattamento delle frequenze dei droni commerciali (come i droni FPV o i modelli DJI modificati) serve a eludere i sistemi di disturbo (*jamming*) ucraini[70]. Alcune unità di artiglieria delle Forze Armate Russe sui droni da ricognizione e sorveglianza hanno installato delle termocamere. Le termocamere consentono agli operatori di osservare e raccogliere informazioni di imint con chiarezza, anche attraverso elementi che celano alla vista gli obiettivi, come la fitta vegetazione o le reti mimetiche.



Immagini tratte dal video che mostra l'Orlan-10 abbattuto, equipaggiato con la fotocamera Canon EOS 750D[71].

Al momento dell'elaborazione di questo *dossier*, la novità del Cremlino in ambito di droni per l'impiego operativo è rappresentata dal *Molniya-13*:

[70] I. Levytska, *A shield against FPV drones: is Ukraine's electronic warfare capability matching drone advancements?,* Ukrainska Pravda, 08/08/2025. https://www.pravda.com.ua/eng/articles/2025/08/08/7525279/.

[71] https://gagadget.com/en/116417-whats-inside-orlan-10-a-canon-consumer-camera-and-a-plastic-bottle-were-found-in-a-drone-shot-down-by-the-armed-forces-of/.

"La Russia ha presentato il Molniya-13, un nuovo drone da combattimento di classe pesante progettato per offrire maggiore potenza di fuoco, capacità di sopravvivenza e flessibilità operativa. Evoluzione della precedente piattaforma Molniya-2, il nuovo drone è dotato di una fusoliera più grande, quattro motori elettrici, una capacità di carico utile di 13 chilogrammi e un raggio d'azione fino a 50 chilometri. Secondo gli sviluppatori russi, il design perfezionato garantisce una maggiore stabilità in condizioni meteorologiche avverse e riduce il rischio di fallimento della missione in caso di danni o perdita di un motore. Il Molniya-13 è concepito per molteplici ruoli di combattimento, tra cui il monitoraggio degli obiettivi, la ricognizione sul campo di battaglia, le missioni di trasporto e gli attacchi aerei contro postazioni fortificate e veicoli leggermente corazzati. Grazie a una velocità di crociera di 120 chilometri orari e a una traccia radar relativamente ridotta, il drone è progettato per raggiungere rapidamente gli obiettivi rimanendo al contempo difficile da individuare[72]."

Rimanendo nell'ambito della *imint*, i media ucraini e inchieste internazionali, hanno evidenziato un ricorrente schema di acquisto di immagini satellitari commerciali ad alta risoluzione da parte della Russia tramite società di copertura[73]. Queste immagini, spesso ordinate poco prima di attacchi missilistici mirati sulle infrastrutture ucraine, evidenzierebbero una carenza qualitativa e quantitativa nella flotta di satelliti spia di Mosca. Nonostante la Russia disponga di una propria rete di satelliti militari, infatti, il numero di unità operative in grado di fornire immagini ottiche ad alta risoluzione in tempo reale è fortemente insufficiente per coprire le esigenze di un conflitto su vasta scala. Molti dei satelliti russi soffrono di obsolescenza tecnologica o di problemi di longevità dei componenti. Le costellazioni commerciali (come quelle gestite da aziende occidentali o da *partner* internazionali) dispongono di centinaia di piccoli satelliti che orbitano intorno alla Terra, garantendo una frequenza di aggiornamento della stessa area anche più volte al giorno. La Russia non ha una costellazione a bassa orbita altrettanto densa, il che crea "buchi temporali" significativi tra un passaggio satellitare e l'altro:

"La dottrina militare russa, come osserva Connell, prevede che le fasi iniziali di un conflitto includano un'offensiva concentrata volta a compromettere la capacità del nemico di osservare, comunicare e coordinarsi. L'attacco AcidRain contro Viasat e la campagna

---

[72] *Russia's new killer drone on cam; more power, heavier payload, longer reach | Molniya-13*, 21/06/2026. https://www.facebook.com/toiworldnews/videos/russias-new-killer-drone-on-cam-more-power-heavier-payload-longer-reach-molniya-/1031763069188870/.

[73] G. Wood, *A Suspicious Pattern Alarming the Ukrainian Military,* The Atlantic, 18/03/2024. https://www.theatlantic.com/international/archive/2024/03/american-satellites-russia-ukraine-war/677775/.

di spoofing del GPS condotta sull'Ucraina prima dell'invasione sono state espressioni dirette di tale dottrina. Ciò che la dottrina russa non aveva previsto era la capacità dell'Ucraina di colmare rapidamente la propria lacuna nel settore satellitare. All'inizio del conflitto, l'Ucraina non disponeva di infrastrutture spaziali proprie, eppure è riuscita a superare questa vulnerabilità grazie al rapido sostegno di fornitori commerciali occidentali, come SpaceX. In pratica, ciò ha significato che l'«attacco informativo» su cui la Russia contava per accecare l'Ucraina non si è mai concretizzato appieno, poiché i servizi spaziali del settore privato sono intervenuti mantenendo l'Ucraina connessa. Del resto, l'uso stesso che la Russia ha fatto dell'intelligence spaziale in Ucraina dimostra a cosa possano portare anni di finanziamenti limitati e scarsa integrazione dei sistemi. Anche quando i satelliti russi acquisivano immagini utili, spesso i militari non riuscivano a trasmettere tali informazioni alle unità in prima linea con la rapidità necessaria per sfruttarle. I dati erano disponibili, ma i canali per trasferirli dagli analisti ai soldati risultavano lenti, frammentati o semplicemente inadeguati ai ritmi del combattimento moderno. L'analisi della RAND sulle lezioni apprese in ambito spaziale dal conflitto in Ucraina conferma tale valutazione, evidenziando come le forze spaziali russe fossero ancora in fase di sviluppo all'inizio delle ostilità e come la portata delle operazioni in Ucraina abbia superato la loro capacità operativa progettuale, rendendole incapaci di gestire le dinamiche in gioco e di fornire informazioni cruciali sul campo di battaglia. Si crea così un paradosso analitico: la Russia possiede credibili capacità di contrasto spaziale, strumenti per attacchi informatici reversibili contro i terminali di terra e piattaforme per il disturbo (jamming) del segnale GPS su vasta scala, eppure la sua capacità di sfruttare le proprie risorse spaziali per ottenere un vantaggio tattico è stata costantemente superata dall'architettura ucraina, potenziata da soluzioni commerciali[74]."

Uno dei fallimenti evidenti dell'intelligence satellitare è stata l'incapacità di rilevare tempestivamente un volume significativo di movimenti ferroviari strategici da parte delle forze ucraine, che nel marzo 2022 raggiungevano i tre o quattro convogli al giorno[75].

Le immagini ottiche *standard*, inoltre, non possono penetrare la fitta copertura nuvolosa, frequente in Ucraina. Le aziende commerciali offrono sempre più spesso tecnologie *Synthetic Aperture Radar* (SAR) capaci di vedere di notte e attraverso le nuvole. La carenza di asset russi avanzati in questo specifico campo costringe Mosca a cercare dati radar altrove. Ma non solo. Inchieste sul campo hanno rivelato che persino gruppi russi di forze irregolari

[74] N. Buzhala, *Assessing Russian Network Warfare Through the Lens of the Ukraine Conflict,* Small Wars Journal. 12/05/2026. https://smallwarsjournal.com/2026/05/12/assessing-russian-network-warfare/.

[75] https://guerillamap.com/russian-spaceborne-imint-imagery-intelligence-capabilities/.

[76] Bernat P., C.A. Kozera, *The Wagner Group Use of Chinese Space Intelligence*, Irregular Warfare Initiative, 03/12/2024. https://www.irregularwarfare.org/the-wagner-groups-use-of-chinese-space-intelligence/.

(come il *Gruppo Wagner* durante la battaglia di Bakhmut) hanno acquistato autonomamente immagini da aziende terze (in quel caso cinesi)[76] a causa dei conflitti di coordinamento e della scarsa condivisione di informazioni da parte del Ministero della Difesa russo. Per eludere le sanzioni internazionali e i controlli interni delle aziende di geo-intelligence, l'intelligence russa sfrutta *network* di rivenditori e *broker* di dati situati in paesi terzi compiacenti o neutrali. L'acquisto di immagini d'archivio o la richiesta di nuovi scatti vengono camuffati come normali transazioni commerciali per scopi civili (agricoltura, logistica o edilizia), rendendo estremamente complessi il tracciamento e il blocco tempestivo da parte dei fornitori.

5. La ricognizione con il fuoco e il movimento

L'incapacità della Russia di sconfiggere l'Ucraina con interventi a fuoco precisi e con un approccio manovriero efficace nei primi giorni dell'invasione ha indotto le forze armate russe a tornare alla loro *comfort zone*, ricorrendo alle tradizionali operazioni di "massa contro manovra". La dottrina della "massa contro manovra" (in russo, *taktika*) è ben documentata nella storia militare russa. Allo stesso modo, il modello di generazione delle forze russo non si concentra su un buon addestramento, ma sull'accumulo di una forza massiccia (ovvero, sulla quantità piuttosto che sulla qualità). Con questa mentalità, non sorprende che la Russia sia disposta a subire perdite significative durante gli attacchi, al fine di scoprire punti di forza e di debolezza nelle difese ucraine. Data l'impossibilità di concentrare grandi masse di veicoli corazzati senza essere immediatamente tracciati dai droni e distrutti dall'artiglieria, l'esercito russo ha dovuto abbandonare i classici gruppi tattici pesanti a livello di battaglione, frammentando le forze in unità più piccole e flessibili. In tutto il Donbass, si sono riscontrati esempi di attacchi esplorativi o di disturbo che, almeno in parte, sembrano essere finalizzati a raccogliere informazioni sulle posizioni ucraine. Uno sviluppo simile è la creazione di "unità di ricognizione-assalto" nelle Forze Terrestri Russe. Le unità di ricognizione e assalto rappresentano un'evoluzione dottrinale e organizzativa introdotta nelle Forze Terrestri della Federazione Russa per adattarsi alla guerra di logoramento ad alta intensità:

> *"La guerra della Russia in Ucraina ha generato un bagaglio straordinario di esperienza di combattimento. La NATO si è comprensibilmente concentrata su ciò che Mosca ha appreso: nuovi approcci ai sistemi senza pilota, guerra elettronica, integrazione tra ri-*

cognizione e attacco, sopravvivenza dei posti comando, difesa aerea, operazioni d'assalto e logistica. ... Se il ciclo russo di ricognizione e ingaggio dipende da un ristretto gruppo di specialisti dotati di un'esperienza fuori dal comune, eliminarli potrebbe sortire un effetto operativo significativo. Se, invece, l'organizzazione ha già addestrato dei sostituti, standardizzato le procedure tecniche, sperimentato catene di comando alternative e predisposto la struttura di supporto necessaria per ripristinare il processo, il medesimo attacco potrebbe causare poco più di una temporanea interruzione delle attività[77]."

Nel settembre 2023, sono stati annunciati piani per la creazione di brigate da ricognizione-assalto in tutte le Armate Combinate (CAA) e nei corpi d'armata delle Forze Terrestri Russe[78]. Queste brigate sono progettate per assaltare le fortificazioni nemiche e condurre ricognizioni nelle immediate retrovie del nemico, non solo per raccogliere informazioni, ma per costringere il difensore a rispondere, rivelando così le proprie postazioni d'artiglieria e di difesa aerea (*hunter-seeker/reconnaissance-in-forc*e). La denominazione "assalto" è stata più spesso associata alle forze aviotrasportate russe (VDV) o alla fanteria di marina. Tuttavia, la combinazione "ricognizione-assalto" deriva probabilmente dalle compagnie da ricognizione-assalto della Compagnia Militare Privata (PMC) *Wagner*. La PMC *Wagner* ha iniziato a impiegare queste unità prima dell'operazione militare siriana nel Donbass e in Siria:

"I distaccamenti d'assalto (shturmovye otryady) costituivano le principali unità combattenti della Wagner, operando in Ucraina, Siria, Libia, Sudan, Mali e Repubblica Centrafricana. Tali unità si erano evolute dalle "compagnie di ricognizione e assalto" impiegate durante la fase iniziale del conflitto nel Donbass (2014-2015). Ciascuna di queste unità contava tra i 93 e i 103 uomini. Documenti relativi agli organici, risalenti a un periodo successivo, indicano che nel tempo la dimensione standard dell'unità arrivò a prevedere fino a 303 effettivi, sebbene i distaccamenti operassero spesso al di sotto del pieno organico[79]."

A differenza delle normali unità di fanteria motorizzata, la brigata o il distaccamento di ricognizione e assalto fonde organicamente elementi che un

---

[77] R.N. McDermott, *NATO is measuring Russian adaptation the wrong way*, Breaking Defense, 18/09/2026. https://breakingdefense.com/2026/09/nato-is-measuring-russian-adaptation-the-wrong-way/.

[78] https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_25-11/.

[79] R. Swit, B. Dalton, C. Rondeaux, *Paramilitary Paper Trails: Mapping the Wagner Group's Ties to Russia with Personnel Data*, New America, 02/10/2024. https://www.newamerica.org/insights/paramilitary-paper-trails/.

[80] N. Cristadoro, *Wagner & Co. Le compagnie di ventura russe ai tempi della guerra in Ucraina*, Il Maglio, 2022, p.p. 167-174.

tempo erano considerati autonomi o di supporto esterno. La seguente tabella riporta la struttura organica di un'unità da ricognizione-assalto.

Componente	Ruolo specifico all'interno dell'unità
Fanteria d'Assalto	Squadre d'assalto a piedi (spesso composte da personale specializzato o unità ex-detenuti/*Storm-Z*[80] per le ondate iniziali).
Gruppi Drone (UAV)	Integrati a livello di plotone/compagnia per la ricognizione aerea costante e il bombardamento tattico con droni FPV prima dell'avanzata della fanteria.
Supporto di Fuoco Organico	Sezioni di mortai leggeri, cannoni automatici, lanciagranate e lanciarazzi termobarici (come l'*RPO-A Shmel*) gestiti direttamente dal comandante d'assalto senza dover attendere l'autorizzazione di artiglierie d'armata.
Genio d'Assalto	Nuclei sminatori integrati per creare varchi immediati nei campi minati durante l'attacco.

Un esempio concreto è offerto dall'8ª Brigata da Ricognizione e Assalto, unità di volontari creata alla fine del 2024, inserita all'interno del Corpo Volontario Russo (*DobroKor*)[81]. La brigata raggruppa diversi noti reparti di volontari attivi nel Donbass e in altre zone operative, tra cui i distaccamenti *Rys, Tigr, ArBat e Krym*[82].

Di seguito, un estratto da un'intervista ad alcuni membri della del distaccamento *Rys*:

> *"Il plotone di droni dell'8ª brigata è un'unità "di servizio". "Siamo equipaggi specializzati in droni. Ovunque si trovi il nemico, noi siamo lì. Il nostro compito è decollare rapidamente, individuare e ingaggiare il nemico", afferma un comandante di plotone con il nome in codice "Yakut".Inoltre, gli operatori dei droni monitorano la rotazione del personale delle Forze Armate ucraine e fanno tutto il possibile per impedire al nemico di rimpiazzare il personale nelle loro posizioni e di rifornirsi di munizioni."Nel nostro plotone abbiamo diverse squadre: quelle specializzate in droni d'attacco, quelle di ricognizione e quelle di tecnici, ovvero coloro che riparano e si occupano della manutenzione dei droni", aggiunge Yakut[83]."*

[81] https://dobrocor.ru/nashi-otryady/8-ya-brigada/.
[82] Ibid.
[83] https://dobrocor.ru/ya-zdes-sebya-nashel-operatory-bpla-8-y-brigady-o-dele-kotoromu-teper-sluzhat/.



Personale dell'8ª Brigata da Ricognizione e Assalto[84]

6. Le intercettazioni attraverso la guerra elettronica (EW) e la *signal intelligence (sigint)* a livello tattico

È difficile reperire dati disponibili da fonti aperte sulle capacità *sigint* della Russia. A differenza dei servizi segreti ucraini che pubblicano decine, se non centinaia, di intercettazioni audio di comunicazioni russe sui *social media*, non vi è alcuno sforzo analogo da parte delle agenzie di sicurezza russe. Vediamo quali sono quelli disponibili su questa disciplina.

Dal 2008, la guerra elettronica è stata un'area di sviluppo fondamentale. La Russia ha costruito una delle forze di guerra elettronica più robuste al mondo, con un'ampia varietà di sistemi efficienti gestiti da personale altamente qualificato. Molti sistemi di guerra elettronica russi raccolgono e analizzano dati raccolti attraverso la sigint tattica per consentire un disturbo mirato ed efficace. Molti sistemi di guerra elettronica a radiofrequenza, come il *Borisoglebsk-2*, sono progettati per raccogliere e analizzare informazioni di ricognizione elettromagnetica. Questo permette alle apparecchiature per il *jamming* del *Bori-*

[84] https://dobrocor.ru/nashi-otryady/8-ya-brigada/.

soglebsk-2 di disturbare le frequenze appropriate per ottenere l'effetto desiderato. La Russia ha concentrato gli sforzi per automatizzare questa funzione nel maggior numero possibile di sistemi di guerra elettronica.

Prima dell'invasione, nel Donbass, probabilmente già nel 2014, il GRU aveva ideato un modo per installare malware sugli *smartphone* degli artiglieri ucraini. L'Ucraina aveva sviluppato una *app* per *smartphone* per velocizzare i calcoli dei dati di tiro per l'obice *D-30* di epoca sovietica. Gli apparati del GRU, venuti a conoscenza di tale soluzione, a loro volta hanno sviluppato una versione della *app* infetta da *malware*. La versione con il malware forniva informazioni generali sulla posizione dell'utente dello smartphone alle unità russe. Queste informazioni potevano essere utilizzate per indirizzare risorse come i droni a localizzare con precisione un'unità di artiglieria equipaggiata con i *D-30* per poi colpirla. Non è facile confermare quanti smartphone ucraini siano stati infettati e con quale successo le forze armate russe abbiano sfruttato questo malware: fonti aperte in un primo momento hanno riferito che l'Ucraina avesse perso oltre l'80% dei suoi obici *D-30* tra il 2014 e il 2015[85]; successivamente, tale percentuale è stata ridimensionata al 15-20%[86].

Durante la guerra del Donbass, nel periodo precedente all'invasione, le forze armate russe hanno utilizzato l'apparato di guerra elettronica *Leer-3* (*RB-341V*) per individuare i numeri di cellulare del personale militare ucraino a supporto di operazioni informative a livello tattico. L'apparato, operativo dal 2025[87], è costituito da una stazione di controllo montata su un camion *KamAZ 5350* e fino a tre droni *Orlan-10* equipaggiati con un carico utile in grado di raccogliere un gran numero di numeri di cellulare e informazioni sui fornitori di servizi. Il sistema *Leer-3* può utilizzare queste informazioni per falsificare numeri di cellulare e fornitori legittimi al fine di inviare al personale ucraino messaggi di testo demoralizzanti, nell'ambito di campagne di operazioni psicologiche; oppure per disturbare le comunicazioni cellulari GSM ucraine (fino a circa 2.000 abbonati) o per localizzare gruppi di utenti di telefonia mobile ucraini per at-

[85] Crowdstrike, *Use of Fancy bear Android Malware in Tracking of Ukrainian Field Artillery Units*, Dec 2016. https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.
[86] Ibid.
[87] B. Clark, *The Fall and Rise of Russian Electronic Warfare,* The Global Network, 30/07/2022. https://space4peace.org/the-fall-and-rise-of-russian-electronic-warfare/.

tacchi cinetici. Il sistema *Leer-3* è impiegato nelle cinque brigate separate di guerra elettronica, di cui riportiamo in tabella le unità che le inquadrano.

	Organizzazione delle Brigate EW Separate	
Unità	**Distretto Militare di Appartenenza**	**Sede Principale**
15ª Brigata EW	**Stato Maggiore Centrale** / ex-Distretto Occidentale	Stroitel (Oblast di Tambov)
16ª Brigata EW	**Distretto Militare di Mosca**	Kursk / Plavsk
17ª Brigata EW	**Distretto Militare Orientale**	Chabarovsk
18ª Brigata EW	**Distretto Militare Centrale**	Ekaterinburg
19ª Brigata EW	**Distretto Militare Meridionale**	Rassvet (Oblast di Rostov)

Una pregiata risorsa russa per la raccolta di dati attraverso la sigint, è la nave *Ivan Khurs*. La nave è stata apparentemente coinvolta in operazioni di sorveglianza marittima nel Mar Nero. L'aeronautica militare ucraina l'ha attaccata con USV nel maggio 2023, ma senza causare danni significativi. La *Ivan Khurs*, varata nel 2017, è una delle navi attrezzate per l'intelligence più moderne della marina militare russa, con un equipaggio di 120 persone. Il sistema di comando *Bridge 18280-23* integra il rilevamento radar e la navigazione e consente il rilevamento e il tracciamento di radar e comunicazioni avversarie di diversa potenza e lunghezza d'onda. Le sue missioni includono la raccolta di informazioni sui segnali, la sorveglianza dei sistemi di difesa missilistica statunitensi e occidentali, l'intercettazione radio, l'*elint* (identificazione e sistematizzazione delle sorgenti di radiazione elettromagnetica), la compilazione di profili elettromagnetici e acustici di navi di superficie e sottomarini, il controllo delle comunicazioni marittime e il monitoraggio della flotta avversaria durante manovre ed esercitazioni.

La 6ª Direzione del GRU controlla direttamente i reggimenti di intelligence elettronica e truppe speciali di trasmissione (dette *osnazovtsi*), che costituiscono le principali unità sigint schierabili sul campo per intercettazioni tattiche e operative[88]. Alcuni *blogger* militari russi hanno lamentato profonde carenze nella capacità di EW russe[89], sottolineando un declino tattico rispetto alle aspettative

[88] https://www.globalsecurity.org/intell/world/russia/gru-org.htm.

[89] R. Rommen, *Russian milbloggers slam Kremlin propagandists for ignoring huge Russian losses and 'blunders' in Ukraine*, Business Insider, 04/02/2024. https://www.businessinsider.com/russian-milbloggers-putin-kremlin-propagandists-war-ukraine-losses-2024-2.

dottrinali. Nonostante la Russia possieda sistemi EW complessi e teoricamente avanzati a livello strategico, l'applicazione sul campo di battaglia in Ucraina ha rivelato che la capacità di intercettazione, localizzazione e protezione delle comunicazioni a livello tattico è risultata in molti casi gravemente compromessa[90]. Mentre la dottrina russa prevede una ricognizione radio centralizzata e l'uso di apparati crittografati, la realtà del fronte ha costretto i soldati russi a ricorrere massicciamente a soluzioni civili e non protette (come le radio cinesi *Baofeng*[91] o i normali *smartphone*) per sopperire alla mancanza di forniture ufficiali. Questo scenario ha provocato due conseguenze letali evidenziate. In primo luogo la ricognizione radio russa fatica a mappare un campo di battaglia saturo di segnali disomogenei ed estremamente frammentati; al contrario, l'intelligence ucraina e occidentale intercetta con estrema facilità le comunicazioni russe, geolocalizzando istantaneamente i nodi di comando russi[92].

Sebbene la Russia abbia recentemente modificato la propria strategia puntando a colpire le infrastrutture fisiche di telecomunicazione e i *data center* [93], le sue attività operative di sigint continuano a essere ostacolate da problemi critici.

Innanzitutto, per un lungo periodo, le unità russe in prima linea hanno fatto ampio affidamento su terminali *Starlink* provenienti dal mercato nero – ottenuti tramite intermediari terzi – per supplire alle carenze delle proprie reti di comando e controllo frammentate[94]. Tuttavia, *SpaceX* ha introdotto rigide restrizioni di *geofencing*, bloccando l'accesso illecito russo alla rete[95]. L'improvvisa perdita di questo pilastro comunicativo ha gravemente compromesso il coordinamento russo al fronte, causando interruzioni nelle comunicazioni che hanno lasciato esposte le truppe avanzate e contribuito direttamente alle controffensive locali ucraine.

---

[90] S. Carvin, *Russia's Stalled Electronic Warfare Betrays Bad Planning,* Poor Training, Centre for International Government Innovation, 04/08/2022. https://www.cigionline.org/articles/russias-stalled-electronic-warfare-betrays-bad-planning-poor-training/.

[91] S. Cranny-Evans, T. Withington, *Russian Comms in Ukraine: A World of Hertz*, RUSI, 09/03/2022. https://www.rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz.

[92] *L'Ucraina punta sulla guerra elettronica tra intercettazioni radio e disturbo del segnale dei droni,* Euronews, 14/02/2024. https://www.youtube.com/watch?v=XAoeVmo0OMU.

[93] J. Lukiv, *Russia targeting 'ordinary life' with attacks on Ukraine's data centres, Zelensky says*, BBC, 25/09/2026. https://www.bbc.com/news/articles/c84gkwgk7d06o.

[94] J. Brodkin, *Report details how Russia obtains Starlink terminals for war in Ukraine*, Ars Technica, 09/04/2024. https://arstechnica.com/tech-policy/2024/04/report-details-how-russia-obtains-starlink-terminals-for-war-in-ukraine/.

[95] *SpaceX limits Starlink internet to keep Russia from using it to target drone strikes*, Scripp News, 03/02/2026. https://www.youtube.com/watch?v=U6iXuF8vTqU&t=47s.

Un altro fattore determinante riguarda gli attacchi dei droni ucraini contro *high value* targets russi, come nel caso del sistema *Artikul-S*, una rara e ingombrante piattaforma *sigint* russa a installazione fissa, utilizzata per intercettare le comunicazioni della difesa ucraina e mappare le reti di comando[96].

L'eliminazione di queste risorse pregiate, di fatto, "acceca" l'intelligence russa in settori chiave del fronte. Per contrastare i collegamenti ucraini, la Russia ha schierato sistemi EW e di intelligence più recenti, come il *Wolna Kupol Garant*, progettati per disturbare le frequenze *Starlink* direttamente nell'orbita terrestre bassa[97]. Sebbene questi moduli montati su rimorchio siano in grado di disturbare le comunicazioni in aree circoscritte, gli analisti della difesa segnalano una vulnerabilità evidente: l'ampia schiera di antenne attive genera una massiccia impronta elettromagnetica, rendendo le unità estremamente vulnerabili all'individuazione e all'acquisizione come bersaglio da parte dei sistemi ucraini di intelligence elettronica[98].

L'apparato di intelligence russo, poi, ha faticato ad adattarsi alla natura decentralizzata della moderna difesa ucraina. Le strategie russe di sigint e di guerra di rete sono spesso rallentate da una rigidità burocratica di tipo *top-down* (gerarchico-verticale). Di contro, l'Ucraina ha integrato architetture agili e potenziate da soluzioni commerciali - come rapidi aggiornamenti *software* forniti dai *partner* occidentali e servizi di intelligence satellitare commerciale accessibili direttamente ai soldati, come quelli dell'azienda *Vantor* [99] - capaci di superare in velocità i cicli di tracciamento russi legati alla guerra elettronica e all'intelligence satellitare, come abbiamo visto in precedenza.

Una problematica più ampia che ha inciso sulla qualità della *sigint* russa, infine, è la diffusione di analisi carenti e dati inattendibili all'interno dei servizi di sicurezza del Paese. Come è accaduto per la *humint*, i rapporti indicano che i comandanti sul campo in svariate occasioni hanno ricevuto informazioni imprecise e mappe basate su dati gonfiati o di provenienza interna non verificata.

---

[96] *Ukrainian forces destroy rare Russian signals intelligence system*, Ukrainska Pravda, 21/01/2026. https://www.pravda.com.ua/eng/news/2026/01/21/8017166/.

[97] T. Kruczek, *The $1.5 Million Starlink Jammer That Ukraine Keeps Blowing Up*, Keep Track, 03/08/2026. https://keeptrack.space/deep-dive/volna-kupol-garant-starlink-jamming.

[98] *Russia Jamming GPS In Ukraine? How Electronic Warfare Is Changing The Battlefield*, WION, 03/08/2026. https://www.youtube.com/watch?v=04y2051YTK4.

[99] *The Game-Changing Role of Commercial Spatial Intelligence in Ukraine*, Vantor, 12/04/2023. https://vantor.com/blog/the-game-changing-role-of-commercial-spatial-intelligence-in-ukraine/.

L'incapacità di sintetizzare in modo sicuro e di ritenere affidabili i dati provenienti dalle intercettazioni ha sovente compromesso capacità di prendere decisioni tattiche in tempo reale lungo tutta la catena di comando militare russa.

7. Miglioramenti nell'analisi intelligence

L'approccio tipico russo al *targeting* è schematico: applicare la formula corretta al bersaglio desiderato e attaccarlo con la quantità e il tipo di munizioni derivati dalla formula, e il gioco è fatto (in teoria). Tuttavia, le forze armate russe hanno evidenziato segni di progressi nell'effettuazione di un *targeting* più preciso, il che indica una migliore raccolta di informazioni e un'analisi situazionale più ponderata. Le forze armate russe potrebbero essere state motivate a stabilire queste TTPs dalla presenza di *high value target*s puntiformi sul campo di battaglia, come i sistemi *Himars* e *Patriot*, dalla necessità di gestire meglio le scorte di munizioni e dalla disponibilità di droni in grado di raccogliere dati informativi da analizzare. Due settori in cui questo sembra verificarsi sono la raccolta e l'analisi della valutazione dei danni sul campo di battaglia (BDA) e dei dati relativi ai modelli comportamentali.

In passato, era molto insolito che le forze armate russe si interessassero alla valutazione dei danni sul campo di battaglia:

> *"Una debolezza critica della campagna di attacchi russa è stata la valutazione dei danni di combattimento. In primo luogo, l'esercito russo sembra aver dato per scontato che, una volta ordinata ed eseguita un'azione, questa avesse avuto successo, a meno di prove dirette del contrario. La conferma del successo sembra essersi basata in misura sproporzionata su tre elementi informativi: la conferma da parte dei piloti di aver colpito il bersaglio; la conferma tramite satelliti russi della presenza di danni in un determinato sito; e la conferma derivante dall'intelligence dei segnali (SIGINT) circa la segnalazione, da parte ucraina, di un attacco e di danni ai propri equipaggiamenti. ... Dopo il 2022, la Russia ha potenziato drasticamente le proprie risorse spaziali, immettendo in orbita quasi 100 nuovi satelliti per svariate finalità. Anche le capacità di intelligence basata su immagini (IMINT) sono migliorate grazie all'aggiunta di almeno 6 nuovi satelliti. Tuttavia, rispetto a Cina e Stati Uniti, la Russia rimane ancora molto indietro sia in termini di qualità che di quantit[100]."*

[100] https://guerillamap.com/russian-spaceborne-imint-imagery-intelligence-capabilities/.

Dall'autunno del 2023, ci sono state indicazioni che i russi stiano eseguendo'con maggiore regolarità l'analisi dei bersagli con il BDA, soprattutto a livello tattico, per raccogliere informazioni sul successo (o il fallimento) dei loro attacchi. La prova di ciò è costituita principalmente da video raccolti da droni come l'*Orlan-30*. L'*Orlan-30* rimane in modalità hovering o circola sopra l'area per registrare gli effetti dell'impatto (esplosione secondaria delle munizioni, fumo, fiamme). Questo serve al comando russo per confermare la distruzione definitiva del bersaglio o ordinare un secondo colpo[101]. I russi tendono a pubblicare video che mostrano distruzioni riuscite, ma è probabile che esistano video non pubblicati che mostrano la raccolta di informazioni BDA per attacchi meno riusciti. Queste TTPs finalizzate al BDA, che sembrerebbero introdotte in tempi relativamente recenti, potrebbero indicare un serio sforzo per non sprecare munizioni predisposte, ma non più necessarie, per colpire obiettivi che risultano già neutralizzati o distrutti.

Oltre alle TTPs per il BDA, le forze armate russe sembrano aver sviluppato delle TTPs per condurre analisi dei modelli di comportamento. Questo è significativo perché rappresenta il riconoscimento da parte della Russia che il *targeting* fondato sull'*imaging* speculare, basato sul presupposto che gli ucraini si comportino come i russi, non funziona molto bene e dimostra anche la volontà di adattarsi alle differenze contingenti, da parte russa. Durante i primi due anni dell'invasione, il processo decisionale spesso si è basato su mappe non aggiornate, informazioni di *humint* discutibili, valutazioni obsolete o modelli inaffidabili. Dal marzo 2024, come parte integrante del loro ciclo di *targeting*, i russi hanno iniziato a integrare le procedure del BDA con studi più dettagliati e attualizzati per la pianificazione degli attacchi agli obiettivi designati. La disponibilità di droni in grado di osservare da altitudini più difficili da rilevare consente agli operatori di droni di raccogliere dati preziosi per l'analisi. I russi hanno perfezionato le TTPs di osservazione per osservare gli obiettivi in diversi momenti della giornata al fine di comprendere le attività degli ucraini. Le squadre di operatori di droni mappano accuratamente le posizioni delle forze ucraine in una determinata area prima di un attacco.

---

[101] *Russia-Ukraine War: Russia's Bird Of Prey*, The Orlan-30, WION, 13/11/2024. https://www.youtube.com/watch?v=m8k7c9fAGNI.

Per completezza di trattazione relativa al *targeting*, sebbene non inerente al BDA, vogliamo menzionare il radar di sorveglianza terrestre portatile *Fara-VR*, di cui un esemplare è stato catturato nel novembre 2023 dalle le forze ucraine[102]. Il Fara-VR è un piccolo ricetrasmettitore su treppiede. La batteria e il pannello di controllo sono collegati tramite un lungo cavo, consentendo così di controllare il radar a distanza da una posizione protetta. La stazione scansiona l'area e identifica automaticamente i bersagli in movimento, determinandone le coordinate. Il raggio di rilevamento di personale appiedato è fino a 4 km; quello di un carro armato fino a 8 km, di un camion fino a 10 km. L'apparato traccia quindi il bersaglio. Il sistema pesa 12 kg e la sua autonomia di funzionamento continuo a batteria è fino a 12 ore.

8. Integrazione dell'intelligence nel Complesso di Ricognizione e Attacco (RUK)

Nel primo capitolo, relativo all'"analisi dottrinale", abbiamo menzionato il Complesso di Ricognizione e Attacco (RUK), costituito dall'insieme delle funzioni intelligence, comando e controllo e fuoco, organizzate per neutralizzare con efficacia e precisione la capacità bellica del nemico. All'inizio dell'invasione, le forze armate russe erano troppo frammentate per coordinare e sincronizzare le componenti ISR, C2 e fuoco. Ma l'adozione da parte della Russia della tecnologia UAS e delle relative TTPs sembra aver consentito non solo enormi miglioramenti nella sincronizzazione dell'intelligence e del C2 con le risorse d'attacco delle forze terrestri, ma anche con quelle aeree e navali:

> *"Lo sviluppo di un nuovo sistema di ricognizione e attacco (RUK) è iniziato nell'interesse del Ministero della Difesa russo, secondo quanto riferito a Izvestia da fonti del dipartimento militare e confermato da fonti dell'industria della difesa. Il nuovo sistema si basa su un velivolo in grado di svolgere missioni ad alta quota, compresa la stratosfera (lo strato atmosferico situato ad altitudini comprese tra 11 e 50 km). Secondo fonti di Izvestia, il velivolo avrà una configurazione modulare. A seconda della missione, potrà essere equipaggiato con sistemi di ricognizione radar, elettronici o optoelettronici. Il nuovo sistema sarà in grado di acquisire bersagli in tempo reale sia sul campo di battaglia che nelle retrovie e di fornire designazioni di bersaglio ad armi a guida di precisione, artiglieria, aerei e navi militari. ... Il velivolo ad alta quota M-55 Geofizik sta attualmente testando la*

[102]https://www.reddit.com/r/UkraineWarVideoReport/comments/17xa81q/ukrainian_soldier_shows_a_captured_russian/.

capacità dei suoi pod sospesi di operare ad alta quota. Sulla base dei risultati dei test, verranno apportate ulteriori modifiche. Si sta inoltre testando la capacità di trasmettere informazioni in tempo reale a terra[103]*."*

La capacità della Federazione Russa di adottare gli sviluppi tecnologici dei droni per perfezionare ulteriormente le TTPs per l'osservazione del terreno e la raccolta dei dati informativi a livello operativo, dunque nell'area della *deep battl*e, appare come la guida motivazionale per la realizzazione del RUK, a lungo perseguita. Una volta che il comparto militare-industriale è riuscito a sviluppare diversi modelli di droni a lungo raggio impiegabili ad alta quota - e quindi con maggiori difficoltà di ingaggio da parte della dalla difesa aerea avversaria - le forze russe hanno avuto la possibilità di raccogliere informazioni mirate e non casuali. Il miglioramento delle TTPs di raccolta informativa è andato di pari passo con quello delle TTPs per coordinare non solo il fuoco indiretto dell'artiglieria e le munizioni circuitanti delle forze terrestri, ma anche le bombe plananti sganciate dalle Forze aerospaziali. In altre parole, il salto di qualità nella capacità di raccolta di dati per l'intelligence a livello operativo sembra aver comportato un significativo miglioramento di coordinare attacchi tempestivi e più precisi attraverso una moltitudine di risorse.

Come rilevato in apertura di questo *dossier*, sembra che la Russia abbia iniziato a concentrarsi sul miglioramento di questa capacità nel 2023, segnatamente implementando TTPs più raffinate nell'impiego dei droni *ZALA Lancet* in coordinamento con quelli per la sorveglianza del campo di battaglia:

"I Lancet sono prodotti dall'azienda aeronautica ZALA Aero Group. ZALA realizza anche piccoli UAV non armati Orlan-10, che la Russia impiega spesso insieme ai Lancet per individuare i bersagli[104]*."*

Con le nuove procedure, le munizioni circuitanti in oggetto vengono impiegate in coppia per aumentarne il livello di letalità, mentre un altro drone da ricognizione e sorveglianza viene poi inviato per il BDA riferito all'obiettivo:

---

[103] A. Ramm, B. Stepovoy, *Высокое размещение: армия РФ получит стратосферный комплекс поиска целей (Schieramento ad alta quota: l'esercito russo riceverà un sistema di acquisizione bersagli stratosferico)*, Izvestia, 08/11/2023.
https://iz.ru/1601565/aleksei-ramm-bogdan-stepovoi/vysokoe-razmeshchenie-armiia-rf-poluchit-stratosfernyi-kompleks-poiska-tcelei.

[104] *Russians deploy Lancet drones for strikes on Ukraine's artillery – UK intelligence*, Ukrainska Pravda, 01/11/2023.https://www.pravda.com.ua/eng/news/2023/11/01/7426676/.

"Nella pratica bellica reale, le munizioni a guida autonoma ZALA Lancet vengono sempre più spesso utilizzate in coppia: una sferra l'attacco, mentre l'altra ne conferma l'esito. L'esperienza dimostra che, per verificare la distruzione dell'equipaggiamento, una terza 'Lancet' viene ora spesso schierata in posizione di stazionamento nell'area designata. Dotato del sistema intelligente di puntamento e riconoscimento IRRA, il drone ZALA è in grado di localizzare e colpire con precisione i bersagli nemici. Allo stesso tempo, un sistema di guida elettro-ottico a doppio asse mantiene una comunicazione continua con l'operatore. In tempo reale, l'equipaggio del drone ZALA riceve immagini video e termiche, che gli consentono di tracciare la traiettoria del bersaglio, correggerne prontamente la rotta e registrare il momento dell'impatto. Pertanto, oltre alle sue capacità offensive, il «Lancet» svolge anche compiti di ricognizione: individua le risorse terrestri nemiche o affina le informazioni in vista di un attacco. Questa duplice funzionalità aumenta l'efficacia operativa, in quanto la conferma visiva dei risultati diventa parte integrante del piano di combattimento[105]."

Per la ricognizione a lungo raggio, accanto agli UAV della famiglia *Orlan*, sono stati introdotti gli innovativi *ZALA Z-16*:

"I droni da ricognizione Z-ZALA-16 continuano a svolgere attività di ricognizione aerea continua. Trasmettono in tempo reale alle unità russe dati sui bersagli individuati e sulle rotte di movimento del nemico. ... Il sistema ZALA Z-16 registra regolarmente anche le prestazioni delle forze aerospaziali, dell'artiglieria e degli equipaggi dei droni d'attacco. Ciò consente al comando di valutare rapidamente l'efficacia del puntamento dei bersagli e di prendere le decisioni successive[106]."

Un accenno, infine, su quello che è considerato come un collegamento critico nel RUK: il sistema *Strelets*. Si tratta di un sistema portatile utilizzato per trasmettere dati informativi raccolti tramite osservazione sul terreno. I russi lo definiscono un "complesso di intelligence, comando e controllo e comunicazione" (KRUS)[107]; quello che nella nostra dottrina indichiamo per brevità come "sistema C3I". Lo *Strelets* è un sistema modulare progettato per digitalizzare e connettere il singolo soldato sul campo di battaglia. Collega un computer portatile indossabile dal militare e diverse periferiche integrate di-

[105] *One strikes, the other confirms: the tactic of paired use of ZALA's "Lancet" reconnaissance and strike complex*, Zala, 09/05/2026. https://zala-aero.com/en/news/odin-byot-vtoroj-podtverzhdaet-taktika-parnogo-primeneniya-ruk-zala-lanczet/.

[106] *Zala Z-16 showed new footage of air strikes on positions of the Ukrainian Armed Forces*, Zala, 30/09/2026. https://zala-aero.com/en/news/zala-z-16-pokazal-novye-kadry-kontrolya-aviaudarov-po-pozicziyam-vsu/.

[107] Y. Zbanatsky, *Russian occupation forces in Donbas received Russian Strelets reconnaissance, command and control systems*, Militarnyi, 09/12/2021. https://militarnyi.com/en/news/russian-occupation-forces-in-donbas-received-russian-strelets-reconnaissance-command-and-control-systems/.

rettamente nei giubbotti tattici. Il sistema consente la navigazione individuale e di gruppo, il rilevamento di oggetti e la misurazione delle coordinate dei bersagli in tempo reale e mette in rete i dati raccolti dai soldati per mostrarli sulle mappe dei comandanti di unità. Ha la capacità di trasmettere direttamente le coordinate dei bersagli identificati per guidare con precisione il supporto aereo dei caccia-bombardieri o dell'artiglieria. Le evoluzioni del *software* e dell'*hardware* alla base dello *Strelets* sono state collegate a progetti russi di automazione della difesa. Un modello base di Strelets è stato inizialmente impiegato nel 2007. Una variante più recente, lo *Strelets-M*, è probabilmente il modello utilizzato nelle operazioni in atto in Ucraina. È in uso presso gli *spetsnaz* del GRU.

9. Misure di *opsec* e di counterintelligence russe

Le misure di counterintelligence adottate dai russi per la sicurezza delle proprie truppe nella guerra in atto in Ucraina sono state contraddistinte un misto di eccessive cautele (in qualche modo tipiche di un regime autoritario e diffidente) e di apparente e inspiegabile superficialità[108]. Da un lato, le agenzie di sicurezza russe si adoperano con ogni mezzo per scovare potenziali informatori tra il personale non combattente, che spesso vuole solo abbandonare le zone in cui sono in corso le operazioni. Esagerano con la *opsec* al punto che, in alcune unità, pochissimi membri hanno un quadro di conoscenza completo della missione assegnata. Dall'altro, le forze armate russe sembrano piuttosto lassiste riguardo alla protezione delle comunicazioni tattiche.

Esistono casi di attacchi sferrati con successo dalle forze armate ucraine contro le unità russe, che sono molto probabilmente attribuibili a una scarsa sicurezza operativa. Uno degli esempi più notevoli si è verificato della notte di Capodanno del 2022, quando un'unità ucraina equipaggiata con i sistemi *Himars* ha attaccato un reggimento di soldati alloggiati in un dormitorio di un istituto tecnico a Makiivka[109]. Sembra che i militari fossero riuniti nell'aula magna

[108] P. Satam, *Defense Magazine SLAMS Russian Army for 'Rookie Mistakes' In Ukraine War That Led To Annihilation Of Its Tanks OPSEC*, EurAsian Times, 16/04/2023. https://www.eurasiantimes.com/defense-magazine-slams-russian-army-for-rookie-mistake/.

[109] *Le macerie di Makiivka rasa al suolo, Kiev: "400 soldati russi uccisi a capodanno nel Donetsk"*, Rai Play, 02/01/2023. https://www.rainews.it/video/2023/01/le-macerie-di-makiivka-rasa-al-suolo-kiev-400-soldati-russi-uccisi-a-capodanno-nel-donetsk-496839a5-be97-4676-8677-f95ea7851456.html.

per ascoltare il messaggio di auguri di Putin per il nuovo anno. L'attacco con gli *Himars* ha causato un numero elevato di vittime e i comandanti reggimentali russi hanno accusato i soldati di aver presumibilmente consentito la geolocalizzazione della loro unità utilizzando i cellulari dal sito bersagliato. Tale eventualità è del tutto plausibile, anche se allo stesso tempo, probabilmente non è stata una buona idea da parte dei comandanti reggimentali concentrare questi soldati in un unico luogo, situato nel raggio d'azione degli *Himars*[110]. Che si sia trattato della una scarsa disciplina nell'uso dei cellulari o sia dipeso da altri motivi, la sicurezza operativa russa era talmente carente che gli ucraini hanno potuto colpire un obiettivo altamente remunerativo.

Nelle retrovie russe, soprattutto in Crimea, la sicurezza operativa russa è imposta principalmente dall'FSB. L'FSB è stato spietato nei confronti dei *post* sui *social media* che potrebbero fornire informazioni utili alle forze ucraine, soprattutto in presenza dei massicci attacchi portati, come abbiamo visto, con sistemi lanciarazzi. A volte si verificano segnalazioni di esplosioni in Crimea, ma a causa dell'azione repressiva dell'FSB, le persone hanno paura di caricare foto che potrebbero fornire informazioni sensibili che potrebbero avvantaggiare l'intelligence militare di Kiev. L'FSB tende a pubblicizzare i propri interventi repressivi verso le attività informative, consapevoli o meno, a favore dell'Ucraina, allo scopo di spaventare la popolazione che non sostiene l'"operazione speciale" e dissuadere altri potenziali informatori, oltre a ottenere una copertura positiva agli occhi dell'opinione pubblica russa. Nell'ottobre del 2023, i media nazionali russi hanno dato risalto alle incursioni dell'FSB e agli arresti a Melitopol e dintorni, nell'*oblast'* di Zaporizhzhia occupata dalla Federazione Russa. Tra questi, l'arresto di amministratori di *RIA-Melitopol* (un'agenzia di stampa russa) e del canale *Telegram "Melitopol Tse Ukraina"* (Melitopol è Ucraina). Presumibilmente, il personale di RIA-Melitopol utilizzava il proprio lavoro per i media russi come copertura per attività filo-ucraine. Secondo l'FSB, uno dei detenuti avrebbe fatto trapelare informazioni sui movimenti e le attrezzature militari russe al Direttorato principale dell'intelligence del Ministero della Difesa ucraino (HUR)[111].

---

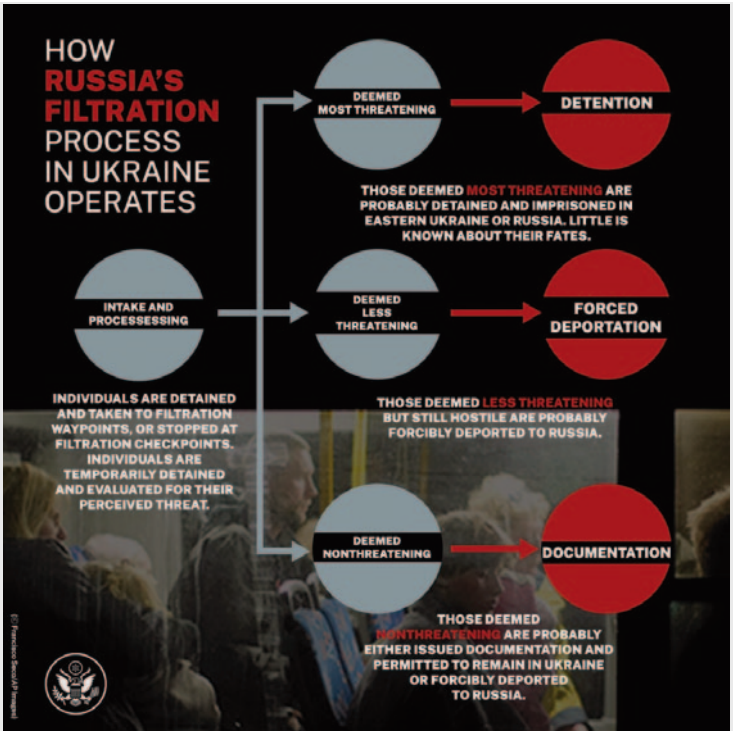
[110] M. Flammini, *L'attacco a Makiivka che ha smentito Putin*, Il Foglio, 02/01/2023. https://www.ilfoglio.it/esteri/2023/01/02/news/lattacco-a-makiivka-che-ha-smentito-putin—164801.

[111] *Russian forces detain administrators of RIA Melitopol Telegram channel*, International Press Institute, 30/10/2023. https://ipi.media/alerts/russian-forces-detain-administrator-of-ria-melitopol-telegram-channel/.

All'inizio di questo documento si è fatto cenno ai "campi di filtraggio" creati dai russi. Vediamo, allora, cosa siano le operazioni di filtraggio della popolazione attuate dall'FSB. Nei primi mesi dell'invasione, le forze russe hanno "filtrato" la popolazione civile in diverse aree occupate. La famigerata pratica del filtraggio richiama quella sovietica della Seconda Guerra Mondiale, con cui il Commissariato del Popolo per gli Affari Interni (NKVD, predecessore del KGB) selezionava e "filtrava" i cittadini e il personale militare sovietico che erano stati circondati o catturati dalle forze tedesche. Il filtraggio nell'occupazione delle regioni dell'Ucraina è un processo con cui la Russia pacifica le città occupate eliminando il sentimento filo-ucraino tra la popolazione civile nelle aree occupate dai russi. Sebbene lo scopo principale di tale attività sia quello di eliminare l'identità culturale ucraina, uno degli obiettivi chiave di questo duro processo è contrastare le attività di intelligence ucraine eliminando i potenziali informatori filo-ucraini.

Le persone individuate per il filtraggio riferiscono di aver atteso ore o addirittura giorni in fila con i loro veicoli privati per essere sottoposte a controlli presso le strutture predisposte a questo scopo. Le procedure attuate sono, di seguito, descritte. Mentre sono in fila, non è loro permesso di uscire per usare i servizi igienici o per prendere da mangiare. Una volta giunti al centro di controllo, i funzionari russi verificano i documenti personali e i telefoni cellulari alla ricerca di eventuali indizi di legami o simpatia verso iniziative filo-ucraine/anti-russe. Queste informazioni vengono confrontate con le liste della Federazione Russa di ucraini sospetti, come i giornalisti filo-ucraini. Gli uomini sono costretti a spogliarsi fino alla biancheria intima per verificare la presenza di tatuaggi compromettenti, come simboli ucraini o altre prove di aver combattuto contro le forze russe dal 2014 (prima dell'"operazione militare speciale"). Alcune donne riferiscono di essere state minacciate di stupro. Gli ucraini ritenuti potenziali informatori possono essere deportati in Russia o inviati a programmi di rieducazione ("denazificazione"). Ci sono segnalazioni di centinaia di migliaia di ucraini deportati in Russia. La rieducazione prevede il collocamento forzato in un campo di filtraggio e l'obbligo di lavorare, leggere e ascoltare costantemente materiale sulla necessità di "denazificare" l'Ucraina. È verosimile che, occasionalmente, i funzionari della Federazione Russa tramite il filtraggio abbiano reclutato con successo informatori da impiegare nelle attività di *humint*:

"Vi sono seri motivi di preoccupazione per il fatto che i civili detenuti da gruppi armati russi e affiliati alla Russia a seguito delle procedure di 'filtraggio' possano subire torture, altri maltrattamenti e sparizioni forzate durante la detenzione. Nel mese di maggio, la Missione di monitoraggio delle Nazioni Unite ha dichiarato di aver "confermato denunce relative a torture e maltrattamenti di persone in stato di detenzione, finalizzati a costringerle a confessare una collaborazione con il governo ucraino, a fornire informazioni o a collaborare con le forze armate russe. In particolare, le vittime hanno riferito di essere state tenute legate e bendate per diversi giorni; picchiate...; sottoposte a simulazioni di esecuzione; minacciate di violenza sessuale; rinchiuse in casse metalliche; costrette a cantare o gridare slogan di esaltazione; private di cibo e acqua (o rifornite in quantità insufficienti); e trattenute in locali sovraffollati e privi di servizi igienici[112]."



Il processo di "filtraggio della popolazione in Ucraina[113]

[112] B. Wille e al., *"We Had No Choice". "Filtration and the Crime of Forcibly Transferring Ukrainian Civilians to Russia*, Human Rights Watch, 01/09/2022. https://www.hrw.org/report/2022/09/01/we-had-no-choice/filtration-and-crime-forcibly-transferring-ukrainian-civilians.
[113] https://2021-2025.state.gov/russias-filtration-operations-and-forced-relocations/.

Dopo il 2022, ci sono poche notizie sul filtraggio in corso. Tuttavia, ci sono alcune notizie risalenti al 2024, riguardanti civili ucraini detenuti in Russia[114] ed è probabile che tali procedure siano state proseguite anche negli anni successivi[115].

Tra le attività della counterintelligence russa possiamo annoverare le azioni di assassinio mirato per eliminare alti funzionari dell'intelligence ucraina. Secondo l'Agenzia di intelligence del Ministero della Difesa dell'Ucraina, la moglie del capo dell'HUR Kyrylo Budanov, Marianna Budanova, è stata avvelenata (con arsenico e mercurio), insieme a diversi dipendenti di alto rango dell'Agenzia. Lo stesso Kyrylo Budanov sarebbe sopravvissuto a 10 tentativi di assassinio compiuti dall'FSB[116]. I servizi segreti russi hanno una storia di utilizzo di veleni contro i presunti nemici. Nel caso degli ucraini possiamo ricordare l'avvelenamento da diossina del 2004 dell'allora candidato alla presidenza ucraina, Viktor Yushchenko. Si ritiene ampiamente che la Russia sia stata dietro il suo avvelenamento, a causa della popolarità di Yushchenko e della sua posizione fortemente filo-occidentale[117].

10. Il reparto speciale *Centro 795*

Una trattazione particolare merita di essere rivolta al *Centro 795* (noto formalmente come Unità Militare 75127), creato per rimpiazzare l'*Unità 29155*, quella del "caso Skripal"[118], ormai "bruciata" dopo anni di indagini giornalistiche. Istituita nel dicembre 2022 e pienamente operativa dal 2023, è stata scoperta al-

---

[114] T. Katrychenko, *Для них немає обміну: Як звільнити українських цивільних з тюрем в Росії (Non c'è possibilità di scambio per loro: come liberare i civili ucraini dalle prigioni in Russia)*, Focus.ua, 23/03/2024. https://focus.ua/uk/politics/634730-dlya-nih-nemaye-obminu-yak-zvilniti-ukrajinskih-civilnih-z-tyurem-v-rosiji.

[115] M. Kulakova, *Russia Sets Up New Filtration Camp in Occupied Territories, Forcibly Distributes Passports*, United 24 Media, 28/02/2025. https://united24media.com/latest-news/russia-sets-up-new-filtration-camp-in-occupied-territories-forcibly-distributes-passports-6316.

[116] M. Serafini, *Marianna Budanova, moglie del capo dei servizi militari ucraini, avvelenata con metalli pesanti. L'ombra di un complotto di Mosca*, Corriere della Sera, 29/11/2023. https://www.corriere.it/esteri/23_novembre_29/marianna-budanova-avvelenata-ad344540-8e29-11ee-80d7-6428e39ac8b7.shtml.

[117] https://www.facebook.com/61565483970760/posts/nel-2004-il-candidato-presidenziale-ucraino-viktor-yushchenko-divenne-vittima-di/122189407622516132/

[118] M. Weiss e al., *Lost in translation: How Russia's new elite hit squad was compromised by an idiotic lapse in tradecraft*, The Insider, 13/03/2026. https://theins.press/en/inv/290235.

l'inizio del 2026 a seguito di una grave e imbarazzante violazione della sicurezza operativa. Un'inchiesta condotta da testate come *The Insider* e *Meduza* ha rivelato il funzionamento dell'unità e le dinamiche del suo collasso. Si tratta di un'unità clandestina voluta dal Cremlino dopo l'invasione dell'Ucraina, composta da agenti del GRU e dell'FSB con il compito di eliminare oppositori, condurre rapimenti e operazioni di sabotaggio in Europa e nel mondo[119].

La direzione era stata affidata a Denis Fisenko, un veterano del *Gruppo Alfa* delle forze speciali dell'FSB e l'unità risponde direttamente al Generale Valerij Gerasimov o ai suoi vice, anziché sottostare alla normale catena di comando del GRU. Il Centro è composto da circa 500 ufficiali scelti, provenienti da vari reparti d'*élite* del GRU, dell'FSB (*Alfa* e *Vympel*), dell'FSO e della *Rosgvardia*[120]. L'unità è stata celata sotto la copertura aziendale del gruppo *Kalashnikov* presso il *Patriot Park* a Kubinka, nell'*oblast'* di Mosca, con il sostegno finanziario di soggetti privati come l'imprenditore Andrei Bokarev. È strutturata su tre direzioni principali (Intelligence, Operazioni d'Assalto e Supporto al Combattimento), articolate in 35 dipartimenti specializzati in attività di sabotaggio, ricognizione e omicidi transnazionali:

> *"La struttura del Centro 795 è suddivisa in tre direzioni: Intelligence, Supporto al Combattimento e Operazioni d'Assalto. La Direzione dell'Intelligence è composta da nove dipartimenti distinti, incaricati, tra le altre cose, di raccogliere e analizzare informazioni provenienti dalle piattaforme dei social media, condurre ricognizioni utilizzando reti satellitari e droni, svolgere attività di intelligence sui segnali, nonché eseguire operazioni di intelligence umana e operazioni segrete, inclusi assassinii e rapimenti[121]."*

In particolare, la Direzione Intelligence si occupa del reclutamento e della gestione di agenti per le azioni di sabotaggio, della *sigint*, dell'*osint*, della ricognizione satellitare e tramite droni, della *humint* e della pianificazione di operazioni segrete.

L'unità è stata compromessa dopo che l'agente Denis Alimov e l'informatore Darko Durovic hanno utilizzato Google Translate per tradurre messaggi in

---

[119] Ibid.

[120] J. Fitsanakis, *Investigation uncovers previously unknown Russian covert action unit*, Intelnews, 16/03/2026. https://intelnews.org/2026/03/16/01-3432/. Per approfondimenti sui reparti speciali indicati nel testo, si suggerisce la lettura di N. Cristadoro, Spetsnaz e corpi paramilitari dei Servizi di Sicurezza Russi. L'antiterrorismo sui campi di battaglia, Il Maglio, 2018.

[121] Ibid.

chiaro mentre coordinavano un complotto per un omicidio all'estero ai danni di dissidenti. Poiché i log in chiaro transitavano su server statunitensi tramite Google Translate, l'FBI ha intercettato le comunicazioni in tempo reale. Ciò ha portato all'arresto di Darko Durovic nel marzo 2025 e alla detenzione di Denis Alimov a Bogotà, in Colombia, il 24 febbraio 2026, in attesa dell'estradizione:

> *"Denis Alimov, il referente del Centro 795 di nazionalità russa, e Darko Durovic, agente di lingua serbo-croata residente negli Stati Uniti, non si parlavano abbastanza bene le rispettive lingue per poter 'comunicare operativamente' in merito a un 'complotto per un omicidio su commissione'. I procuratori federali statunitensi sostengono che Alimov abbia reclutato Durovic come suo 'principale agente sul campo' per un'operazione incentrata sull'assassinio di membri della diaspora cecena in Europa che aspiravano all'indipendenza dalla Russia. Alimov avrebbe offerto a Durovic una ricompensa di 1,5 milioni di dollari per ogni obiettivo ucciso o deportato. 'La loro soluzione era semplice e, a quanto pare, catastrofica: hanno usato Google Traduttore', afferma l'inchiesta. I rapporti di Durović dal campo in Serbia e le istruzioni di Alimov in Russia venivano trasmessi tramite applicazioni crittografate che i due uomini ritenevano sicure. Tuttavia, Google opera su server situati negli Stati Uniti, ai quali l'FBI può accedere tramite un mandato di sorveglianza. Gli investigatori sono stati in grado di accedere a 'ogni istruzione e rapporto sullo stato di avanzamento' in 'voci leggibili e con data e ora'[122]."*

È possibile che la significativa compromissione relativa alle identità degli agenti e i conseguenti fallimenti delle operazioni pianificate possa portare al completo smantellamento dell'unità, anche se al momento della pubblicazione di questo dossier non si hanno notizie in tal senso.

11. Conclusioni

Nonostante le debolezze dell'intelligence strategica e operativa russa, causate da pregiudizi e corruzione, la Russia sta riuscendo ad adattarsi. L'errata valutazione iniziale della Russia sulla capacità di resistenza dell'Ucraina e sulla sua coesione interna è stata probabilmente dovuta a una combinazione tra un eccesso di ottimismo e l'aspettativa che le stime dell'intelligence dell'FSB e di altre agenzie si sarebbero allineate in ossequio ai disegni preconcetti di Vladimir Putin. Questo aspetto, a sua volta, potrebbe aver influito sull'approssimazione con cui la Russia ha affrontato la raccolta di *humint*.

---

[122] H. Wright, *'Sloppy tradecraft': How Russia's elite hit squad was foiled by Google Translate slip-up,* TPWorld, 14/03/2026. https://tvpworld.com/92091959/russias-elite-hit-squad-foiled-by-google-translate.

A ciò si aggiunge la probabile corruzione tra i reclutatori di fonti dell'FSB e del GRU, ed è comprensibile perché gran parte delle informazioni raccolte non fosse utilizzabile per colpire obiettivi specifici. I responsabili russi della pianificazione degli obiettivi si sono ritrovati con modelli speculari ai propri modelli procedurali per determinare obiettivi a profondità operativa che non producevano gli effetti desiderati.

La situazione è cambiata quando la Russia ha adottato l'uso di droni per raccogliere dati di intelligence facilmente utilizzabili per colpire il *targeting*.

Le informazioni raccolte tramite droni colmano gran parte della lacuna lasciata dalla cattiva qualità della *humint*. Questo successo con i droni sembra aver spinto le forze armate russe a migliorare drasticamente il coordinamento del fuoco, non solo per l'artiglieria e i lanciarazzi multipli, ma anche per tutti i tipi di sistemi d'arma disponibili per attacchi su obiettivi sia a livello tattico, sia a livello operativo.

Questa è almeno una parziale realizzazione dell'ambizione russa di disporre di un complesso di ricognizione e attacco funzionale.

Nonostante questa impressionante capacità di adattamento dimostrata, permangono delle lacune relativamente alla *humint* e alle capacità *imint*, soprattutto a livello satellitare. Le difficoltà della Russia con la *comsec* e, a volte, in materia di *opsec* - si pensi all'eclatante compromissione del *Centro 795* - creano anch'esse delle vulnerabilità.

Bibliografia e sitografia

ALTMAN, Howard, Russia Creates New Military Branch Dedicated To Drone Warfare, The War Zone, 13/11/2025. https://www.twz.com/news-features/russia-creates-new-military-branch-dedicated-to-drone-warfare.

ARMITAGE, Rebecca, Denys Kireyev was a Ukrainian spy hailed as a hero who saved Kyiv from Russian invaders. So why was he killed for treason?, ABC, 02/02/2023. https://www.abc.net.au/news/2023-02-03/mystery-over-killing-ukrainian-spy-denys-kireyev/101915844.

Army officer in Ukraine faces charges for failed recruitment of Russian pilots, Tass, 21/04/2023. https://tass.com/defense/1607951.

BERNAT, Pawel, KOZERA, Cyprian A., The Wagner Group Use of Chinese Space Intelligence, Irregular Warfare Initiative, 03/12/2024. https://www.irregularwarfare.org/the-wagner-groups-use-of-chinese-space-intelligence/.

BOROGAN, Irina, SOLDATOV, Andrei, GROSSFELD, Elena, RICHTEROVA, Daniela, What impact has the war on Ukraine had on Russian security and intelligence?, King's College London, 22/02/2023. https://www.kcl.ac.uk/what-impact-has-the-war-on-ukraine-had-on-russian-security-and-intelligence.

BOSTOCK, Bill, Video shows Ukrainian soldier taking apart a Russian drone and discovering its components include a plastic bottle top for a fuel cap, Business Insider, 11/04/2022. https://www.businessinsider.com/video-ukraine-soldier-disassembles-russian-drone-reveals-unsopisticated-handiwork-2022-4.

BRODKIN Jon, Report details how Russia obtains Starlink terminals for war in Ukraine, Ars Technica, 09/04/2024. https://arstechnica.com/tech-policy/2024/04/report-details-how-russia-obtains-starlink-terminals-for-war-in-ukraine/.

BUTUSOV, Yurii, Reasons and responsibility for tragedy in 128th Mountain Assault Brigade, Censor.net, 05/11/2023. https://censor.net/en/resonance/3453741/reasons_and_responsibility_for_tragedy_in_128th_mountain_assault_brigade.

BUZHALA, Nysret, Assessing Russian Network Warfare Through the Lens of the Ukraine Conflict, Small Wars Journal. 12/05/2026. https://smallwarsjournal.com/2026/05/12/assessing-russian-network-warfare.

CARVIN, Stephanie, Russia's Stalled Electronic Warfare Betrays Bad Planning, Poor Training, Centre for International Government Innovation, 04/08/2022. https://www.cigionline.org/articles/russias-stalled-electronic-warfare-betrays-bad-planning-poor-training/.

CHARPENTREAU, Clement, Ukraine probes failed plot to recruit Russian military pilots, AeroTime, 21/04/2023. https://www.aerotime.aero/articles/ukraine-probes-failed-plot-to-recruit-russian-military-pilots.

CLISZCZ, Eric, Russian top ex-commander says Moscow was 'unprepared' for invading Ukraine, TVP, 03/12/2025. https://tvpworld.com/90354057/russian-ex-commander-chirkin-moscow-was-unprepared-for-ukraine-war.

CLARK, Bryan, The Fall and Rise of Russian Electronic Warfare, The Global Network, 30/07/2022. https://space4peace.org/the-fall-and-rise-of-russian-electronic-warfare/.

CLOVER, Charles, DEPREZ, Fabrice, The elite Russian unit hunting Ukraine's drone warriors, The Financial Times, 13/11/2025. https://www.ft.com/content/05ca82cc-2613-4144-a4e0-fd595246df8e.

Congessional Research Service, Russian Hybrid Warfare Activities in Europe: Considerations for Congress, 11/08/2026.

Corso di artiglieria per operatori di sistemi aerei a pilotaggio remoto (UAS), San Pietroburgo, 2022.

CRANNY-EVANS, Sam, WITHINGTON, Thomas, Russian Comms in Ukraine: A World of Hertz, RUSI, 09/03/2022. https://www.rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz.

Crowdstrike, Use of Fancy bear Android Malware in Tracking of Ukrainian Field Artillery Units, Dec 2016. https://www.crowdstrike.com/en-us/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

CRISTADORO, Nicola, La cooperazione russo-iraniana per la produzione di droni e il contributo della Cina, Istituto Gino Germani, Settembre 2025.

CRISTADORO, Nicola, Spetsnaz e corpi paramilitari dei Servizi di Sicurezza Russi. L'antiterrorismo sui campi di battaglia, Il Maglio, 2018.

CRISTADORO, Nicola, Wagner & Co. Le compagnie di ventura russe ai tempi della guerra in Ucraina, Il Maglio, 2022.

Darnytskyi Car Repair Plant after Russia's missile strikes: Production shops destroyed but no tanks, Ukrinform, 06/06/2022. https://www.ukrinform.net/rubric-ato/3500583-darnytskyi-car-repair-plant-after-russias-missile-strikes-production-shops-destroyed-but-no-tanks.html.

DIAKONOV, Ivan, Russia creates separate regiments of unmanned systems to strengthen its army – ISW, Ukrainska Pravda, 29/01/2025. https://www.pravda.com.ua/eng/news/2025/01/29/7495735/.

"Dronefall" reaches a new level - Dozens of Shaheds downed by Ukrainian Army, Savelife.in Ua, 1/06/2025. https://savelife.in.ua/en/materials/news-en/dronefall-reaches-a-new-level-dozens-of-en/.

DÜBEN, Björn Alexander, "There is no Ukraine": Fact-Checking the Kremlin's Version of Ukrainian History, LSE, 01/07/2020. https://blogs.lse.ac.uk/lseih/2020/07/01/there-is-no-ukraine-fact-checking-the-kremlins-version-of-ukrainian-history/.

FITSANAKIS, Joseph, Investigation uncovers previously unknown Russian covert action unit, Intelnews, 16/03/2026. https://intelnews.org/2026/03/16/01-3432/.

FLAMMINI, Micol, L'attacco a Makiivka che ha smentito Putin, Il Foglio, 02/01/2023. https://www.ilfoglio.it/esteri/2023/01/02/news/lattacco-a-makiivka-che-ha-smentito-putin—164801.

HARDIE, John, Russia announces plans to form Unmanned Systems Forces, FDD's Long War Journal, 20/12/2024. https://www.longwarjournal.org/archives/2024/12/russia-announces-plans-to-form-unmanned-systems-forces.php.

How Is Russia Using Orlan-30 UAVs to Enhance Their Artillery, Defence Central, 27/03/2024, https://www.youtube.com/watch?v=ivlHtUw2-J8.

How Russia recruits spies through social media, Kyiv Independent, 02/08/2026. https://www.youtube.com/watch?v=pITde5slL0A.

https://2021-2025.state.gov/russias-filtration-operations-and-forced-relocations/.

https://dobrocor.ru/nashi-otryady/8-ya-brigada/.

https://dobrocor.ru/ya-zdes-sebya-nashel-operatory-bpla-8-y-brigady-o-dele-kotoromu-teper-sluzhat/.

https://gagadget.com/en/116417-whats-inside-orlan-10-a-canon-consumer-camera-and-a-plastic-bottle-were-found-in-a-drone-shot-down-by-the-armed-forces-of/.

https://guerillamap.com/russian-spaceborne-imint-imagery-intelligence-capabilities/.

https://t.me/s/obtf_kaskad/588.

https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_25-11/.

https://www.facebook.com/61565483970760/posts/nel-2004-il-candidato-presidenziale-ucraino-viktor-yushchenko-divenne-vittima-di/12218940 7622516132/.

https://www.globalsecurity.org/intell/world/russia/gru-org.htm.

https://www.reddit.com/r/UkraineWarVideoReport/comments/17xa81q/ukrai nian_soldier_shows_a_captured_russian/.

https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-may-13-2026.

https://www.russiamatters.org/news/russia-ukraine-war-report-card/russia-ukraine-war-report-card-may-20-2026.

HWANG, Ji-Jen, Reassessing Biddle's Modern System: data-linked kill chains, advanced algorithms, and the evolution of combined arms warfare in the Russo-Ukrainian war, Taylor&Francis, 12/05/2026, https://www.tandfonline.com/doi/full/10.1080/14702436.2026.2672089?scroll=top&needAccess=true#abstract.

Igor Girkin: rebel Donbas leader turned Kremlin critic, France 24, 28/08/2023. https://www.france24.com/en/live-news/20230829-igor-girkin-rebel-donbas-leader-turned-kremlin-critic.

JHANJHI, Noor Ul Amin, e al., The Rise of GPS Spoofing Attacks on Drones in the Russia-Ukraine War, TechRxiv, 09/07/2025. https://www.techrxiv.org/doi/full/10.36227/techrxiv.175203757.71749390/v1.

KAKISSIS, Joanna, Ukraine hunts for pro-Moscow collaborators suspected of helping Russia strike targets, Npr, 21/09/2022. https://www.npr.org/2022/09/21/1124108146/ukraine-russia-suspected-collaborators-mykolaiv.

KATISHEV, Kostyantin, Разоблачены наводчики ракеты на село Гроза (I responsabili del puntamento del missile sono stati smascherati), Kommersant, 11/10/2023. https://korrespondent.net/ukraine/4630596-razoblacheny-navodchyky-rakety-na-selo-hroza.

KATRYCHENKO, Tetyana, Для них немає обміну: Як звільнити українських цивільних з тюрем в Росії (Non c'è possibilità di scambio per loro: come liberare i civili ucraini dalle prigioni in Russia), Focus.ua, 23/03/2024. https://focus.ua/uk/politics/634730-dlya-nih-nemaye-obminu-yak-zvilniti-ukrajinskih-civilnih-z-tyurem-v-rosiji.

KRAVETS, Roman, Ukraine's Security Service catches man who facilitated Russian missile strike at Frankivsk Airport, Ukrainska Pravda, 02/03/2022. https://www.pravda.com.ua/eng/news/2022/03/02/7327421/.

KRUCZEK, Theodore, The $1.5 Million Starlink Jammer That Ukraine Keeps Blowing Up, Keep Track, 03/08/2026. https://keeptrack.space/deep-dive/volna-kupol-garant-starlink-jamming.

KULAKOVA, Maria, Russia Sets Up New Filtration Camp in Occupied Territories, Forcibly Distributes Passports, United 24 Media, 28/02/2025. https://united24media.com/latest-news/russia-sets-up-new-filtration-camp-in-occupied-territories-forcibly-distributes-passports-6316.

KUSHNIKOV, Vadim, For the first time, Ukrainian paratroopers have shot down a Russian Horizon S-100 drone, Militarnyi, 20/04/2022. https://mili-

tarnyi.com/en/news/for-the-first-time-ukrainian-paratroopers-have-shot-down-a-russian-horizon-s-100-drone/.

KUSHNIKOV, Vadim, Ukrainian air defense shot down an enemy drone "Kartograf," which has a camera with 12 lenses, Militarnyi, 02/09/2022. https://militarnyi.com/en/news/ukrainian-air-defense-shot-down-an-enemy-drone-kartograf-which-has-a-camera-with-12-lenses/.

KUSHNIKOV, Vadim, Ukrainian Ground Forces announced the destruction of almost 60 reconnaissance UAVs in a week, Militarnyi, 21/07/2024. https://militarnyi.com/en/news/ukrainian-ground-forces-announced-the-destruction-of-almost-60-reconnaissance-uavs-in-a-week/.

L'Ucraina punta sulla guerra elettronica tra intercettazioni radio e disturbo del segnale dei droni, Euronews, 14/02/2024. https://www.youtube.com/watch?v=XAoeVmo0OMU.

Le macerie di Makiivka rasa al suolo, Kiev: "400 soldati russi uccisi a capodanno nel Donetsk", Rai Play, 02/01/2023. https://www.rainews.it/video/2023/01/le-macerie-di-makiivka-rasa-al-suolo-kiev-400-soldati-russi-uccisi-a-capodanno-nel-donetsk-496839a5-be97-4676-8677-f95ea7851456.html.

LEGALOV, Evgeny, DOBRYNIN, Sergey, KRUTOV, Mark, Тайна "Рубикона". БПЛА-спецназ в парке "Патриот" (Il mistero di Rubicon:droni delle forze speciali al Patriot Park), Radio Svoboda, 17/09/2025. https://www.svoboda.org/a/tayna-rubikona-bpla-spetsnaz-v-parke-patriot-/33531165.html.

LEVYTSKA, Iryna, A shield against FPV drones: is Ukraine's electronic warfare capability matching drone advancements?, Ukrainska Pravda,

08/08/2025. https://www.pravda.com.ua/eng/articles/2025/08/08/7525279/.

LITNAROVYCH, Vlad, Russia's Rare Merlin-VR Recon Drone Eliminated by Ukrainian FPV Crews, Video, United 24, 16/01/2025. https://united24media.com/latest-news/russias-rare-merlin-vr-recon-drone-eliminated-by-ukrainian-fpv-crews-video-5144.

LUKIV, Jaroslav, Russia targeting 'ordinary life' with attacks on Ukraine's data centres, Zelensky says, BBC, 25/09/2026. https://www.bbc.com/news/articles/c84gkwgk7d06o.

LYTOVCHENKO, Viktoria, Russia tries to recruit spies among Ukrainians using blackmail, Online.Ua, 04/04/2024. https://news.online.ua/en/russia-tries-to-recruit-spies-among-ukrainians-using-blackmail-876092/.

MacALPINE, Audrey, Russian soldiers disguised in civilian clothes infiltrating front-line city, The Telegraph, 13/08/2025.

https://www.telegraph.co.uk/world-news/2025/08/13/russian-soldiers-disguised-civilian-clothing-infiltrating/.

MARZHETSKY, Sergey, Как БПЛА "Орион" может стать эффективным охотником на морские дроны (Come il drone Orion potrebbe diventare un efficace cacciatore di droni marittimi), AviaPort, 06/09/2024. https://www.aviaport.ru/news/kak-bpla-orion-mozhet-stat-effektivnym-okhotnikom-na-morskie-drony/.

McBRIDE, Julian, How Small Reconnaissance Units are Playing a Critical Role in Russian Frontline Movements in 2025, Atlas institutw for International Affairs, 19/11/2025. https://atlasinstitute.org/how-small-reconnais-

sance-units-are-playing-a-critical-role-in-russian-frontline-movements-in-2025/.

McDERMOTT, Roger N., NATO is measuring Russian adaptation the wrong way, Breaking Defense, 18/09/2026. https://breakingdefense.com/2026/09/nato-is-measuring-russian-adaptation-the-wrong-way/.

McDERMOTT, Roger N., Russia's New Unmanned Systems Forces and the Strategic Role of DKO Weapons, The Saratoga Foundation, 20/06/2025. https://www.saratoga-foundation.org/p/russias-new-unmanned-systems-forces.

MILLER, Greg, BELTON, Catherine, Russia's spies misread Ukraine and misled Kremlin as war loomed, The Washington Post, 19/08/2022. https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/.

Network of agents and coordinates of the deployment of Ukrainian troops: law enforcement officers detained a Russian woman in Sumy region, MSV, 08/09/2023. https://mvs.gov.ua/en/news/mereza-agentiv-ta-koordinati-rozmishhennia-ukrayinskix-viisk-pravooxoronci-zatrimali-rosiianku-na-sumshhini.

One strikes, the other confirms: the tactic of paired use of ZALA's "Lancet" reconnaissance and strike complex, Zala, 09/05/2026. https://zala-aero.com/en/news/odin-byot-vtoroj-podtverzhdaet-taktika-parnogo-primeneniya-ruk-zala-lanczet/.

RAMM, Alexey, STEPOVOY, Bogdan, Высокое размещение: армия РФ получит стратосферный комплекс поиска целей (Schieramento ad alta quota: l'esercito russo riceverà un sistema di acquisizione bersagli stratosferico), Izvestia, 08/11/2023.

https://iz.ru/1601565/aleksei-ramm-bogdan-stepovoi/vysokoe-razmeshchenie-armiia-rf-poluchit-stratosfernyi-kompleks-poiska-tcelei.

ROMMEN, Rebecca, Russian milbloggers slam Kremlin propagandists for ignoring huge Russian losses and 'blunders' in Ukraine, Business Insider, 04/02/2024. https://www.businessinsider.com/russian-milbloggers-putin-kremlin-propagandists-war-ukraine-losses-2024-2.

ROSHCHINA, Olena, Saboteurs are operating in Kyiv, Russian troops are going round in circles near Kyiv - head of the Kyiv Military Administration, Ukrainska Pravda, 17/03/2022. https://www.pravda.com.ua/eng/news/2022/03/17/7332137/.

Russia demonstrates the Lancet-E RUK at the Dubai Airshow, Zala, 19/11/2025. https://zala-aero.com/en/news/rossiya-demonstriruet-rabotu-ruk-lanczet-e-na-aviashou-v-dubae/.

Russia establishes Unmanned Systems Forces, Tass, 12/11/2025. https://tass.com/defense/2042371.

Russia Jamming GPS In Ukraine? How Electronic Warfare Is Changing The Battlefield, WION, 03/08/2026. https://www.youtube.com/watch?v=04y2051YTK4.

Russia ramps up drone production, reshaping the war in Ukraine, You Tube, 20/08/2025. https://www.youtube.com/watch?v=sjT8GhPGBMU&t=1s.

Russian agent arrested in Odesa, Kyiv Post, 15/08/2022. https://www.kyivpost.com/post/1745.

Russian forces detain administrators of RIA Melitopol Telegram channel, International Press Institute, 30/10/2023. https://ipi.media/alerts/russian-forces-detain-administrator-of-ria-melitopol-telegram-channel/.

Russian “Inokhodets” drone destroyed in occupied Crimea, UA.News, 04/04/2026. https://ua.news/en/war-vs-rf/v-okupovanomu-krimu-znishcheno-rosiiskii-bezpilotnik-inokhodets.

Russians deploy Lancet drones for strikes on Ukraine's artillery – UK intelligence, Ukrainska Pravda, 01/11/2023.https://www.pravda.com.ua/eng/news/2023/11/01/7426676/.

Russia-Ukraine War: Russia's Bird Of Prey, The Orlan-30, WION, 13/11/2024. https://www.youtube.com/watch?v=m8k7c9fAGNI.

Russia's new killer drone on cam; more power, heavier payload, longer reach | Molniya-13, 21/06/2026. https://www.facebook.com/toiworldnews/videos/russias-new-killer-drone-on-cam-more-power-heavier-payload-longer-reach-molniya-/1031763069188870/.

SAMAR, Valentyna, MARCHENKO, Vladimiro, «GROM Kaskad». Who Fights against Ukraine in the First Russian Drone Brigade, Center of Journalistic Investigations, 18/05/2024. https://investigator.org.ua/en/investigations/266753/.

SATAM, Parth, Defense Magazine SLAMS Russian Army for ‘Rookie Mistakes’ In Ukraine War That Led To Annihilation Of Its Tanks OPSEC, EurAsian Times, 16/04/2023. https://www.eurasiantimes.com/defense-magazine-slams-russian-army-for-rookie-mistake/.

SAUER, Pjotr, Hundreds of Ukrainians forcibly deported to Russia, say Mariupol women, The Guardian, 22/04/2022. https://www.theguardian.com/world/2022/apr/04/hundreds-of-ukrainians-forcibly-deported-to-russia-say-mariupol-women.

SBU arrested an FSB agent in Odesa for spying on Ukrainian defenses, Mezha, 30/06/2026. https://mezha.net/eng/news/7c7210b2_sbu_arrested_an/.

SERAFINI, Marta, Marianna Budanova, moglie del capo dei servizi militari ucraini, avvelenata con metalli pesanti. L'ombra di un complotto di Mosca, Corriere della Sera, 29/11/2023. https://www.corriere.it/esteri/23_novembre_29/marianna-budanova-avvelenata-ad344540-8e29-11ee-80d7-6428e39ac8b7.shtml.

SHUMLIANSKYI, Dmytro, "Russians Completes Formation of First UAV regiment, Presents it at May 9 Parade", Militarnyi, 11/05/2025. https://militarnyi.com/en/news/russians-completes-formation-of-first-uav-regiment-presents-it-at-may-9-parade/.

SIMPSON, John, GARDHAM, Duncan, Telegram,'trash fishing' and the Wagner Group plot to groom UK criminals for'grey zone' attacks, The Observer, 12/07/2025. https://observer.co.uk/news/national/article/telegram-trash-fishing-and-the-wagner-group-plot-to-groom-uk-criminals-for-grey-zone-attacks.

SpaceX limits Starlink internet to keep Russia from using it to target drone strikes, Scripp News, 03/02/2026. https://www.youtube.com/watch?v=U6iXuF8vTqU&t=47s.

STERNE, David L., Russian missile strikes brigade in Zaporizhzhia, Ukraine says, The Washington Post, 05/11/2023. https://www.washingtonpost.com/

world/2023/11/05/russia-ukraine-128th-mountain-brigade-strike/.

SWIT, Rafael, DALTON, Ben, RONDEAUX, Candace, Paramilitary Paper Trails: Mapping the Wagner Group's Ties to Russia with Personnel Data, New America, 02/10/2024. https://www.newamerica.org/insights/paramilitary-paper-trails/.

TARADIUK, Yuliia Russia establishes Unmanned Systems Forces, Ukraine says it's just "copying our successful approaches", The Kyiv Independent, 12/11/2025. https://kyivindependent.com/russia-establishes-its-unmanned-systems-forces-copying-ukraines-successful-approaches/.

The Game-Changing Role of Commercial Spatial Intelligence in Ukraine, Vantor, 12/04/2023. https://vantor.com/blog/the-game-changing-role-of-commercial-spatial-intelligence-in-ukraine/.

The war of no man: Russia creates drone army 'Unmanned Systems Forces' to rival Ukraine, The Week Magazine, 13/11/2025. https://www.theweek.in/news/defence/2025/11/13/the-war-of-no-man-russia-creates-drone-army-unmanned-systems-forces-to-rival-ukraine.html#google_vignette.

TREVELYAN, Mark, MALENKO, Anastasiia, STOLYAROV, Gleb, "A complete intelligence failure": how Russia looked the wrong way as Ukraine invaded, Breakingnews, 17/08/2024. https://www.breakingnews.ie/explained/analysis-how-russia-looked-the-wrong-way-as-ukraine-invaded-1662303.html.

Ukrainian forces destroy rare Russian signals intelligence system, Ukrainska Pravda, 21/01/2026. https://www.pravda.com.ua/eng/news/2026/01/21/8017166/.

Unmanned systems forces "hunted down" a rare enemy drone "Forpost-R" over the Kursk region, UNN, 27/07/2026. https://unn.ua/en/news/unmanned-systems-forces-hunted-down-a-rare-enemy-drone-forpost-r-over-the-kursk-region.

US company Iridium provides navigation for FSB drones during combat, Ukrainska Pravda, 28/09/2023. https://www.pravda.com.ua/eng/news/2023/09/28/7421863/.

VILLAREAL, Daniel, State-Run Russian News Site Accidentally Declares Ukraine's Defeat, Newsweek, 28/02/2022. https://www.newsweek.com/state-run-russian-news-site-accidentally-declares-ukraines-defeat-1683455.

VOLZHSKY, Ilya, KANEVSKAYA, Sofia, Коррупционный полк (Reggimento della corruzione), Novaya Gazeta Europa, 15/11/2025. https://novayagazeta.eu/articles/2025/11/15/korruptsionnyi-polk.

War of Drones: what kind of 'kamikaze' drones Ukraine and Russia use, Espreso, 28/07/2023. https://global.espreso.tv/war-of-drones-what-kind-of-kamikaze-drones-ukraine-and-russia-use.

Weapons & equipment seized from alleged Russian saboteurs in Ukraine (2022), ARES, 25/03/2022. https://armamentresearch.com/weapons-equipment-seized-from-alleged-russian-saboteurs-in-ukraine-2022/.

WEISS, Michael e al., Lost in translation: How Russia's new elite hit squad was compromised by an idiotic lapse in tradecraft, The Insider, 13/03/2026. https://theins.press/en/inv/290235.

WILLE, Belkis e al., “We Had No Choice”. “Filtration and the Crime of Forcibly Transferring Ukrainian Civilians to Russia, Human Rights Watch, 01/09/2022. https://www.hrw.org/report/2022/09/01/we-had-no-choice/filtration-and-crime-forcibly-transferring-ukrainian-civilians.

WOOD, Graeme, A Suspicious Pattern Alarming the Ukrainian Military, The Atlantic, 18/03/2024. https://www.theatlantic.com/international/archive/2024/03/american-satellites-russia-ukraine-war/677775/.

WRIGHT, Helen, ‘Sloppy tradecraft’: How Russia’s elite hit squad was foiled by Google Translate slip-up, TPWorld, 14/03/2026. https://tvpworld.com/92091959/russias-elite-hit-squad-foiled-by-google-translate.

Zala Z-16 showed new footage of air strikes on positions of the Ukrainian Armed Forces, Zala, 30/09/2026. https://zala-aero.com/en/news/zala-z-16-pokazal-novye-kadry-kontrolya-aviaudarov-po-pozicziyam-vsu/.

ZBANATSKY, Yuriy, Russian occupation forces in Donbas received Russian Strelets reconnaissance, command and control systems, Militarnyi, 09/12/2021. https://militarnyi.com/en/news/russian-occupation-forces-in-donbas-received-russian-strelets-reconnaissance-command-and-control-systems/.

В Минобороны создали центр перспективных беспилотных технологий "Рубикон" (Il Ministero della Difesa ha istituito il Centro per le tecnologie avanzate senza pilota Rubicon), Tass, 11/10/2024. https://tass.ru/armiya-i-opk/22099195.

Elenco degli acronimi

BAI: *Battlefield Area Interdiction* (Interdizione dell'Area della Battaglia)

BDA: *Battle Damage Assessment* (valutazione dei danni da battaglia)

C2: *Command and Control* (Comando e Controllo)

CAA: *Combined Arms Army* (Armata Combinata)

Comsec: *Communications Security* (Sicurezza delle Comunicazioni)

DRG: *Diversionno Razvedyvatel'nyye Gruppi* (Gruppo di Ricognizione e Sabotaggio)

DNR: *Doneckaja Narodnaja Respublika* (Repubblica Popolare di Donetsk)

Elint: *Electronic-signals Intelligence* (intelligence dei segnali elettronici)

EW: *Electronic Warfare* (Guerra Elettronica)

FPV: Fi*rst Person View* (Visuale in prima persona)

FSB: *Federál'naja služba bezopásnosti* (Servizio di sicurezza federale)

GRU: *Glavnoe razvedyvatel'noe upravlenie* (Direzione generale per le informazioni militari)

Humint: *Human Intelligence* (intelligence delle fonti umane)

HUR: *Holovne Upravlìnnjâ Rozvìdki* (Direttorato Principale dell'Intelligence)

HVTs: *High Value Targets* (Bersagli di Valore Elevato)

Imint: *Imagery Intelligence* (intelligence delle immagini)

ISR: *Intelligence, Surveillance, Reconnaissance* (Intelligence, Sorveglianza, Ricognizione)

KGB: *Komitet Gosudarstvennoj Bezopasnosti* (Comitato per la Sicurezza dello Stato)

KRUS: *Kompleks Razvedki, Upravleniya i Svyazi* (Complesso di Ricognizione, Controllo e Comunicazione)

LCC: *Line of Contact e Combat* (linea di contatto e di combattimento)

MALE: *Medium-Altitude Long-Endurance* (Quota Media, Lunga Autonomia)

MTO: *Material Technical Organization* (Organizzazione Tecnica e dei Materiali)

NKVD: *Narodnyj komissariat vnutrennich del* (Commissariato del popolo per gli affari interni)

OBTF: *Operativno-boyevoye takticheskoye formirovaniye* (Formazione Tattica Operativa da Combattimento)

Opsec: *Operations Security* (Sicurezza delle Operazioni)

PMC: *Private Military Company* (Compagnia Militare Privata)

RUK: *Razvedyvatel'no-udarnyy komplek*s (Complesso di Ricognizione e Attacco)

SAR: *Synthetic Aperture Radar* (Radar ad apertura sintetica)

SBU: *Služba Bezpeky Ukraïny* (Servizio di Sicurezza dell'Ucraina)

Sigint: *Signal Intelligence* (intelligence delle trasmissioni)

TTPs: *Technical-Tactical Procedures* (Procedure Tecnico-Tattiche)

UAV: *Unmanned Aerial Vehicles* (veicoli aerei senza pilota)

USV: *Unmanned Surface Vehicles* (veicoli di superficie senza pilota)

VBS: *Voyska bespilotnykh sistem* (Forze dei sistemi senza pilota)

VDV: *Vozdušno-desantnye vojska* (Forze aviotrasportate)

VKS: *Vozdušno-kosmičeskie sily* (Forze Aerospaziali)

Finito di stampare
ottobre 2026