NUOVA ANTOLOGIA MILITARE
RIVISTA INTERDISCIPLINARE DELLA SOCIETÀ ITALIANA DI STORIA MILITARE

Fascicolo Speciale 2021

Intelligence militare, guerra clandestina e Operazioni Speciali

a cura di
GÉRALD ARBOIT

Società Italiana di Storia Militare

Nuova Antologia Militare
Rivista interdisciplinare della Società Italiana di Storia Militare
Periodico telematico open-access annuale (www.nam-sism.org)
Registrazione del Tribunale Ordinario di Roma n. 06 del 30 Gennaio 2020

Direzione, Via Bosco degli Arvali 24, 00148 Roma
Contatti: direzione@nam-sigm.org ; virgilio.ilari@gmail.com

Grafica: Nadir Media Srl - Via Giuseppe Veronese, 22 - 00146 Roma
info@nadirmedia.it

Gruppo Editoriale Tab Srl -Viale Manzoni 24/c - 00185 Roma
www.tabedizioni.it

ISSN: 2704-9795

ISBN Fascicolo Speciale 2021: ISBN: 978-88-9295-270-6

L'*intelligence* militare russa
Il GRU nel decennio 2010-2020.
Il più potente servizio di *intelligence* della Russia contemporanea

di Nicola Cristadoro

Abstract. This article, based on Western open sources, tries an appreciation of the present Russian military intelligence (GR, former GRU), the most powerful intelligence agency which has maintained its identity in the dramatic transition from the Soviet Union to the Russian Federation. The agency is responsible for all levels of military intelligence, from tactical to strategic, through consolidated networks for humint and sigint activities. The GRU also employs the Spetsnaz brigades, whose traditional tasks range from reconnaissance missions on the battlefield, raids into enemy targets, sabotage actions, as well as training and supervising pro-Russian paramilitary and partisan units or units of mercenaries in the pay of the Kremlin. Alongside the traditional roles related to combat and intelligence, the GRU conducts operations of cyberwar, disinformation, propaganda and, nonetheless, the elimination of opponents deemed dangerous by the Moscow government. In the last decade, the failure of some of these operations and the identification of several of its operational agents have brought to light the responsibilities of the organization and have significantly contributed to outlining its operational procedures, which have always been wrapped in an understandable framework of secrecy.

Keywords. Spetsnaz, humint, sigint, cyberwar, info-ops, Gerasimov, Skripal'

Premessa

Il GRU (*Glavnoe Razvedyvatel'noe Upravlenie* - Direzione Principale dell'Intelligence) è l'agenzia di *intelligence* militare russa. Si tratta di una grande, articolata e potente organizzazione con compiti di raccolta informativa all'estero e responsabile dell'impiego delle unità delle forze speciali russe (*Vojska Spetsialnogo Naznačenija*, i famosi *spetsnaz*[1]) inquadrate nelle Forze

[1] In Russia vi sono numerosi reparti d'*élite* indicati come *Spetsnaz*, ma che non sono inquadrati alle dipendenze del GRU. In questo saggio prendiamo in considerazione solo quelli alle dipendenze di questa agenzia. Per un approfondimento sui reparti Spetsnaz non impie-

Armate. Dal 2010 la sua denominazione ufficiale è "Direzione Principale" (*Glavnoe Upravlenie*) dello Stato Maggiore Generale, formalmente indicata in forma abbreviata come GU, tuttavia è ancora comunemente nota con l'acronimo GRU.

Il GRU svolge un ruolo di primaria importanza nella politica estera e di sicurezza della Federazione Russa. Negli ultimi anni, sono state attribuite a questa organizzazione alcune delle operazioni di *intelligence* più aggressive poste in atto dalla Russia ed assurte agli onori della cronaca. Si ritiene che l'agenzia abbia contribuito in modo determinante all'occupazione russa della Crimea e nella destabilizzazione dell'Ucraina orientale; sia responsabile del tentativo di assassinio dell'ex ufficiale dell'intelligence russa Sergei Skripal' nel Regno Unito; sia stata l'artefice di interferenze nelle elezioni presidenziali statunitensi del 2016; abbia condotto campagne di disinformazione e di propaganda rivolte contro l'Occidente e sia responsabile, altresì, di alcuni degli attacchi informatici più dannosi a livello globale. Secondo l'*intelligence* americana Mosca sarebbe arrivata ad impiegare il GRU offrendo "ricompense" ai combattenti legati ai talebani per attaccare il personale statunitense in Afghanistan.

Diversi analisti evidenziano che il GRU ha una differente identità organizzativa in relazione al suo duplice *status* di organizzazione di *intelligence* e di organizzazione militare. A partire dalla sua costituzione, inoltre, il GRU ha primeggiato tra i diversi organi di sicurezza russi per risorse e responsabilità. In generale, le altre agenzie di *intelligence* hanno costantemente cercato di avere le stesse missioni e responsabilità del GRU, sovente ingenerando un'intensa concorrenza e, talvolta, una inutile o addirittura deleteria, duplicazione degli sforzi. Tale situazione ha indotto alcuni analisti e ricercatori a sottolineare che la cultura organizzativa peculiare del GRU e la concorrenza con le altre agenzie possono influire sulla sua volontà di condurre operazioni aggressive e spesso sconsiderate, per esaltare l'utilità di questo organo militare di *intelligence* per la *leadership* politica russa.[2] Questo saggio si propone di esaminare le origini, le missioni, le operazioni documentate o riferite del GRU. In primo luogo si sofferma brevemente

gati dal GRU v. N. Cristadoro, *Spetsnaz e corpi paramilitari dei servizi di sicurezza russi. Il controterrorismo sui campi di battaglia*, Il Maglio Edizioni, 2018.

2 Mark Galeotti, *Putin's Hydra: Inside Russia's Intelligence Services*, Policy Brief of the European Council for Foreign Relations, May 11. 2016, p.2.

Emblemi grande e medio (Большая / Средняя эмблема) e patch (Нарукавный знак) della Direzione generale dei servizi segreti (ГУ: Главном разведывательном управлении) dello stato maggiore generale (ГШ: Генерального штаба) delle Forze Armate (ВС: Вооруженных Сил) adottati nel 1997 e 2015- La granata a tre fiamme è il simbolo dello SM generale russo, sovrapposto a quello del GRU sovietico.

sulla storia e sul *background* dell'agenzia, allo scopo di inquadrare il contesto per comprenderne la gli obiettivi e le responsabilità tradizionalmente attribuitegli. Quindi si esamina la struttura organizzativa del GRU; si analizzano le varie missioni che, come detto, spaziano dalla raccolta informativa, al controllo delle unità *spetsnaz*, fino alla pianificazione e condotta di operazioni di *cyberwarfare*. Il saggio si conclude con una breve valutazione delle prospettive future del GRU.

1. Il GRU dalle origini ad oggi

Le origini dell'*intelligence* militare russa possono essere fatte risalire al 1918, sotto Lev Trockij.[3] In maniera simile alle agenzie civili di *intelligence* create dai bolscevichi durante la guerra civile russa, l'*intelligence* militare inizialmente si concentrò sulla protezione del regime dai "controrivoluzionari" attivi all'estero. All'inizio della sua storia, l'organizzazione militare preposta all'attività di *intelligence* venne denominata "Dipartimento di Ricognizione" (*Razvedupravlenie* o *Razvedupr*), nota anche come "Quarto Direttorato" dell'Armata Rossa.[4] Nel tempo, l'attenzione rivolta alla raccolta di informazioni all'estero e al sostegno della

3 Raymond W. LEONARD, «Studying the Kremlin's Secret Soldiers: A Historiographical Essay on the GRU, 1918–1945», *Journal of Military History*, vol. 56, no. 3, 1992, pp. 403–422.

4 Jonathan HASLAM, *Near and Distant Neighbors: A New History of Soviet Intelligence*, Farrar, Straus and Giroux, New York, 2015.

politica estera sovietica è gradualmente aumentata.[5] Le attività dell'agenzia includevano la gestione di risorse *humint*,[6] oltre alla condotta di operazioni note in epoca sovietica come "misure attive" (*aktivnye meroprijatija*) e che comprendevano attività di propaganda, disinformazione e di sabotaggio in territorio straniero. Durante gli anni '20 e '30 del XX secolo, il "Quarto Direttorato" si guadagnò la fama di organizzazione aggressiva e spesso imprudente, dando luogo a numerosi incidenti diplomatici. Già all'epoca del "Quarto Direttorato" la rivalità con le agenzie civili di *intelligence* sovietiche era molto accesa, relativamente alle missioni assegnate, all'influenza esercitata e alle responsabilità attribuite alle diverse organizzazioni.[7] Ad esempio, il fondatore della *Čeka*[8] Feliks Edmundovič Dzeržinskij (1877-1926) si lamentava dell'«irresponsabile attività del Razvedupr, che ci trascina in conflitti con gli Stati vicini»[9]. Lo stretto collegamento del "Quarto Direttorato" con il *Comintern* (l'Internazionale Comunista), attraverso il quale conduceva molte attività e reclutava agenti, creò inoltre degli attriti con il Commissariato del Popolo per gli Affari Esteri dell'Unione Sovietica (il Ministero degli Esteri dell'epoca), proprio a causa delle incaute procedure adottate.

Le continue lotte intestine e la necessità di snellire le operazioni indussero nel 1942 a fondare l'organizzazione oggetto del nostro interesse: la Direzione Principale dell'Intelligence dello Stato Maggiore, nota come GRU. Durante la II Guerra Mondiale, il GRU supervisionò le azioni di sabotaggio, resistenza e guerriglia contro i nazisti.[10] Terminata la guerra, il GRU fu posto sotto il comando diretto dello Stato Maggiore della Difesa. Accanto al "Primo Direttorato Centrale" del KGB, ricevette il compito di condurre operazioni di *intelligence* all'estero sia legali (sotto copertura diplomatica), sia illegali (senza copertura diplomatica, dunque non ufficiali), incentrate principalmente sulla ricerca e l'elaborazione di dati di carattere militare, come quelli relativi alla tecnologia occidentale o la valuta-

5 Raymond W. Leonard, *Secret Soldiers of the Revolution: Soviet Military Intelligence, 1918-1933,* Greenwood Press, Westport (CT), 1999.

6 *Human Intelligence.*

7 Leonard, *Secret Soldiers,* pp. 7, 17-19.

8 La *Čeka*, il cui nome è una contrazione di *Večeka* (ВЧК-VČK), sigla di "Commissione straordinaria di tutte le Russie per combattere la controrivoluzione e il sabotaggio", è stata la prima agenzia dei servizi segreti sovietici, antesignana del celebre KGB.

9 Haslam, *op. cit*., p. 29.

10 David M. Glantz, *Soviet Military Intelligence in War*, Frank Cass, New York, 1990.

zione delle capacità militari strategiche degli avversari.[11] Il GRU, inoltre, fu incaricato di creare unità di forze speciali: quei nuclei di militari che sono diventati noti come *spetsnaz*. Formatisi sull'esperienza sovietica durante la guerra civile russa, sia l'NKVD[12] che il GRU organizzarono l'addestramento di unità specializzate in operazioni di sabotaggio e guerriglia, chiamate *razvedchiki* (letteralmente, "*scout*").[13] Questa iniziativa si rivelò di altissimo valore durante la II Guerra Mondiale, quando i Sovietici ricorsero al massiccio impiego di formazioni partigiane, che necessitavano di un addestramento adeguato per assolvere i compiti loro assegnati. Arriviamo al 1950, anno in cui questa tipologia di combattenti diede origine agli *spetsnaz*, creati per svolgere operazioni di sabotaggio e ricognizione a lungo raggio sul campo di battaglia, mirate specificamente alle strutture di comando e controllo della NATO e ai siti ove erano custoditi gli armamenti nucleari. Durante la Guerra Fredda, gli *spetsnaz* del GRU hanno acquisito una vasta esperienza supportando, addestrando e supervisionando le forze alleate locali in numerosi conflitti.[14] Le unità *spetsnaz* hanno svolto un ruolo chiave nelle invasioni sovietiche dell'Ungheria nel 1956 e della Cecoslovacchia nel 1968. Hanno anche acquisito una significativa esperienza e notorietà durante l'invasione sovietica dell'Afghanistan (1979-1989). In Afghanistan gli *spetsnaz* hanno condotto colpi di mano, operazioni di interdizione areale e imboscate, ma vogliamo ricordarli, in particolare, per la partecipazione all'assalto del palazzo presidenziale a Kabul e all'eliminazione del Presidente Hafizullah Amin (1929-1979). In tale occasione gli uomini del 154° Distaccamento Forze Speciali Indipendente del GRU[15] – il cosiddetto "Battaglione Musulmano" in quanto formato esclusivamente da militari Uzbeki, Tagiki e Turkmeni – operarono al fianco degli *spetsnaz* dei reparti *Grom*, appartenente al "Gruppo Alfa" e *Zenit*, proveniente dall'"Istituto

11 Raymond L. Garthoff, *Soviet Leaders and Intelligence: Assessing the American Adversary During the Cold War*, Georgetown University Press, Washington D.C., 2015, pp. 13-15, 46.

12 Il "Commissariato del popolo per gli affari interni", noto anche con l'acronimo NKVD (*Narodnyj Komissariat Vnutrennich Del*) è stato un dicastero attivo nella Russia sovietica dal 1917 al 1930, successivamente riorganizzato a livello centrale, in Unione Sovietica dal 1934 al 1946. L'organizzazione nacque dalla trasformazione della *Čeka*.

13 Mark Galeotti, *Spetsnaz: Russia's Special Forces*, Osprey Publishing, Oxford, 2015, pp.8-11.

14 Mark Galeotti, *Spetsnaz: Operational Intelligence, Political Warfare and Battlefield Role*, Marshall Center Security Insights, n. 46, February 2020.

15 Vadim Udmantsev, «Боевое крещение 'мусульман'» (Battesimo del fuoco 'musulmano'), *ВПК,* n. 50, 29/12/2004. http://vpk-news.ru.

dei Corsi per Addestramento Avanzato per Ufficiali" (*Kursy Usovershenstvovaniya Ofitserskogo Sostava* - KUOS).[16] *Grom* e *Zenit* erano elementi delle forze speciali alle dipendenze del KGB, dunque non del GRU.

Dopo la dissoluzione dell'Unione Sovietica nel 1991, come è accaduto per il Ministero della Difesa e per gli altri servizi di *intelligence*, anche il GRU si è ritrovato a lottare per il sostegno finanziario e politico in Russia. In particolare, ricordiamo che lo scioglimento del KGB ha dato origine a diverse agenzie di *intelligence*, tra cui le più importanti sono il "Servizio Federale di Sicurezza" (*Federal'naja Služba Bezopasnosti* - FSB) ed il "Servizio Informazioni Estero" (*Služba Vnešnej Razvedki* - SVR). È con queste agenzie che il GRU ha dovuto competere per affermare la sua rilevanza e per mantenere le proprie prerogative sulle missioni.[17]

Comunemente si reputa che in epoca sovietica il KGB fosse l'organizzazione più forte e più temibile dell''U.R.S.S.; in realtà l'esistenza del GRU era talmente tutelata dal segreto che non se ne conobbe l'esistenza fino all'epoca della *perestrojka* e gli stessi segretari del Partito Comunista non potevano accedere al Quartier Generale del GRU senza essere perquisiti. Proprio il fatto di appartenere all'apparato militare anziché a quello politico, fu il punto di forza che consentì a questo servizio segreto di uscire indenne dalle trasformazioni che invece portarono alla scissione del KGB nei servizi di sicurezza interno (FSB) e di raccolta informativa estera (SVR).

Nonostante i massicci esodi di personale e i tagli di bilancio, il GRU ha conservato il suo ruolo di organismo deputato alla raccolta *intelligence* all'estero e la propria autonomia funzionale, restando inquadrato nello Stato Maggiore della Difesa.[18]

Anche gli *spetsnaz* del GRU hanno sofferto pesantemente per i tagli al bilancio e la mancanza di obiettivi chiaramente definiti, in quanto il conflitto con la NATO è diventato altamente improbabile. Molti ufficiali hanno intravisto miglio-

16 Nicola Cristadoro, *Spetsnaz e corpi paramilitari dei servizi di sicurezza russi. Il controterrorismo sui campi di battaglia*, Il Maglio Edizioni, 2018, p. 8.

17 Amy Knight, *Spies Without Cloaks: The KGB's Successors*, Princeton University Press, Princeton, 1996, pp. 119-120.

18 Amy Knight, *This Russian Spy Agency Is in the Middle of Everything*, Daily Beast, August 10, 2018.

ri prospettive in un reimpiego nelle forze aviotrasportate (VDV), che si presentavano come un'unità di risposta rapida più capace ed elitaria rispetto ai propri reparti di appartenenza. Altri ex *spetsnaz* si sono "riciclati" nelle organizzazioni criminali.[19] Nel corso degli anni '90 e 2000 il GRU e le unità *spetsnaz* hanno partecipato ai combattimenti ed all'addestramento delle forze locali leali a Mosca, nelle guerre contro la regione separatista della Cecenia.[20] Durante la guerra con la Georgia del 2008, i discutibili risultati ottenuti dal GRU[21] - che continuava a mantenere la funzione di comando sulle forze speciali - furono segnati da una serie di situazioni imbarazzanti. Nonostante alla fine del conflitto le Forze Armate russe siano risultate vincitrici, non si può dire che abbiano operato in modo sempre efficace ed efficiente. Troppe sono state le carenze nella gestione della catena di Comando e Controllo; è emersa una certa mancanza di coordinamento le diverse branche operative e anche l'accuratezza delle informazioni relative alle forze georgiane è risultata alquanto approssimativa.[22] La raccolta di dati di scarsa qualità ha determinato il bombardamento di aeroporti e di installazioni militari vuote; diversi sono stati gli incidenti per "fuoco amico" e le errate valutazioni sulle capacità e sul morale delle forze georgiane. Le agenzie di sicurezza e di *intelligence* concorrenti del GRU cercarono di trarre vantaggio dall'indebolimento della sua posizione politica. A causa della sua ampiezza e della vastità delle sue aree di missione, in seguito alla guerra georgiana il GRU ha sofferto della mancanza di un ruolo chiaramente definito.[23] Nel 2009, il Direttore del GRU, che ricopriva quell'incarico dal 1997, fu sostituito dal suo vice.[24] Nel 2011, poi, il GRU fu sottoposto a un drastico ridimensionamento, con la riduzione di oltre 1.000 funzionari, molti dei quali mandati in pensione o trasferiti; anche le

19 Graham H. Turbiville, «Organized Crime and the Russian Armed Forces», *Transnational Organized Crime* vol. 1, n. 4, 1995, pp. 57-104.

20 Mark Galeotti, *Spetsnaz: Russia's Special Forces*, pp. 31-35.

21 Tor Bukkvoll, «Russia's Military Performance in Georgia», *Military Review,* vol. 89, no. 6, 2009, pp. 57-62.

22 Ariel Cohen – Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications*, Strategic Studies Institute, Carlisle (PA), 2011.

23 Mark Galeotti, *Putin's Secret Weapon*, Foreign Policy, July 7, 2014. https://foreignpolicy.com.

24 Mark Galeotti, *Korabelnikov Leaves Russian Military Intelligence*, In Moscow's Shadows, April 26, 2009.

attività dell'agenzia all'estero subirono una consistente riduzione.[25]

Le fortune del GRU hanno cominciato a cambiare con la nomina di Igor Sergun al suo vertice nel 2011.[26] Sergun ha contribuito a una rivitalizzazione del prestigio del GRU. A differenza dei suoi predecessori, gli analisti avrebbero considerato Sergun (che aveva un passato come addetto alla difesa e ufficiale dell'intelligence) come un *leader* politicamente astuto in grado di fare pressioni per gli interessi dell'agenzia.[27] Sotto la direzione di Sergun il GRU ha incrementato la politica dell'attuazione di "misure attive" o della condotta di operazioni aggressive come omicidi, controllo delle guerre per procura, sovversione politica e, non ultime, operazioni informatiche.[28]

Il GRU ha svolto un ruolo fondamentale durante l'occupazione della Crimea e il conflitto scoppiato in Ucraina orientale, nel 2014.[29] L'operazione russa in Crimea ha fatto grande affidamento sull'*intelligence* del GRU e sulle unità *spetsnaz* per conquistare punti strategici in tutta la penisola.[30] Il successo del GRU è continuato nelle regioni di Donec'k e Luhans'k, nell'Ucraina orientale, con l'organizzazione e la supervisione delle numerose formazioni paramilitari filo-russe che, perfettamente in linea con i dettami della "Dottrina Gerasimov", conducono la guerra per procura di Mosca contro il governo ucraino.

L'esperienza del GRU nella gestione delle forze speciali e irregolari ha continuato a dimostrarsi utile durante l'intervento della Russia in Siria.[31] In particola-

---

25 Brian Whitmore, *Resetting the Siloviki*, RFE/RL Power Vertical, October 21, 2011.

26 Denis Telmanov, *GRU Headed by Igor Sergun*, Izvestia, December 26, 2011.

27 Roger McDermott, «Russian Military Intelligence: Shaken but Not Stirred», *Eurasia Daily Monitor*, Jamestown Foundation, February 7, 2012; Mark Galeotti, *We Don't Know What to Call Russian Military Intelligence and That May Be a Problem*, War On The Rocks, January 19, 2016; Galeotti, *Putin's Hydra*, p. 13.

28 Galeotti, *Putin's Hydra*, p.7.

29 Charles K. Bartles - Roger McDermott, «Russia's Military Operation in Crimea: Road Testing Rapid Reaction Capabilities», *Problems of Post-Communism,* vol. 61, no. 6, 2014, pp. 46-63; Michael Kofman et al., *Lessons From Russia's Operations in Crimea and Eastern Ukraine*, RAND, 2014.

30 Anton Lavrov, «Russian Again: The Military Operation for Crimea», *Brothers Armed: Military Aspects of the Crisis in Ukraine*, East View Press, Minneapolis (MN), 2015, pp. 157-186.

31 Sarah Fainberg, «Russian Spetsnaz, Contractors, and Volunteers in the Syrian Conflict», *Russie.nei Visions*, IFRI, December 2017; Brian Katz – Nicholas Harrington, *The Military Campaign*, in *Moscow's War in Syria*, ed. Seth G. Jones (CSIS, 2020), pp. 18-40.

re, gli *spetsnaz* si sono dimostrati determinanti nell'addestramento, consulenza delle forze locali filo-governative,[32] nelle tradizionali missioni di ricognizione sul campo di battaglia e nel *targeting*, per il coordinamento degli attacchi aerei condotti sia dai Russi sia dall'aeronautica siriana.[33] Successivamente, senza trascurare quelle che sono le sue attività peculiari, il GRU ha cominciato a investire sempre più risorse in capacità cibernetiche.[34] Lo sviluppo di questo tipo di capacità avrebbe consentito al GRU di operare in un ambiente caratterizzato da confusione e da un approccio tecnologico ai conflitti sempre più marcato.[35] In riferimento alla *information warfare*, la Russia applica una strategia di "basso profilo", indicando sé stessa come una «nobile nazione che applica una postura difensiva in un ambiente caratterizzato da avversari aggressivi».[36] Non è esattamente così. Situazioni di "guerra ibrida", come il conflitto ucraino e la *cyber*-arena in cui tutte le potenze del mondo si combattono quotidianamente, hanno fornito al GRU un'altra occasione per giustificare e dimostrare la sua importanza alla *leadership* politica russa.[37] Negli ultimi anni, sono state scoperte diverse operazioni di *hacking* riconducibili GRU che hanno evidenziato la responsabilità del Cremlino e, di conseguenza, complicato le relazioni diplomatiche.[38] È legittimo domandarsi se le imprudenze che hanno reso possibile l'individuazione delle attività del GRU siano il risultato di incompetenza e dilettantismo.[39] Abbiamo

32 Mark Galeotti, *The Three Faces of Russian Spetsnaz in Syria*, War on the Rocks, March 21, 2016; Thomas Gibbons-Neff, *How Russian Special Forces Are Shaping the Fight in Syria*, Washington Post, March 29, 2016.

33 Anton Lavrov, «Russian Aerial Operations in the Syrian War», *Russia's War in Syria: Assessing Russian Military Capabilities and Lessons Learned*, ed. Robert E. Hamilton, Chris Miller, Aaron Stein, Philadelphia (PA), Foreign Policy Research Institute, 2020, p. 95.

34 Anton Troianovski – Ellen Nakashima, *How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West*, Washington Post, December 28, 2018.

35 Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York, 2019, pp. 237-242; Bilyana Lilly - Joe Cheravitch, «The Past, Present, and Future of Russia's Cyber Strategy and Forces», *12th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, 2020, pp. 140-142.

36 Lilly - Cheravitch, *ibid*., p.148.

37 Andrew Roth, *How the GRU Spy Agency Targets the West, from Cyberspace to Salisbury*, The Guardian, August 6, 2018.

38 Sarah Rainsford, *Have Russian Spies Lost Their Touch?*, BBC, October 6, 2018.

39 Karina Orlova, *Russia's Intelligence Failures*, American Interest, October 10, 2018; Luke Harding, *A Chain of Stupidity: The Skripal' Case and the Decline of Russia's Spy Agencies*,

detto della competizione che ha costantemente caratterizzato i rapporti tra i vari servizi segreti di Mosca e diverse fonti mediatiche suggeriscono che le altre agenzie di sicurezza russe concorrenti del GRU abbiano cercato di sminuirne l'immagine a proprio vantaggio.[40] Per comprendere la natura della "concorrenza" tra i vari servizi speciali, tuttavia, è importante capire alcuni punti fondamentali. In primo luogo, quali siano le contraddizioni negli interessi e negli obiettivi delle diverse organizzazioni dell'*intelligence*, l'intero sistema dei servizi segreti russi si fonda sulla resistenza all'influenza esterna. Quindi, anche se qualcuno nell'SVR fosse tentato di sferrare un colpo al GRU, ciò non potrebbe in alcun modo essere fatto rafforzando le affermazioni occidentali sul coinvolgimento della Russia nel crimine di Salisbury. In questo caso, il desiderio dell'SVR di prendere le distanze dagli eventi non equivale affatto all'intenzione di danneggiare il GRU.[41]

Nel 2016-2018 si sono avvicendati alla testa del GRU i colonnelli generali Igor Dmitrievič Sergun (1955) e Igor Valentinovič Korobov (1956), entrambi deceduti in servizio, ufficialmente per malattia: coincidenza che ovviamente ha indotto i cremlinologi occidentali a supporre faide e purghe, anche se non risultano altri indicatori che il GRU sia caduto in disgrazia.[42]

Nel discorso del novembre 2018 per il Centenario del GRU (di poco successivo al tentato assassinio dell'ex ufficiale del GRU Sergei Skripal' nel Regno Unito) Putin ha ringraziato l'agenzia e ha dichiarato: «In qualità di comandante supremo, ovviamente conosco le vostre capacità che senza esagerare considero uniche, inclusa quella di condurre operazioni speciali».[43]

Sebbene non sia chiaro esattamente come la *leadership* politica russa veda il GRU, le operazioni condotte dall'agenzia e le informazioni disponibili indicano che esso rimane una risorsa preziosa, soprattutto per operazioni aggressive e con un elevato livello di rischio.

The Guardian, June 23, 2020.

40 Tatiana Stanovaya, *GRU Exposure: A Sign of Internal Power Struggles?*, Riddle, October 16, 2018.

41 Stanovaya, *ibid.*

42 Mark Galeotti, *Russia's Military Intelligence Agency Isn't Stupid*, Foreign Policy, September 6, 2018.

43 Tom Balmforth, *Putin Praises Skills of GRU Spy Agency Accused of UK Poison Attack*, Reuters, November 2, 2018.

Capi del GU dal 26 dicembre 2011 a oggi: 5 Igor Dmitrievič Sergun († 3.1.2016); 6 Igor Valentinovič Korobov († 21.11.2018); 7 Igor Olegovič Kostyukov

2. *Struttura organizzativa*

Il Comando dell'apparato di *intelligence* militare russo è situato in *uliza* Grizodubovoj n. 3, nel distretto di Chorošovskij, a Mosca.[44] Attualmente al vertice del GRU vi è l'Ammiraglio Igor Olegovič Kostyukóv,[45] in carica dal 22 novembre 2018. I vertici del GRU rispondono del loro operato al Ministro della Difesa Sergej Kužugetovič Šojgu ed al Capo di Stato Maggiore della Difesa Valerij Vasil'evič Gerasimov e, come detto, mantiene un elevato livello di autonomia operativa. Tra le prerogative dell'agenzia vi è quella di poter riferire direttamente anche al Presidente Putin.[46]

L'*intelligence* militare russa è responsabile della ricerca informativa all'estero attraverso tutte le risorse tipiche di questa attività: *humint*, *cyber*, *imint*[47] (anche satellitare), *sigint*.[48] Svolge attività di analisi e, avvalendosi delle unità *spetsnaz* alle proprie dipendenze, compie missioni di ricognizione e di sabotaggio nelle zone di guerra dove è chiamata ad operare. Questo significa che il GRU

44 President of Russia, *President Vladimir Putin visited the new headquarters of the Russian Armed Forces General Staff Chief Intelligence Directorate (GRU)*, press release, November 8, 2006. http://en.kremlin.ru.

45 TASS, *First Naval Officer Nominated to Head Russia's GRU*, November 22, 2018.

46 Galeotti, *Putin's Hydra*, p. 2.

47 *Imagery Intelligence.*

48 *Signal Intelligence.*

sovrintende ad attività di ricerca dal livello tattico a quello strategico.[49]

Negli ultimi anni il GRU ha incrementato le sue capacità *cyber*, come dimostrato dalle interferenze nelle elezioni in Stati stranieri, da diversi attacchi informatici e da campagne di disinformazione orientate ai Paesi esteri, potenziando il tradizionale apparato *sigint* di cui da sempre si avvale.[50]

In virtù del suo duplice ruolo, il GRU ha una notevole capacità ed esperienza per organizzare forze ed alleanze locali in numerose aree di conflitto, così come di condurre omicidi di elementi "scomodi" o avversari che ricoprano ruoli di rilievo ed altri attacchi ad obiettivi specifici. Nonostante gestiscano operazioni di *intelligence* e l'impiego di forze speciali, non tutti gli Ufficiali e i funzionari del GRU sono in possesso di una formazione o di un *background* specialistici in tali ambiti.[51] È opinione di alcuni analisti che l'abitudine alla supervisione di entrambi i tipi di operazioni ha portato a una cultura di accettazione e di assunzione del rischio molto elevata e tale "spregiudicatezza" contribuirebbe ad una maggiore probabilità di esposizione nello svolgimento delle operazioni.[52]

Naturalmente compiti e organici del GRU sono tutelati da livelli di elevata classifica, tuttavia, sulla base della letteratura disponibile e reputata sufficientemente attendibile,[53] abbiamo ricostruito l'organigramma dell'agenzia e dei relativi compiti delle singole componenti (Figura 1). Il GRU è articolato in quindici

49 Roth, *op. cit.*

50 "Il GRU ha sempre svolto operazioni *sigint* su vasta scala, ma le sue capacità sono state notevolmente incrementate con l'acquisizione delle capacità di intercettazione radio-elettronica di cui disponeva la disciolta "Agenzia Federale Governativa per le Comunicazioni e le Informazioni" (FAPSI), nel 2003"
Gordon Bennet, *FPS and FAPSI – RIP*, Conflict Studies Research Center, Occasional Paper n. 96, p. 4.

51 Mark Galeotti, *Special Troops of GRU Will Be Growing Headache for the West*, Raamoprusland, September 28, 2018.

52 Galeotti, *Putin's Hydra*, p. 2.

53 Jacques Baud, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2004; Congressional Research Service (CRS), *interview with Mark Galeotti*; Viktor Suvorov, *Inside the Aquarium: The Making of a Top Soviet Spy*, MacMillan New York, 1985; Stanislav Lekarev, *Two Types of Russian Intelligence Are Unified*, Nezavisimaya Gazeta, August 31, 2001; Daniil Turovsky, *What Is the GRU? Who Gets Recruited to Be a Spy? Why Are They Exposed So Often?*, Meduza, November 6, 2018; Mark Urban, *The Skripal' Files: The Life and Near Death of a Russian Spy*, Henry Holt and Company New York, 2018; RFE/RL, *On the Trail of the 12 Indicted Russian Intelligence Officers*, July 19, 2020.

La sede del GU-GSVS a Mosca (uliza Grizodubovoj)

"direttorati", di cui quattro orientati ad attività mirate ad aree geografiche del pianeta e undici organizzati per l'assolvimento di specifiche missioni.

a. Direttorati regionali

1° Unione Europea;

2° Continente Americano, Regno Unito, Australia, Nuova Zelanda;

3° Asia;

4° Africa e Medio Oriente.

b. Direttorati per missioni specifiche

5° *intelligence* militare (forze terrestri, aeree e navali);

6° *sigint*. Anche le attività *cyber* sono condotte da questo direttorato. Al suo interno, ad esempio, sono collocate le unità 21165 e 74455, deputate ad azioni di *cyber-attack* e di cui ci occuperemo più avanti;

7° *intelligence* sulla NATO;

8° gestione "affari speciali" (impiego degli *spetsnaz*);

9° analisi tecnologie militari straniere;

10° analisi della gestione dell'economia e della produzione bellica dei paesi stranieri;

11° dottrine e armamenti strategici;

12° *Information Warfare*;

13° *intelligence* spaziale;

14° intelligence tecnico-operativa;

15° relazioni con l'estero.

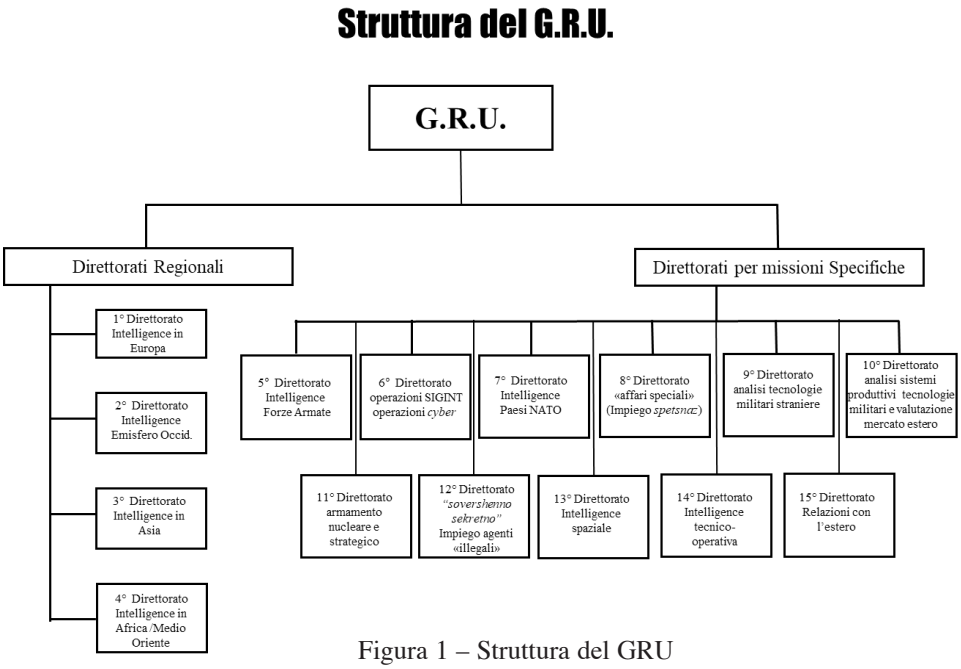

Figura 1 – Struttura del GRU
(autore: N. Cristadoro)

3. Relazioni con le altre agenzie di intelligence russe

La ripartizione e spesso, la "sovrapposizione" di incarichi tra le diverse agenzie di intelligence russe non facilita i rapporti intercorrenti tra le stesse e talvolta sfocia in veri e propri conflitti di competenza.[54] Il GRU opera insieme al Servizio Informazioni Estero (SVR), al Servizio Federale di Sicurezza (FSB) e al Servizio Federale di Protezione *(Federalnaya Sluzhba Okhrani - FSO)*. Il GRU e l'SVR sono le principali agenzie di *intelligence* della Russia responsabili della raccolta di *intelligence* straniera.

Come abbiamo visto, l'attività del GRU è indirizzata 24 ore su 24 all'acquisizione di informazioni di livello strategico-operativo relative alle potenzialità militari di tutti i Paesi, in particolare di quelli membri della NATO. Lo SVR, invece, è l'agenzia che ha ereditato i compiti del Primo Direttorato Centrale del

54 Brian D. Taylor, *State Building in Putin's Russia: Policing and Coercion After Communism* Cambridge University Press, Cambridge, 2011.

KGB, in epoca sovietica deputato allo spionaggio verso l'estero in tutti i settori: politico, economico, sociale, industriale, scientifico.

Abbiamo anche detto in precedenza che le agenzie competono tra loro per maggiori responsabilità, *budget* e influenza politica, spesso a scapito di altre agenzie.[55] Questo ambiente competitivo spesso contribuisce a sforzi di *intelligence* non coordinati e duplicati.[56]

Nondimeno, numerosi sono i problemi interni a ciascun "servizio" dovuti a situazioni di criminalità e corruzione, come ben documentato dalla studiosa russa Tatiana Stanovaya relativamente ai reati commessi da alcuni ufficiali dell'FSB: Dmitry Frolov, ex vicedirettore del Dipartimento per i Crimini Finanziari ("Dipartimento – K"), il suo assistente Andrey Vasilyev ed il loro collega Kirill Cherkalin. Il referente di questi funzionari sarebbe il Generale Ivan Tkachev, anch'egli figura di spicco dell'FSB. Quest'ultimo risulta collegato ai traffici dell'oligarca Igor Sechin, a sua volta ex militare e funzionario del GRU.[57]

L'FSB è responsabile del controspionaggio, dunque di un'attività prevalentemente rivolta all'interno della nazione. Questo servizio, tuttavia, ha cercato di estendere la propria influenza nell'attività di *intelligence* all'estero e nelle operazioni internazionali, in particolare negli stati post-sovietici confinanti con la Russia.[58] Tale atteggiamento ha causato, come era presumibile, degli attriti significativi in seno alla comunità dell'*intelligence* russa, in particolare con il GRU e lo SVR, che considerano la raccolta informativa estera una loro responsabilità primaria.[59] L'FSO, infine, fornisce una sintesi di ciò che accade all'interno dell'*élite* nazionale.

---

55 Peter Reddaway, *Russia's Domestic Security Wars: Putin's Use of Divide and Rule Against His Hardline Allies*, Palgrave Pivot, London, 2018; Joss I. Meakins, «Squabbling Siloviki: Factionalism Within Russia's Security Services», *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 2, 2018, pp. 235-270.

56 Mark Galeotti, *The Intelligence and Security Services and Strategic Decision-Making*, Marshall Center Security Insights, n. 30, May 2019.

57 Tatiana Stanovaya, *Why the Kremlin Can't Keep Its Chekists in Check*, Riddle, July 25, 2019. https://www.ridl.io.

58 Mark Galeotti, *The Spies Who Love Putin*, Atlantic, January 17, 2017.

Per un approfondimento sulle attività delle forze speciali dipendenti dal FSB in Cecenia v. Nicola Cristadoro, *Spetsnaz e corpi paramilitari dei servizi di sicurezza russi. Il controterrorismo sui campi di battaglia*.

59 Andrei Soldatov, *Russian foreign intelligence might be in for a mor prominent political role*, Raamoprusland, May 24, 2019.

Forte di circa 20.000 elementi, Il Servizio di Protezione Federale supervisiona le comunicazioni governative di alto livello, gestisce e protegge i centri di comando sotterranei, mantiene lo speciale sistema di metropolitana che collega le strutture chiave del Governo nella zona di Mosca e protegge le altre strutture strategiche, oltre ai velivoli ed ai treni speciali a disposizione delle alte cariche dello Stato (i treni sono a disposizione anche delle forze missilistiche strategiche). A partire dalla fine del 1960 diverse migliaia di dirigenti di ministeri, dipartimenti e redazioni delle principali testate giornalistiche sono stati collegati tramite una rete telefonica automatizzata gestita dal Governo (definita "linea calda"). Tra le prerogative dell'organizzazione vi sono il diritto di condurre ricerche, controllare i documenti di identità, fare arresti, dare ordini ad altri organi dello Stato, effettuare intrusioni nei locali senza il consenso dei proprietari, vietare l'accesso ai luoghi pubblici e reclutare e utilizzare informatori segreti. Le leggi sul Servizio di Protezione Federale attribuiscono all'organizzazione un potere non inferiore a quello dell'FSB o del Ministero degli Interni. Al FSO è consentito di condurre la sorveglianza e le ricerche per monitorare tutte le comunicazioni e di condurre attività clandestine, senza alcuna autorizzazione da parte di un tribunale. Una delle unità più importanti del FSO è il Reggimento del Cremino. Il 7 agosto 2004 nell'organico del FSO è stato inserito il Servizio Speciale Russo per le Comunicazioni e le Informazioni (*Sluzhba spetsial'noy svyazi i informatsii, Spetssvyaz' Rossii - Spetssviaz*),[60] le cui funzioni sono assimilabili a quelle della *National Security Agency* statunitense.

Abbiamo detto del grande potere esercitato dal GRU in epoca sovietica, anche sulla compagine governativa dell'U.R.S.S.. Allo stato attuale, tuttavia, Mark Galeotti indica una deriva dell'autocrazia putiniana in quella che definisce "spettrocrazia" ("*spookocracy*"), che consisterebbe nella crescente attitudine del Presidente russo a circondarsi di figure compiacenti individuate tra i "compagni" del passato, piuttosto che in consiglieri dotati di onestà intellettuale e sinceri nelle opinioni espresse. Anche le relazioni con i servizi di *intelligence* subirebbero pesantemente questa influenza negativa. Infatti, nonostante il GRU possa infor-

60 Il Servizio Speciale Russo per le Comunicazioni e l'Informazione è un'agenzia di *intelligence* responsabile della raccolta e dell'analisi di dati in materia di *sigint* e, in generale, delle comunicazioni effettuate dai Paesi stranieri, oltre alla protezione delle comunicazioni e dei sistemi di trasmissione nazionali, con particolare riguardo agli apparati ed ai codici "cripto".

Discorso di Putin per il 100° anniversario del GRU

mare direttamente il Presidente, non ha lo stesso livello di accesso diretto dell'SVR, dell'FSB o dell'FSO e, in virtù di quanto sopra descritto, oggi come oggi dunque non avrebbe più quel potere che ha avuto in passato.[61] Pertanto, allo stato attuale, l'influenza del GRU sembrerebbe dipendere dalla capacità del suo capo di sviluppare buone relazioni personali con la *leadership* politica russa.[62]

4. I ruoli del GRU e dell'SVR nell'attività di intelligence all'estero

Il GRU e l'SVR condividono la responsabilità della raccolta informativa all'estero. Sotto questo aspetto, possiamo individuare diversi settori di sovrapposizione tra il GRU e l'SVR. Il GRU, con i primi quattro "direttorati" della sua organizzazione, opera rispettivamente nei paesi europei, in quelli dell'emisfero occidentale (la piattaforma continentale americana), in Asia e nelle aree africana e mediorientale. L'SVR espleta analoghe mansioni attraverso il "Direttorato R", con i suoi "dipartimenti" capillarmente distribuiti in corrispondenza di tutte le nazioni del pianeta.

61 Mark Galeotti, *Spooks in the Kremlin*, Foreign Policy, April 27, 2019.
62 Galeotti, *ibid.*

Una delle peculiarità della raccolta informativa attuata tanto dal GRU, quanto dal SVR, è il ricorso ad agenti "illegali" (*sovershenno sekretno*),[63] cioè privi della copertura diplomatica che tutela le spie impiegate all'estero in caso di individuazione e cattura. La gestione della rete informativa di entrambi i servizi, infatti, contempla l'impiego non solo dei funzionari diplomatici sul territorio, ma anche individui ben inseriti nel tessuto sociale di un Paese, sotto falsa identità o con coperture non ufficiali:[64] per quanto riguarda il GRU si tratta di attività riconducibili verosimilmente alle operazioni *top secret* del 12° Direttorato (*Information Warfare*), mentre per l'SVR gli agenti operano alle dipendenze del "Direttorato S", incaricato della formazione degli stessi e delle attività di raccolta clandestina.

Gli agenti del GRU sono addestrati presso l'Accademia Militare Diplomatica dello Stato Maggiore della Difesa.[65] In ogni ambasciata gli agenti del GRU e dell'SVR operano separatamente, ognuno con strutture di comando dedicate.[66]

L'attività del GRU è istituzionalmente orientata alla ricerca informativa su dati rilevanti riferiti alle capacità delle forze armate straniere in termini di consistenza numerica, tipologia di armamenti ed equipaggiamenti, procedure tecnico-tattiche, *leadership* e procedure decisionali, ricerca e sviluppo nella tecnologia militare. Questi obiettivi, tuttavia, non precludono la raccolta informativa su aspetti di carattere politico, di norma compito dell'SVR.[67]

È interessante l'osservazione dell'analista Mark Galeotti, secondo cui

> «Le operazioni di ricerca informativa in Russia non solo sono molto attive, ma anche estremamente professionali. L'assegnazione dei compiti, tuttavia, fa meno impressione. Sebbene l'SVR e il GRU abbiano le idee chiare sui segreti militari e tecnologici di cui intendono appropriarsi, i loro

63 "Secondo una valutazione occidentale del GRU fatta dalla Reuter, il GRU ha un programma a lungo termine per impiegare spie "illegali" - quelle che lavorano senza copertura diplomatica e che vivono per anni sotto un'identità fittizia per ordine di Mosca. La valutazione recita: (il GRU) "ha un programma a lungo termine di "illegali" riservati ai compiti più sensibili o che non devono essere ammessi, nello spettro delle operazioni del GRU".
Guy Faulconbridge, *What is Russia's GRU military intelligence agency?*, Reuters, 05/10/2018. https://www.reuters.com.

64 Turovsky, *What Is the GRU?*

65 Turovsky, *What Is the GRU?*

66 Urban, *op. cit.*

67 Amie Ferris-Rotman – Ellen Nakashima, *Estonia Knows a Lot About Battling Russian Spies, and the West Is Paying Attention*, Washington Post, November 1, 2018.

obiettivi politici a volte appaiono ingenui.»[68]

Questa tendenza potrebbe essere indicativa di una scarsa comprensione dei sistemi politici democratici.

I recenti arresti di agenti del GRU illustrano il livello di attività dell'organizzazione. Il rapporto annuale del 2019 del Servizio di Intelligence Estero estone, ad esempio, riferisce della scoperta di cinque agenti del GRU ed otto del FSB operativi in Estonia dal 2014 al 2018.[69] Nel 2020, tra gli agenti del GRU individuati vi è un ufficiale delle forze armate francesi in servizio presso il Comando della NATO di Napoli[70] e un ufficiale in pensione dell'esercito austriaco,[71] nonché un ex ufficiale delle forze speciali statunitensi.[72]

Per quanto riguarda, poi, le operazioni svolte delle forze più o meno regolari che attualmente agiscono nei vari teatri di interesse strategico per la Russia di Putin, l'attività di spionaggio sviluppata dai due servizi può essere ragionevolmente considerata come un'indispensabile premessa alle stesse. GRU e SVR risulta che siano stati - e che verosimilmente lo siano tuttora - attivamente impegnati in Siria. Nel dicembre 2012 la pagina in inglese[73] del portale *website* "Kavkaz Center" (Centro del Caucaso),[74] riportava l'arresto della giornalista ucraina Ankhar Kochneva da parte dell'"Esercito Siriano Libero", organizzazio-

68 Galeotti, *Putin's Hydra*, p. 7.

69 Michael Weiss, *The Hero Who Betrayed His Country*, Atlantic, June 26, 2019; Estonian Foreign Intelligence Service, *International Security and Estonia*, Annual Report, 2019, pp. 45-46.

70 Anais Ginori, *Breccia russa nell'esercito francese: arrestato un ufficiale di stanza alla Nato in Italia*, La Repubblica, 30/08/2020; Victor Mallet, *French Military Officer Held on Suspicion of Spying*, Financial Times, August 30, 2020.

71 RFE/RL, *Retired Austrian Army Colonel Found Guilty of Spying for Russia*, June 10, 2020.

72 U.S. Department of Justice, *Former Army Special Forces Officer Charged in Russian Espionage Conspiracy*, press release, August 21, 2020.

73 *Free Syrian Army warns on forthcoming attacks on Russian targets in Syria*, Department of Monitoring Kavkaz Center, 14/12/2012. www.kavkazcenter.com.

74 Il *Kavkaz Center* (Centro del Caucaso) è un sito *web* privato con lo scopo di essere "un'agenzia internet cecena indipendente, internazionale ed islamica". La missione dichiarata del sito è quella di riferire eventi relativi alla Cecenia e "fornire alle agenzie giornalistiche internazionali *news-letters*, informazioni ed assistenza per svolgere un'attività giornalistica indipendente nel Caucaso". Dalla sua attivazione ha diramato opinioni in supporto dell'indipendenza della Repubblica Cecena dell'Ichkeria e, successivamente dell'Emirato Caucasico e dei *mujahideen* in tutto il mondo. Il sito è pubblicato in cinque lingue: inglese, arabo, ucraino, russo e turco.

ne paramilitare ostile al regime di Bashar al-Assad. La giornalista veniva ripetutamente indicata come spia al servizio del SVR ed i toni usati nei confronti della Russia erano pesanti, pregni di disprezzo per quelli che venivano reiteratamente ed in modo piuttosto confuso, definiti "banditi" del KGB, del FSB, del SVR, del GRU … di tutti i servizi segreti russi, per farla breve, presenti e passati. È risaputo che il portale è apertamente ostile alla politica di Mosca ed è orientato alla propaganda *jihadista*, tuttavia, al di là della veridicità o meno delle accuse mosse alla giornalista e della funzione marcatamente propagandistica del sito, non si può negare la massiccia ingerenza dei servizi segreti militari e di sicurezza del Cremlino nello scenario siriano.

In particolare, il GRU è l'agenzia di *intelligence* responsabile dell'impiego operativo di tutte le forze speciali (*spetsnaz*) impiegate da Mosca e nel teatro siriano con compiti di "consulenza militare" e, soprattutto, in supporto al *targeting* effettuato delle forze aeree protagoniste della campagna in sostegno del governo di Assad. É certa la partecipazione del GRU all'invasione della Crimea e nella campagna organizzata in supporto ai movimenti separatisti filo-russi nel Donbass, in Ucraina. Gli *spetsnaz* delle unità dipendenti dal GRU possono essere annoverati anche tra i famosi "omini verdi" che, senza insegne di riconoscimento sulle uniformi, hanno operato in Crimea e nel Donbass, regioni dell'Ucraina tuttora al centro di conflitti e dispute che influenzano pesantemente i rapporti tra la Russia e l'Occidente, in particolare quelli con l'Europa.

La presenza del GRU e dell'SVR è ampiamente tracciabile anche in Africa, dalla Libia, all'Egitto, dalla Repubblica Centrafricana, fino al Sudan; in Venezuela a sostegno del governo di Nicolas Maduro ed anche le rivendicazioni e la militarizzazione di ampie aree che si affacciano sul Mar Glaciale Artico probabilmente vedono il coinvolgimento degli operatori del GRU e del SVR.

5. Il GRU e l'impiego degli spetsnaz[75]

Soffermiamoci, adesso, sull'8° Direttorato, incaricato dell'impiego degli *spetsnaz* nelle loro missioni all'estero.

75 Il presente capitolo è basato su un estratto del testo dell'autore sulla "Dottrina Gerasimov": v. Nicola Cristadoro, *La Dottrina Gerasimov*, La Libellula, Tricase (LE), 2018, pp. 131-135.

Distintivi delle brigate autonome spetsnaz (отдельная бригада специального назначения) 2a, 3a, 14a 16a 22a e 24a. Tranne la 2a e la 24a, le altre hanno il titolo "della guardia" (гвардейская). La 14a ha sede nel Distretto Militare (военный округ) dell'Estremo Oriente (КДВО) e la 22a in quello del Caucaso Sett. (СКВО)

Il GRU, notoriamente, è un'organizzazione con la propensione ad assumersi rischi elevati, in cui anche le attività di *routine* prevedono il ricorso ad agenti *non-ortodossi* per operazioni *non-ortodosse*. É prassi normale che, per la condotta delle proprie operazioni si avvalga, dell'operato di "signori della guerra" locali, di mercenari e, non di rado, di malavitosi appartenenti alla criminalità organizzata. Gli *spetsnaz*, tuttavia, rimangono l'arma più importante di cui il GRU dispone e, in prospettiva, continueranno ad esserlo.

Attualmente esistono sette brigate regolari *spetsnaz* delle Forze Terrestri, note come Brigate Indipendenti per Incarichi Speciali (*Otdel'naja Brigada Special'nogo Naznačenija* - OBrSpN), cui si aggiungono la 100a Brigata, il 25° Reggimento Indipendente per Incarichi Speciali di Stavropol (*Otdel'nyj Polk Special'nogo Naznačenija* - OPSpN). Ogni Brigata inquadra due o più Distaccamenti Indipendenti per Incarichi Speciali (*Otdel'nyj Otryad Special'nogo*

Naznačenija - OOSpN), che sono equiparabili a reggimenti con un organico di circa 500 uomini. Queste unità differiscono leggermente le une dalle altre in termini di forza organica, equipaggiamento ed addestramento, in base alle esigenze locali. Le Brigate sono le seguenti:

- 2a OBrSpN (Promešicy, Pskov Oblast');
- 3a OBrSpN (Tol'jatti);
- 10a OBrSpN (Mol'kino);
- 14a OBrSpN (Ussurijsk);
- 16a OBrSpN (Tambov);
- 22a OBrSpN (Stepnoj, Rostov Oblast');
- 24a OBrSpN (Irkutsk).

La 100^ Brigata è un'unità operativa a pieno titolo, tuttavia si occupa principalmente di sperimentare gli equipaggiamenti ed i sistemi d'arma di nuova adozione, nonché di provare le tattiche di nuova concezione. Il personale di questa unità è stato il primo ad utilizzare la nuova tenuta da combattimento "Ratnik", poi distribuita in tutti i reparti.

La 100^ Brigata ed il 25° OPSpN sono stati creati in occasione dei Giochi Olimpici invernali di Sochi nel 2014, manifestamente per fornire ulteriore sicurezza all'evento. I giochi olimpici invernali, infatti, con la minaccia del terrorismo sempre incombente sull'evento, fornirono la giustificazione per un significativo rinforzo degli *spetsnaz* e, in tale occasione, tutti i loro reparti furono portati a pieno organico.

Un altro reparto sotto comando operativo del GRU è il 45° Reggimento da Ricognizione Indipendente delle Guardie (OPSpN VDV), reparto delle Truppe aviotrasportate di stanza a Kubinka, specializzato per operazioni in profondità dietro le linee nemiche.

Non vanno dimenticate, infine, le unità per operazioni speciali della Marina Militare, genericamente indicate come "uomini-rana" nella divulgazione dei *mass-media*, denominati Distaccamento Navale da Ricognizione per Incarichi Speciali (*Otdel'nyj morskoj razvedyvatel'nij punkt Special'nogo Naznačenija* – OmrpSpN):

- 442° OmrpSpN (Flotta del Pacifico);
- 420° OmrpSpN (Flotta del Nord);

- 431° OmrpSpN (Flotta del Mar Nero);
- 561° OmrpSpN (Flotta del Baltico).

L'addestramento e le peculiarità di impiego di queste unità le rende simili agli *U.S. Seals* ed al reparto israeliano *Shayetet 13*.[76]

Esistono altre unità che hanno le stesse caratteristiche degli *spetsnaz*, sebbene inquadrate sotto Comandi differenti: alcune compagnie di *razvedchiki* (scouts), appartenenti ad unità quali la 200a Brigata Artica Motorizzata Indipendente di Pečenga (sul confine con la Norvegia), possono essere considerate *spetsnaz* per i compiti ad esse devoluti.

Alcune Brigate sono oggi totalmente professionalizzate, mentre altre hanno il 20-30 % di coscritti. Anche i professionisti, comunque, non sono tutti in possesso di una particolare esperienza, in quanto circa la metà di essi sono in servizio per la prima (e spesso l'unica) volta con una ferma triennale, attirati dalla paga e dalle condizioni di vita migliori per la ferma prolungata. Di conseguenza, potrebbero aver maturato solo un anno o due di esperienza. Sforzi notevoli sono stati compiuti per rendere gli *spetsnaz* una forza basata tutta su personale volontario, nonostante i tempi-limite di volta in volta imposti per raggiungere tale obiettivo (nel 1999, nel 2003 e nel 2013) siano trascorsi senza che si sia verificato alcun cambiamento.

Questo può spiegare come mai la maggioranza degli *spetsnaz*, sebbene rappresentino indubbiamente un'*élite* a confronto del grosso delle forze terrestri russe, non possono essere considerati forze speciali di prima grandezza. Per certi aspetti, la gran parte degli *spetsnaz* attuali è assimilabile ai *Rangers* statunitensi, praticamente forze di intervento rapido basate su reparti di fanteria leggera in possesso di un buon livello di addestramento. Si calcola che vi siano circa 17.000 uomini appartenenti alle forze speciali. Sono molti, troppi in una galassia già di per sé variegata e confusa quale è quella delle Forze Armate russe e, sicuramen-

76 *Shayetet 13* ("Flottiglia" 13), è un'unità di forze speciali della Marina Militare israeliana, tra le più segrete unità militari d'Israele. E' specializzata in incursioni terrestri portate dal mare, operazioni controterrorismo, raccolta intelligence marittima, sabotaggio, recupero di ostaggi, abbordaggio. L'unità è addestrata per svolgere non solo operazioni marittima, ma anche sulla terraferma ed aeree. I militari di leva che si offrono volontari per prestare servizio nel *Shayetet 13* devono sottoscrivere una ferma di quattro anni e mezzo, diversamente dai loro coscritti il cui servizio obbligatorio è di 36 mesi. L'unità è nota col soprannome di "Gente del Silenzio".

te un tale numero di individui non possiede i requisiti normalmente necessari per essere considerato un militare delle forze speciali. Paradossalmente, gli *spetsnaz* degni di essere considerati tali sono pochi e sono, per lo più, alle dipendenze dei servizi di sicurezza (FSB, SVR) e del Ministero degli Affari Interni *(Ministerstvo Vnutrennich Del* - MVD).

Il Generale Gerasimov, Capo di Stato Maggiore della Difesa, vede le forze speciali come componente critica della guerra "ibrida", per via della loro abilità ad operare come "moltiplicatore di forza", in linea di massima clandestinamente. Nell'articolo che lo ha reso celebre[77] e che ha decretato la definizione di una dottrina a lui attribuita, egli afferma:

> «Le azioni asimmetriche sono diventate uno strumento di uso comune, permettendo di neutralizzare i vantaggi nemici in un conflitto armato. Nel novero di queste azioni deve contarsi l'uso di forze per operazioni speciali e di opposizioni interne per creare un fronte operativo permanente nell'intera estensione del territorio del paese nemico, così come azioni mediatiche: strumenti e mezzi che sono tutti in corso di costante perfezionamento.»
>
> «Tutto questo è realizzato con mezzi militari a carattere occulto, inclusa la realizzazione di azioni di guerra delle informazioni e le azioni delle forze speciali. L'uso manifesto della forza (per la maggior parte sotto le mentite spoglie del peacekeeping e della gestione delle crisi) è riservato solo ad una certa fase, principalmente per il conseguimento del successo finale nel conflitto.»

In sostanza, Gerasimov è convinto che le operazioni delle forze speciali nella guerra "ibrida" siano lo strumento militare più efficace. Diversamente dalle forze convenzionali, la natura clandestina e le ridotte dimensioni conferiscono a questi reparti una maggiore flessibilità operativa; le forze convenzionali, anche quando supportate da un'efficace campagna *info-ops*, sono in qualche modo limitate nel loro impiego. Sebbene le forze speciali operino su scala ridotta rispetto alle forze convenzionali, hanno il vantaggio di poter agire al di fuori dei vincoli politici cui le forze convenzionali devono sottostare.

77 Valerij Vasil'evič Gerasimov, «Ценность Науки в Предвидении» (Il valore della scienza nella previsione), *Corriere Militare-Industriale*, a cura dell'Accademia Russa di Scienze Militari, 23/02/2013.

Da sinistra a destra: il Capo di stato Maggiore della Difesa Gen. Gerasimov, il Presidente Putin, il Ministro della Difesa Šojgu e il Direttore del GRU Amm. Kostyukóv (foto: Sergej Kanev - east2w)

6. Il GRU e le operazioni "non – ortodosse". L'Unità 29155.

Il GRU e gli spetsnaz hanno maturato un'esperienza significativa nella creazione e nella gestione di forze alleate locali che operino in favore del governo russo nei vari teatri operativi in cui Mosca ha attivato conflitti di prossimità, in modo da non rendere ufficiale l'intervento del Cremlino in tali teatri. In perfetta aderenza a quanto prefigurato nella "Dottrina Gerasimov", sovente queste forze sono costituite da una rete che vede interagire elementi della criminalità organizzata, "signori della guerra" locali, gruppi ribelli e paramilitari che, su base prevalentemente etnica, operano in nome della "Grande Madre Russia". Nella maggior parte dei casi il personale degli *spetsnaz* svolge incarichi di supervisione e addestramento, agevolando la creazione di nuove unità direttamente subordinate al GRU. Questo sistema consente al GRU un maggiore controllo diretto nelle guerre per procura e incrementa la sua possibilità di esercitare pressioni sui politici locali.

Vogliamo ricordare che durante la 2a Guerra Cecena (1999-2009) il GRU – unitamente ad altre agenzie, come l'FSB – ha gestito diverse unità paramilitari cecene filo-russe, che hanno dimostrato di essere molto efficaci contro i ribelli ceceni.[78] Tra queste, le unità più note sono i Battaglioni *Zapad* e *Vostok*, che nel 2008 hanno anche partecipato al conflitto tra Russia e Georgia.[79] Durante l'invasione russa dell'Ucraina nel 2014, il GRU ha ampiamente sfruttato la propria esperienza nella gestione delle guerre per procura; diverse fonti medianiche hanno riferito della presenza del Battaglione *Vostok* – ricostituito dopo la smobilitazione avvenuta nel 2008 - nell'area del Donbass, nonché dell'identificazione dell'ufficiale del GRU Oleg Ivannikov, indicato come responsabile del trasporto del sistema contraereo con cui è stato abbattuto il volo di linea delle *Malaysian Airlines*, nel 2014.[80] Non ultime, risulta che le compagnie militari private russe impiegate sia in Ucraina, sia in Siria, compreso il "Gruppo Wagner", abbiano stretti legami con il GRU.[81]

Abbiamo visto come il GRU sia dotato di capacità militari che consentono a questa struttura di effettuare attacchi su obiettivi specifici all'estero, ritenuti di elevato valore. Un altro aspetto, peculiare di questa organizzazione particolarmente degno di interesse riguarda la sua implicazione in numerosi omicidi, tentati e riusciti, ed in altrettanti "attacchi mirati". Alcuni di questi attacchi sono stati scoperti a causa degli errori commessi da operatori imprudenti o poco brillanti, che hanno portato ad accuse di incompetenza nei confronti del GRU.[82] Condividiamo l'ipotesi formulata da alcuni analisti, secondo cui lo scopo di alcuni degli attacchi mirati effettuati sia più quello di inviare un messaggio forte e chiaro agli avversari dell'attuale *leadership* politica russa, piuttosto che nascon-

78 Emil A. Souleimanov, *An Ethnography of Counterinsurgency: Kadyrovtsy and Russia's Policy of Chechenization*, Post-Soviet Affairs, vol. 31, n. 2, 2015, pp. 91-114.

79 Tomáš Šmíd - Miroslav Mareš, «Kadyrovtsy: Russia's Counterinsurgency Strategy and the Wars of Paramilitary Clans», *Journal of Strategic Studies*, vol. 38, n. 5, 2015, pp. 650-677.

80 Claire Bigg, *Vostok Battalion, a Powerful New Player in Eastern Ukraine*, RFE/RL, May 30, 2014; Andrew Roth, *A Separatist Militia in Ukraine with Russian Fighters Holds a Key,* New York Times, June 4, 2014; Bellingcat, *MH17 - Russian GRU Commander 'Orion' Identified as Oleg Ivannikov*, May 25, 2018. https://www.bellingcat.com.

81 Andrew S. Bowen, «Russian Private Military Companies (PMCs)», *Congressional Research Service*, In Focus IF11650, September 16, 2020.

82 Bellingcat, *305 Car Registrations May Point to Massive GRU Security Breach*, October 4, 2018. https://www.bellingcat.com.

dere il ruolo che questa avrebbe nell'organizzazione degli stessi.[83] In tal caso, l'esposizione del GRU e degli altri servizi non sarebbe un fallimento, quanto piuttosto un efficace vettore per trasmettere il messaggio della capacità e della volontà di Putin di colpire i suoi oppositori ovunque essi cerchino rifugio.[84]

Uno degli omicidi più noti e di alto profilo attribuiti al GRU è avvenuto nel 2004, quando l'ex presidente separatista ceceno Zelimkhan Yandarbiyev e suo figlio di 13 anni sono stati uccisi in un attentato con un'autobomba in Qatar, dove vivevano in esilio.[85] In quell'occasione il Qatar ha condannato due agenti russi per l'omicidio, mentre un terzo è stato rilasciato a causa del suo *status* di primo segretario dell'ambasciata russa, protetto dall'immunità diplomatica.[86] Secondo quanto riferito, gli uomini sarebbero stati agenti del GRU. Hanno ottenuto di essere rimpatriati in Russia per scontare la pena, ma al loro rientro sono scomparsi nel nulla.[87]

Nell'ambito della struttura del GRU le operazioni "non – ortodosse" sarebbero una prerogativa della cosiddetta "Unità 29155". Si tratta di un'unità d'*èlite* incaricata di condurre operazioni su obiettivi di elevato profilo, compresi omicidi di personalità di rilievo,[88] fuori dai confini della Russia. Si ritiene che l'unità sia operativa dal 2008, ma la sua esistenza è nota solo dal 2019.[89] L'unità risulta alle dipendenze del Centro per Operazioni Speciali *Senezh* (dal nome del lago vicino a cui sorge il Centro), di stanza presso la cittadina di Solnečnogorsk (*'oblast* di Mosca) e un ulteriore elemento che conferma la sua natura operativa è la notizia che il Comando dell'unità sarebbe situato presso il 161° Centro di Addestramento Specialisti per Incarichi Speciali, una struttura per l'addestramento degli *spetsnaz*.[90] Nel 2021 risulta ancora al vertice dell'agenzia il Maggior Generale

83 David V. Gioe - Michael S. Goodman – David S. Frey, «Unforgiven: Russian Intelligence Vengeance as Political Theater and Strategic Messaging», *Intelligence and National Security*, vol. 34, n. 4, 2019, pp. 561-575.

84 Galeotti, *Russia's Military Intelligence Agency Isn't Stupid*.

85 Nick Paton Walsh, *Top Chechen Separatist Dies in Qatar Bomb Blast*, The Guardian, February 13, 2002.

86 Steven Lee Myers, *Qatar Court Convicts 2 Russians in Top Chechen's Death*, New York Times, July 1, 2004.

87 Sarah Rainsford, *Convicted Russia Agents "Missing"*, BBC, February 17, 2005.

88 Michael Schwirtz, *Top Secret Unit Seeks to Destabilize Europe, Security Officials Say*, The New York Times, October 8, 2019

89 Michael Schwirtz, *How a Poisoning in Bulgaria Exposed Russian Assassins in Europe*, The New York Times, December 22, 2019.

90 Schwirtz, *Top Secret Unit Seeks to Destabilize Europe, Security Officials Say*.

Andrei Vladimirovich Averyanov, un ex *spetsnaz*, così come proviene dagli *spetsnaz* Anatoliy Vladimirovich Chepiga, colonnello del GRU sospettato del tentativo di avvelenamento di Sergei Skripal' e di sua figlia nel 2018, a Salisbury. Chepiga nel 2017 era presente alle nozze della figlia di Averyanov[91] il che dimostra, quantomeno, il legame esistente tra i due ufficiali dell'agenzia. Diversi magistrati e giornalisti sostengono che l'Unità 29155 abbia partecipato a diversi atti ostili portati in territorio europeo negli ultimi anni. Tra questi sono indicati:

- l'invasione e l'occupazione della Crimea nel 2014;
- l'avvelenamento del mercante d'armi bulgaro Emilian Gebrev nel 2015;[92]
- il tentato colpo di stato nel 2016 per rovesciare il Primo Ministro del Montenegro Milo Đukanović, per impedire l'adesione del Paese alla NATO;[93]
- l'avvelenamento dell'ex agente del GRU Sergei Skripal' nel 2018, divenuto "fonte" dell'MI6.

Nel 2016, poi, è stato individuato in Svizzera l'agente dell'Unità 29155 Denis Sergeev, in continuo movimento tra Ginevra e Losanna.[94] Questo accadeva nel periodo in cui il GRU sferrava un attacco informatico contro la *World Anti-Doping Agency* (WADA) in relazione all'attività svolta per decidere la sorte dell'atleta russa Anna Chičerova (campionessa olimpica di salto in alto), accusata di *doping*. Nello stesso periodo risulta che il cellulare di Sergeev si sia ripetutamente collegato al ripetitore interno alla *Maison du Sport* di Losanna, edificio in cui ha sede anche la *World Anti-Doping Agency* di quella città.[95] Anche l'Alta Savoia, in Francia, ha visto la presenza di agenti del GRU per un certo periodo.[96] Si può ragionevolmente ritenere che l'intera area sia idonea come base per muoversi

91 Sarah Rainsford – Will Vernon, *Russian Spy Poisoning: Woman 'Identifies' Suspect as Anatoliy Chepiga*, BBC News, September 29, 2018. https://www.bbc.com; Bellingcat, *Skripal' Poisoner Attended GRU Commander Family Wedding*, October 14, 2019.

92 Shaun Walker - Maria Georgieva, *'I almost died': arms dealer whose poisoning may be linked to Skripal's'*, The Guardian, February 18, 2019; Schwirtz, *How a Poisoning in Bulgaria Exposed Russian Assassins in Europe.*

93 Shaun Walker, *Alleged Russian Spies Sentenced to Jail over Montenegro Coup Plot*, The Guardian, May 9, 2019

94 Bellingcat, *GRU Globetrotters 2: The Spies Who Loved Switzerland*, July 6, 2019. https://www.bellingcat.com.

95 Bellingcat, *GRU Globetrotters 2: The Spies Who Loved Switzerland*

96 Diego Malcangi, *L'Alta Savoia tra spie e informatori: GRU, ma non solo*, Euronews, 06/12/2019. https://it.euronews.com.; Jacques Follorou, *La Haute-Savoie camp de base d'espions russes specialises dans les assassinats cibles*, Le Monde, 04/12/2019.

agevolmente su tutto il territorio europeo. Nel 2017 ritroviamo Denis Sergeev in Spagna, precisamente a Barcellona. È un fatto che il viaggio risalga più o meno all'epoca del *referendum* sull'indipendenza non autorizzato, organizzato dai separatisti catalani. Sul viaggio di Sergeev Madrid ha avviato un'inchiesta.[97]

Arriviamo al giugno 2020, quando l'*intelligence* statunitense ha concluso che agenti del GRU avrebbero offerto pagamenti ai militanti legati ai *talebani* per attaccare le forze statunitensi e le altre forze internazionali presenti in Afghanistan. Secondo quanto riferito, l'organizzazione incaricata dell'intermediazione per questi pagamenti sarebbe stata l'Unità 29155.[98]

Anche gli altri servizi di intelligence russi gestiscono squadre clandestine per operazioni su obiettivi sensibili all'estero. L'FSB controlla le unità antiterrorismo d'élite, Alpha e Vympel, Alpha è la principale forza antiterrorismo russa.[99] Vympel è responsabile delle operazioni esterne, inclusi sabotaggi, presunti omicidi e sorveglianza segreta. L'unità Vympel sarebbe collegata all'assassinio dell'ex comandante militare ceceno Zelimkhan Khangoshvili, avvenuto nel 2019 a Berlino.[100]

Sempre all'FSB sarebbe riconducibile il tentativo di avvelenamento ai danni di Aleksej Naval'nyj, oppositore di Putin assurto agli onori della cronaca proprio in seguito all'episodio dell'avvelenamento, per certi versi assimilabile a quello di Skripal''. Per il tentativo di eliminazione di Naval'nyj, infatti, sarebbe stato utilizzato l'agente nervino *Novichok*, giù utilizzato per l'ex membro del GRU che ha disertato nel Regno Unito. L'SVR, infine, ha alle dipendenze l'unità *spetsnaz* chiamata *Zaslon* ("barriera"), coperta da un livello di segretezza tale da insinuare il dubbio sulla sua reale esistenza. Tale unità, diversamente da quelle fin qui presentate, non risulta ufficialmente riconosciuta dal governo di Mosca.[101] La sua presenza, tuttavia, è stata documentata in Siria.[102]

---

97 Oscar Lopez-Fonseca - Lucia Abellan - Maria R. Sahuquillo, *Western Intelligence Services Tracked Russian Spy in Catalonia*, El Pais, November 22, 2019.

98 Charlie Savage – Eric Schmitt – Michael Schwirtz, *Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says*, New York Times, June 26, 2020.

99 Cristadoro, *Spetsnaz e corpi paramilitari dei servizi di sicurezza russi. Il controterrorismo sui campi di battaglia.*

100 Bellingcat, *FSB's Magnificent Seven: New Links Between Berlin and Istanbul Assassinations*, June 29, 2020. https://www.bellingcat.com.

101 Cristadoro, *Spetsnaz e corpi paramilitari dei servizi di sicurezza russi. Il controterrorismo sui campi di battaglia.*

102 Mark Galeotti, *The Three Faces of Russian Spetsnaz in Syria.*

7 Cyberintelligence e Infowar

Dal 2008, il GRU ha sviluppato significative capacità cibernetiche, integrandole con la sua lunga esperienza nella conduzione di operazioni psicologiche e informative.[103] Lo sviluppo delle capacità cibernetiche del GRU ha coinciso con l'elaborazione della dottrina e delle procedure tecnico –tattiche in due settori più ampi della sicurezza e del pensiero militare russi: l'impiego degli strumenti non cinetici nei conflitti e la *information warfare*, entrambi finalizzati a colpire l'avversario nella sfera cognitiva, piuttosto che su obiettivi materiali.[104] La dottrina militare russa ha adottato una visione evolutiva della guerra, in cui il confine tra pace e conflitto è sempre più sfumato e l'utilità degli strumenti per il *soft-targeting* è sempre più importante. Tale principio è l'asse portante della "Dottrina Gerasimov", che vede nella risoluzione armata, segnatamente riferita all'impiego di truppe regolari sul terreno, solo l'ultima fase di un ciclo di operazioni accuratamente predisposte nel tessuto politico-socio-economico del nemico, da attuarsi proprio attraverso campagne di *cyberwarfare* e di *information operations* tra loro complementari. Le Forze Armate russe considerano le operazioni cibernetiche come uno strumento efficace e relativamente economico (in parte dovuto alla possibilità di negare la responsabilità degli attacchi portati negabilità e alla difficoltà di attribuzione di tale responsabilità) per indebolire, sovvertire e manipolare le strutture e le organizzazioni avversarie.[105]

Gli strumenti informatici sono diventati una componente sempre più cruciale negli sforzi della Russia per portare a termine una serie di compiti nel quadro più ampio della *infowar*[106] e, contestualmente, le dottrine militari e di sicurezza russe considerano le operazioni di informazione e disinformazione come uno strumento cruciale di politica estera.[107]

---

103 Ellen Nakashima, *U.S. Sanctions Russian Lab That Built What Experts Say Is Potentially the World's Deadliest Hacking Tool*, Washington Post, October 23, 2020.

104 Lilly - Cheravitch, *op. cit.*, pp. 130-134.

105 Timothy L. Thomas, *Russia's Reflexive Control Theory and the Military*, Journal of Slavic Military Studies, vol. 17, no. 2 (2004), pp. 237-256; Cristadoro, *La Dottrina Gerasimov*.

106 Stephen Blank, «Cyber War and Information War à la Russe», *Understanding Cyber Conflict*, ed. George Perkovich G. and Ariel E. Levite, Georgetown University Press, Washington, DC, 2017, pp. 81-98; Michael Connell – Sarah Vogler, *Russia's Approach to Cyber Warfare*, CNA, March 2017; Andrew Radin – Alyssa Demus – Krystyna Marcinek, *Understanding Russian Subversion: Patterns, Threats, and Responses*, RAND, February 2020, pp. 12-16.

107 Roland Heickero, *Emerging Cyber Threats and Russian Views on Information Warfare and*

Fin dal tempo dell'Unione Sovietica, le autorità russe hanno attribuito grande importanza alle operazioni psicologiche e, a partire dagli anni '90 del secolo scorso, hanno oculatamente seguito l'evoluzione delle tecniche e delle metodologie informative, in aderenza al mutare degli scenari internazionali e al progredire degli strumenti disponibili.[108]

La facilità con cui oggigiorno le notizie possono essere diffuse ed a queste si può accedere, per i *decision makers* di ogni paese, a tutti i livelli, presenta sia pericoli che opportunità. Questo aspetto investe in modo significativo la *leadership* russa che, da un lato può sfruttarlo le proprie attività di propaganda, dall'altro subisce preoccupata gli effetti destabilizzanti del libero flusso informativo, capace di fomentare proteste popolari e alimentare il malcontento sociale.[109] Effetti ritenuti tanto più dannosi quanto più si è consolidata la convinzione russa che i governi occidentali abbiano manipolato le informazioni per rovesciare i governi dei propri avversari.[110].

Durante le recenti proteste in Bielorussia contro il presidente Alexander Lukashenko, il capo dell'SVR russo Sergei Naryshkin ha accusato l'Occidente di aver condotto

> «…un tentativo mal camuffato di organizzare un'altra "rivoluzione colorata" e un colpo di stato anticostituzionale, i cui scopi ed obiettivi non hanno nulla a che vedere con gli interessi dei cittadini bielorussi.»[111]

La Russia si considera il reale obiettivo di queste campagne di *info-ops* e la dottrina militare e le politiche di sicurezza di Mosca descrivono i pericoli rappresentati dall'opinione pubblica nazionale da parte straniera.[112]

Information Operations, Swedish Defense Research Agency (FOI), March 2020.

108 Herbert Romerstein, «Disinformation as a KGB Weapon in the Cold War», *Journal of Intelligence History*, vol. 1, no. 1 (2001), pp. 54–67; Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, New York, 2020.

109 Karrie J. Koesel – Valerie J. Bunce, «Diffusion Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations Against Authoritarian Rulers», *Perspectives on Politics*, vol. 11. no. 3, 2013, pp. 753-768.

110 Dmitry Gorenburg, «Countering Color Revolutions: Russia's New Security Strategy and Its Implications for U.S. Policy», *PONARS Eurasia*, no. 342, September 2014; Tracey German, «Harnessing Protest Potential: Russian Strategic Culture and the Colored Revolutions», *Contemporary Security Policy*, vol. 41, no. 4, 2020, pp. 541-563.

111 Tom Balmforth, *Russia Accuses U.S. of Promoting Revolution in Belarus, Toughens Stance*, Reuters, September 16, 2020.

112 Nicolas Bouchet, «Russia's "Militarization" of Colour Revolutions», *Policy Perspectives*,

D'altra parte, dicevamo che l'uso e la manipolazione delle informazioni offre delle notevoli opportunità alla Russia.[113] L'architettura del sistema relativo alle "misure attive" (figura 2) implementate dal governo di Mosca è immutata nei compiti delle organizzazioni istituzionali.

A causa della percezione da parte dei responsabili politici russi che l'Occidente prenda costantemente di mira la Russia con campagne di *info-ops*, i servizi di *intelligence* e sicurezza di Mosca cercano, dunque, di infiltrare e indebolire attivamente la politica interna degli avversari e, allo stesso tempo, di contrastare e dichiarare infondata qualsiasi accusa di colpevolezza russa.[114] L'esperienza maturata nei settori delle *information operations* e della *sigint* ha consentito al GRU di sviluppare le proprie capacità nelle operazioni informatiche. La tattica di disinformazione russa sovente non è cercare un risultato particolare, quanto, piuttosto, provocare il caos e indebolire la legittimità interna del governo di un avversario. Gli attacchi informatici, invece, sono strumenti che il Cremlino ha utilizzato per promuovere gli obiettivi russi in politica estera russa o infliggere punizioni agli avversari in relazione a torti subiti, veri o presunti.[115] Questi attacchi sono stati effettuati in Paesi stranieri contro reti elettriche, settori bancari, istituzioni governative e persino eventi sportivi, sempre in funzione di una serie di obiettivi prefissati dalla Russia in politica estera.

I resoconti dei media indicano che per sviluppare le sue capacità cibernetiche, l'FSB ha fatto affidamento sulla cooptazione, sulla coercizione e sul reclutamento di individui in possesso di particolari abilità dalla comunità criminale informatica russa, spesso sotto la minaccia di procedimenti penali.[116] Al contrario, il

vol. 4, no. 2 , Center for Security Studies, January 2016.

113 Martin Kragh – Sebastian Asber, «Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case», *Journal of Strategic Studies*, vol. 40, no. 6 , 2017, pp. 773-816; Clint Watts, «Russia's Active Measures Architecture: Task and Purpose», *Alliance for Securing Democracy*, May 22, 2018.

114 Peter Pomerantsev, *Russia and the Menace of Unreality*, Atlantic, September 9, 2014; Renee Diresta – Shelby Grossman, *Potemkin Pages and Personas: Assessing GRU Online Operations*, 2014-2019, Stanford Internet Observatory Cyber Policy Center, 2019.

115 Benjamin Jensen – Brandon Valeriano – Ryan Maness, «Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist», *Journal of Strategic Studies*, vol. 42, no. 2, 2019, pp. 212-234; Greenberg, *Sandworm*, pp. 46-49.

116 Cory Bennett, *Kremlin's Ties to Russian Cyber Gangs Sow US Concerns*, The Hill, October 11, 2015; Daniil Turovsky, *It's Our Time to Serve the Motherland: How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers*, Me-

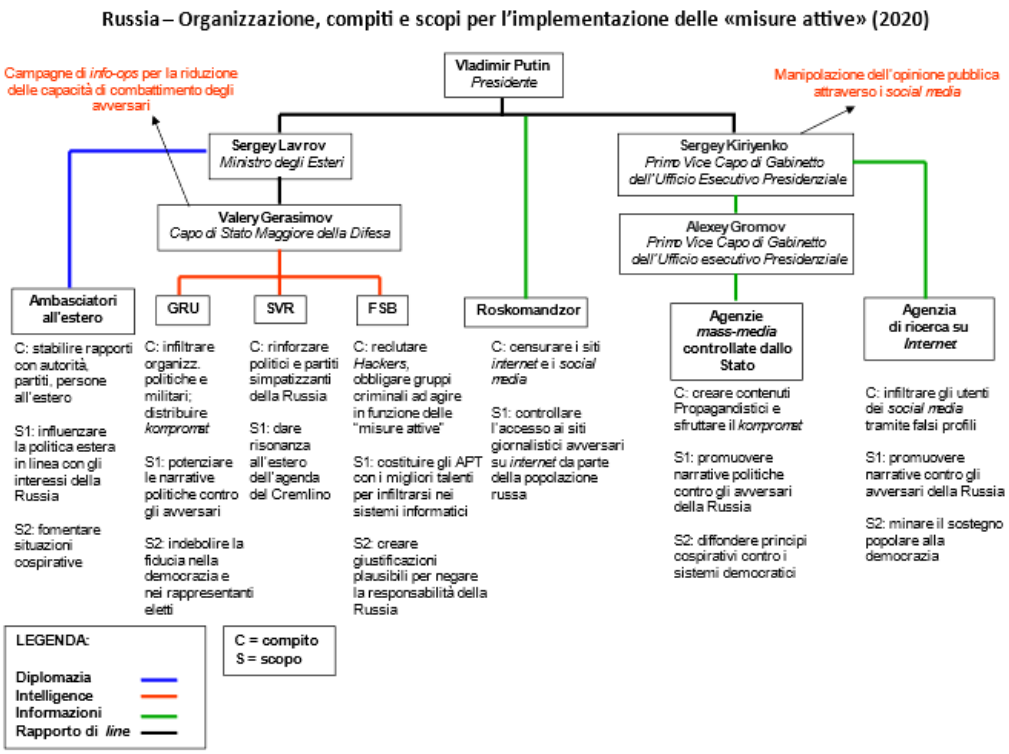

Figura 2 - Organizzazione per l'implementazione delle "misure attive" (autore: N. Cristadoro)

GRU apparentemente ha cercato di coltivare al proprio interno gli *hacker* e ha sviluppato diversi percorsi di reclutamento.[117]

In un atto d'accusa dell'ottobre 2020 rivolto contro l'unità GRU 74455, l'Assistente Procuratore Generale degli Stati Uniti per la Sicurezza Nazionale John C. Demers ha dichiarato:

> «Nessun paese ha armato le proprie capacità cibernetiche in modo fraudolento o irresponsabile come la Russia, causando arbitrariamente danni senza precedenti per perseguire piccoli vantaggi tattici e per soddisfare attacchi portati per dispetto.»[118]

---

duza, August 7, 2018; Liliya YAPPAROVA, *The FSB's Personal Hackers*, Meduza, December 12, 2018; Joseph MARKS, *Evil Corp Indictments Show Cybercrime Pays—For Those At The Top*, Washington Post, December 6, 2019; Mike ECKEL, *More Glimpses of How Russian Intelligence Utilized Hackers Revealed in U.S. Trial*, RFE/RL, March 16, 2020.

117 TROIANOVSKI – NAKASHIMA, *op. cit.*

118 U.S. DEPARTMENT OF JUSTICE, *Six Russian GRU Officers Charged in Connection with World-*

Vediamo quali sono unità del GRU deputate alla *cyber- warfare*.

La prima è l'Unità 26165, creata come "85° Centro Principale di Servizi Speciali" durante la Guerra Fredda ed incaricata della crittografia dell'*intelligence* militare.[119] Spesso indicata come APT 28 o *Fancy Bear*, l'Unità 26165 è una delle unità identificate dal governo degli Stati Uniti come responsabili dell'attività di *hackeraggio* ai danni del *Democratic Congressional Campaign Committee* (DCCC), del *Democratic National Committee* (DNC) e della campagna presidenziale di Hillary Clinton. Secondo la comunità dell'i*ntelligence* statunitense, la Russia ha compiuto un grande sforzo per interferire nelle elezioni presidenziali statunitensi del 2016. Le unità 26165 e 74455 sono state individuate come quelle direttamente responsabili dell'attività di intrusione nelle reti e di sottrazione dei dati.[120] L'unità 26165, in particolare, avrebbe condotto lo sforzo maggiore mirato a violare le *e-mail* e i sistemi del DCCC e del DNC, nonché gli *account* di posta elettronica di persone impegnate nella campagna elettorale della Clinton.[121] Figura di spicco dell'unità è Dmitry Badin, ritenuto implicato non solo nelle interferenze nella campagna presidenziale del 2016, ma anche nell'attacco informatico contro il *Bundestag* avvenuto l'anno precedente e per il quale la Germania ha emanato un mandato d'arresto contro questo Ufficiale del GRU.[122] Per gli attacchi del 2016, nell'ottobre del 2020 l'Unione Europea e gli Stati Uniti hanno sanzionato Badin e il Direttore del GRU, Igor Kostyukov.[123]

Ricordiamo che questa attività di intrusione informatica rientra nella più complessa attività di intromissione nelle elezioni americane che videro l'affermazione di Donald Trump e che è nota come *Russiagate*.[124]

---

wide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, press release, October 19, 2020.

119 Lilly - Cheravitch, *The Past, Present, and Future of Russia's Cyber Strategy and Forces*, p. 145.

120 U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 5 vol., 2019-2020.

121 U.S. Congress, Senate Select Committee on Intelligence, *ibid.*

122 Kate Connolly, *Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel*, The Guardian, May 13, 2020; Catherine Stupp, *Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament*, Wall Street Journal, June 11, 2020.

123 Robin Emmott, *EU Imposes Sanctions on Russian Military Intelligence Chief*, Reuters, October 22, 2020.

124 Il *Russiagate* è un'inchiesta giudiziaria nata a seguito di sospette ingerenze da parte della Russia nella campagna elettorale per le elezioni presidenziali negli Stati Uniti d'America del 2016. Secondo il New York Times l'ingerenza russa si sviluppò lungo tre direttrici: in-

Un altro *team* di *hacker* coinvolto nell'interferenza elettorale è noto come APT 29 o *Cozy Bear*, che si ritiene sia gestito in concorso dall'FSB e dall'SVR (figura 3);[125] dalle analisi effettuate dall'*Algemene Inlichtingen- en Veiligheidsdienst* (AIVD - Servizio Generale di Intelligence e Sicurezza) olandese risulterebbe che l'APT 29 dipende dall'SVR.[126]

Nel Luglio del 2020 l'ATP 29 è stato accusato dalla *National Security Agency* (NSA) americana, dal *National Cyber Security Center* (NCSC) inglese e *dal Communication Security Establishment* (CSE) canadese di aver tentato di rubare dati e trattamenti relativi al *covid-19*, di proprietà dei tre Paesi indicati.[127] Sempre nel 2020, APT 29 sarebbe stato l'artefice dell'attacco informatico su vasta scala definito *SUNBURST Malware Supply Chain Attack*, con cui vennero violate le reti di centinaia di organizzazioni in tutto il mondo, incluse molte agenzie del governo degli Stati Uniti.[128]

Abbiamo citato anche l'Unità 74455, denominata "Centro Principale per le Tecnologie Speciali" e comunemente nota come *Sandworm*, come co-responsabile dell'azione mirata ad interferire nelle elezioni presidenziali americane del 2016. Le indagini svolte documentano in che modo l'Unità 74455 si sarebbe impossessata di migliaia di documenti rubati tramite falsi *account* intestati a persone fittizie - tra cui *DCLeaks* e Guccifer 2.0[129] - e come li avrebbe divulgati in

---

tercettazione e divulgazione di documenti del partito rivale; massicce attività fraudolente mediante profili *Facebook* e *Twitter*; contatto con associati alla campagna presidenziale di Trump. In proposito, sempre il *New York Times* già aveva riportato che il figlio omonimo del presidente, Donald J. Trump, il 9 giugno 2016 incontrò alla *Trump Tower* l'avvocato russo Natalia Veselmitskaya, che aveva rapporti diretti con il Cremlino. L'inchiesta ha portato all'incriminazione di dodici cittadini russi funzionari del GRU. Paul Manafort, responsabile della campagna elettorale di Donald Trump, è stato posto prima agli arresti domiciliari, e in seguito, il 15 giugno 2018, trasferito in carcere, dopodiché ha accettato di patteggiare su alcune delle accuse rivoltegli; una parte dei termini di questo patteggiamento sono poi stati revocati per aver nascosto i suoi contatti con un consulente russo, su cui si era assunto l'impegno di riferire al magistrato inquirente.

125 Fonte: Välisluureamet (Estonian Foreign Intelligence Service), *International Security and Estonia*, 2018.

126 Huib *Modderkolk, Dutch agencies provide crucial intel about Russia's interference in US-elections, de Volkskrant. 25 January 2018.*

127 NCSC, *Advisory: APT29 targets COVID-19 vaccine development*, 16 July 2020.

128 David E. *Sanger – Nicole Perlroth – Eric Schmitt, Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit, The New York Times, December 15, 2020.*

129 Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, pp. 183-183, 188.

coordinamento con *WikiLeaks*.[130]

Questa unità è collegata ad alcune delle operazioni cibernetiche più temerarie ed aggressive condotte della Russia, come l'attacco *NotPetya* del 2017 in Ucraina.[131] Il 19 ottobre 2020, il Dipartimento di Giustizia degli Stati Uniti ha avviato un'inchiesta contro sei membri dell'Unità 74455,[132] accusati di attacchi informatici contro vari obiettivi internazionali, tra cui:

- l'attacco nel 2015 - 2016 alle reti elettriche, al Ministero delle Finanze e all'Agenzia del Fisco in Ucraina, utilizzando i *malware* noti come *BlackEnergy*, *Industroyer* e *KillDisk*;
- le campagne di *spearphishing* nei mesi di aprile e maggio 2017 e i relativi tentativi di *hack-and-leak* mirati al partito del presidente francese Macron *La République En Marche!*, a politici francesi e a governi locali francesi prima delle elezioni del 2017;
- gli attacchi del 27 giugno 2017 utilizzando il *malware* noto come *NotPetya*, che hanno infettato computer in tutto il mondo, inclusi ospedali e altre strutture mediche *nell'Heritage Valley Health System* (Heritage Valley) nel distretto occidentale della Pennsylvania; una controllata di *FedEx Corporation*, la *TNT Express B.V.* e un'importante casa farmaceutica statunitense, causando perdite per quasi 1 miliardo di dollari;
- le campagne di *spearphishing* dal dicembre 2017 al febbraio 2018, rivolte a cittadini e funzionari sudcoreani, atleti olimpici, *partner*, visitatori e funzionari del Comitato Olimpico Internazionale (CIO), in occasione delle Olimpiadi Invernali di Pyeongchang nel 2018;
- l'attacco del 9 febbraio 2018, con il *malware* noto come *Olympic Destroyer* mirato a sabotare la cerimonia d'apertura dei Giochi Olimpici invernali in Corea. L'attacco cercò di dissimulare la responsabilità del GRU cercando di attribuirlo ad *hacker* nordcoreani;

---

130 Thomas Rid, *How Russia Pulled Off the Biggest Election Hack in U.S. History*, Esquire, October 20, 2016.

131 Ellen Nakashima, *Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, Washington Post, January 12, 2018.

132 U.S. Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, press release, October 19, 2020.

- le campagne di *spearphishing* dell'aprile 2018, rivolte alle indagini dell'Organizzazione per la Proibizione delle Armi Chimiche (OPCW) e del Laboratorio di Scienza e Tecnologia della Difesa del Regno Unito (DSTL) sull'avvelenamento da agenti nervini di Sergei Skripal' e di sua figlia;
- la campagna di *spearphishing* del 2018 - 2019, rivolta a un'importante società di media e al Parlamento della Georgia per comprometterne la funzionalità.

Vogliamo soffermarci sull'episodio del 4 marzo 2018, a Salisbury, quando l'ex ufficiale del GRU Sergei Skripal'' e sua figlia sono stati esposti a un agente chimico altamente tossico e potenzialmente letale, identificato come *Novichok* ed appartenente ad una classe di agenti nervini sviluppata nell'Unione Sovietica. Per confermare questi risultati, i campioni della sostanza furono inviati all'Organizzazione per la Proibizione delle Armi Chimiche (OPCW) a L'Aia, in Olanda. L'OPCW stava anche indagando sulle accuse di un presunto attacco di gas in Siria da parte del regime di Bashar al-Assad contro la città di Douma. Il 10 aprile 2018, quattro agenti del GRU che viaggiavano con passaporti diplomatici sono entrati nei Paesi Bassi. Tra l'11 e il 12 aprile, gli agenti condussero una ricognizione dell'area intorno alla sede dell'OPCW, fermandosi in un hotel direttamente accanto all'OPCW. Il 13 aprile, in collaborazione con l'*intelligence* britannica, i servizi di sicurezza olandesi arrestarono i quattro uomini. Nell'auto di un agente del GRU furono scoperte apparecchiature *hi-tech*, che idonee per penetrare le reti *wi-fi* dell'OPCW. L'attrezzatura venne confiscata e gli agenti espulsi dal paese. Successivamente, i Paesi Bassi e il Regno Unito hanno tenuto una conferenza stampa congiunta il 4 ottobre 2018,[133] descrivendo in dettaglio l'operazione del GRU e identificando gli agenti. Lo stesso giorno, il Dipartimento di Giustizia degli Stati Uniti ha accusato sette ufficiali del GRU per il tentato attacco dell'OPCW, nonché per aver violato l'Agenzia Mondiale Antidoping nel 2016;[134] l'agenzia stava indagando sull'assunzione di farmaci che migliorano le prestazioni, da parte degli atleti russi durante le Olimpiadi invernali di Sochi 2014. In risposta all'attacco di Skripal' e al tentativo di *hacking* dell'OPCW, più di 26 paesi hanno espulso più di 150 diplomatici russi. Il Regno Unito ne allontanò 23;

133 Government of the Netherlands, *Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW*, press release, October 4, 2018.

134 U.S. Department of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*, press release, October 4, 2018.

gli Stati Uniti mandarono via 60 funzionari e chiusero il consolato russo a Seattle, oltre a due strutture ricreative nel Maryland e a Long Island, presumibilmente utilizzate per la raccolta di informazioni.

Arriviamo all'ultima delle unità di cui vogliamo parlare: l'Unità 54777. Questa unità, nota anche come "72° Centro Servizi Speciali", sarebbe responsabile delle operazioni psicologiche del GRU.[135] L'unità opera in supporto di altre unità informatiche del GRU e, a livello tattico, conduce attività di guerra elettronica e *psyops*. Fanno parte dell'unità diverse organizzazioni "di copertura", come l'agenzia giornalistica *InfoRos* e l'Istituto per gli Studi e l'Integrazione della Diaspora Russa.[136] L'unità trae origine dall'agenzia di epoca sovietica GlavPUR (*Glavnoye Politicheskoye Upravlenie*, - Direttorato Politico Principale)[137] e fu creata agli inizi degli anni '90 dal Colonnello Aleksandr Viktorovich Golyev, i cui memoriali sono stati pubblicati nel 2020, insieme ad altri documenti del GRU. All'epoca della sua fondazione l'unità si occupava principalmente di fare disinformazione nelle neonate repubbliche formatesi dal dissolvimento dell'U.R.S.S., come la Lituania o la Cecenia. Successivamente ha sviluppato un più ampio spettro di attività, che vanno dalla gestione di NGOs rivolte all'individuazione dei compatrioti russi espatriati in Occidente, alla manipolazione dell'opinione pubblica in Russia e all'estero, al fine di creare un terreno favorevole a conflitti armati, quali quelli in Georgia, Donbass e Siria.[138] Gerasimov impera.

Il GRU sembra continuare e adattare le sue operazioni informatiche all'estero, nonostante le numerose accuse e la scoperta di molte operazioni attribuibili all'agenzia. Anche l'attuale Presidente Joe Biden sarebbe un *target* privilegiato delle attività di *cyberwar* delle Russia. Nel settembre 2020, il direttore dell'FBI Christopher Wray ha dichiarato che la Russia si era data molto fa fare per inter-

135 Troianovski – Nakashima, *op. cit.*

136 Troianovski – Nakashima, *ibid.*

137 Organo preposto all'indottrinamento ed al controllo ideologico all'interno delle Forze Armate in Unione Sovietica. Alle dipendenze del GlavPUR erano poste l'Accademia politico-militare V.I. Lenin, preposta alla formazione dei "commissari politici", 11 scuole superiori per la formazione politico-militare, i dipartimenti ideologici inseriti in 20 accademie militari e in150 scuole.

138 Michael Weiss, *Aquarium Leaks. Inside the GRU's Psychological Warfare Program*, Free Russia Foundation, Washington DC, 2020.

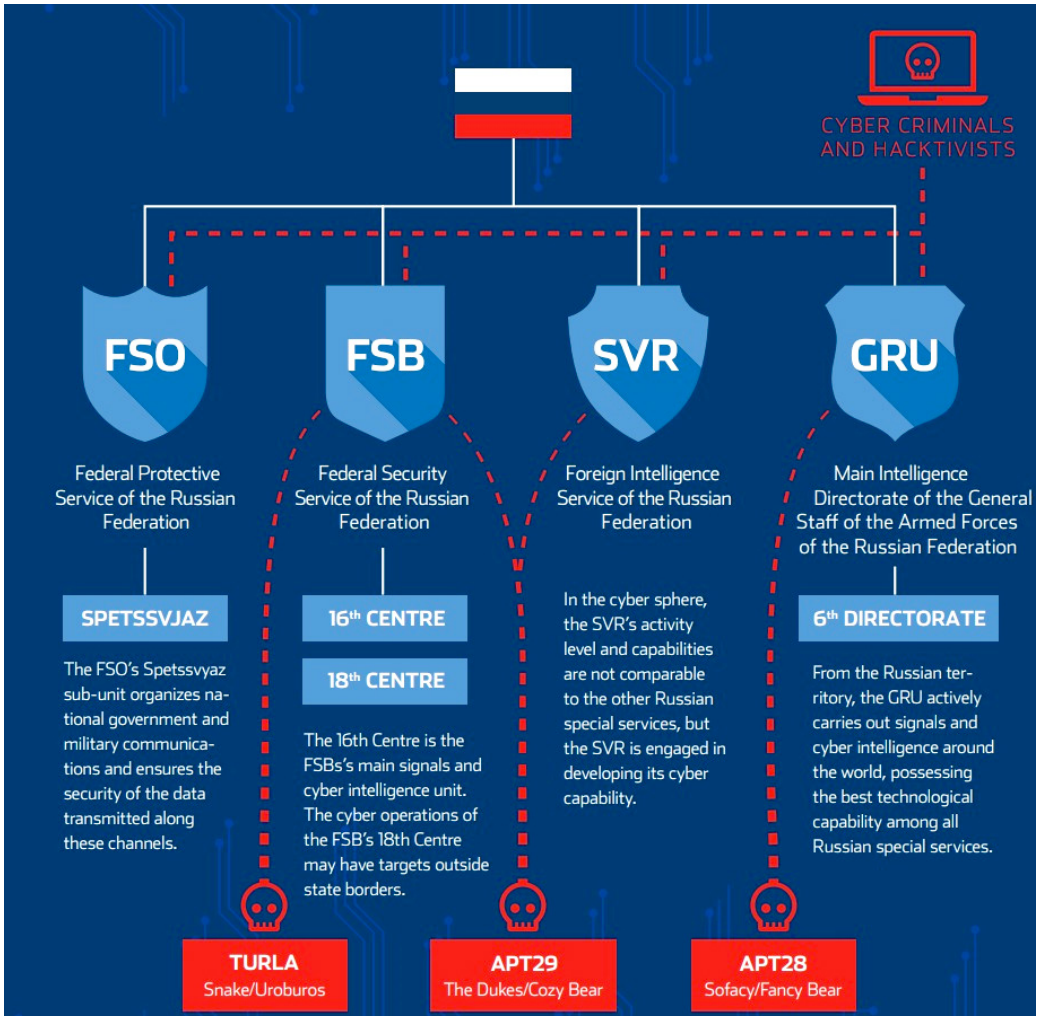

Figura 3 – Organizzazione *cyber-intelligence* russa
(fonte: *Estonian Foreign Intelligence Service*)

ferire nelle elezioni del 2020.[139] Il GRU, con le sue unità specialistiche, inoltre, avrebbe anche violato le reti di computer della società ucraina di gas naturale *Burisma*, di cui il figlio di Joe Biden, Hunter Biden, è stato un membro del consiglio direttivo.[140]

139 Kyle CHENEY, *Wray Says Russia Engaged in "Very Active Efforts" to Interfere in Election, Damage Biden*, Politico, September 17, 2020.

140 Nicole PERLROTH – Mattew ROSENBERG, *Russian Hacked Ukrainian Gas Company at Cen-*

Conclusioni

Ad oggi il GRU dimostra di essere un'istituzione forte, con le radici solidamente affondate nel proprio passato e lo sguardo rivolto al futuro. Le sue procedure sono consolidate e, nondimeno, sono proiettate verso tutto ciò che la tecnologia offre per la ricerca informativa e per la condotta di azioni improntate all'aggressività e caratterizzate da un profilo di rischio elevato. Le sue capacità di adeguamento delle tecniche e delle strategie da adottare in aderenza al mutare delle situazioni e degli scenari sono decisamente tempestive. Accanto allo spionaggio tradizionale svolto attraverso le fonti umane, gestite da una capillare "rete diplomatica" nella cui trama gli agenti del GRU si mescolano ai colleghi di altri servizi di sicurezza, possiamo trovare nuclei di tecnici in grado di sviluppare indifferentemente attività di *virtual* HUMINT, attacchi informatici ed *hacking* finalizzato alla sottrazione di migliaia di dati sensibili dai computer di tutto il mondo. Le azioni mirate all'eliminazione di singoli individui sono affiancate dall'organizzazione e dalla gestione di operazioni su vasta scala, quali il rovesciamento di governi ritenuti ostili (Montenegro), o l'invasione di territori appartenenti ad altri Stati (Ucraina) o il sostegno di regimi amici di Mosca (Siria). Una tale attitudine, sostenuta dalla consapevolezza che la *leadership* politica russa trova utile avere un'agenzia di questo tipo, capace e disposta a condurre tali operazioni, induce a ritenere che azioni mirate esclusivamente contro il GRU potrebbero non avere il livello di impatto desiderato.

Va detto, tuttavia, che nel clima che contraddistingue la compagine governativa di Putin e, in fondo, che da sempre ha caratterizzato tutti i governi nella storia della Russia e dell'Unione Sovietica, non manca quel tratto di arroganza che può rappresentare una vulnerabilità. Infatti, alla capacità di aderire alla rapida evoluzione degli scenari geostrategici, non sempre corrisponde il conseguimento dei risultati prefissati.

Il fallimento di "collaudati" sistemi degni delle tradizionali *spy stories*, quali l'eliminazione degli obiettivi fisici attraverso l'avvelenamento (casi Skripal'' e Gebrev) o l'individuazione delle unità *spetsnaz* alle dipendenze dell'agenzia, sia in Crimea, sia in Siria, hanno consentito di svelare la *longa manus* della potente organizzazione di *intelligence* militare russa dietro tali iniziative.

---

ter of Impeachment, New York Times, January 13, 2020.

La scoperta delle operazioni del GRU, altresì, ha fatto emergere le lotte intestine tra le agenzie di sicurezza russe che cercano di trarre vantaggio da queste rivelazioni, minando così le capacità russe.

Un'altra conseguenza del fallito tentativo di assassinio ai danni di Sergei Skripal' nel 2018 nel Regno Unito, che ha inferto un colpo significativo alla rete dell'*intelligence* del Cremlino, sono state le sanzioni che gli Stati Uniti e diversi Stati occidentali alleati hanno emanato contro la Russia, unitamente all'espulsione di numerosi diplomatici russi e di funzionari sospettati di essere ufficiali dell'*intelligence*. Queste misure, inoltre, hanno creato delle tensioni all'interno del governo russo, che ha incolpato il GRU per la situazione in cui si è venuto a trovare il Paese alla base della perdita di fiducia nei confronti del governo. È da valutare se i falliti tentativi di avvelenamento, che presentano diverse analogie con il più recente "caso Naval'nyj" ascrivibile all'FSB, siano realmente frutto di errori dovuti a scarsa professionalità o, piuttosto, scelte strategiche con lo scopo di dare un segnale "forte" da parte di Putin ai suoi avversari, qualcosa tipo: "*sappiate che siamo in grado di colpirvi come e quando vogliamo*". A prescindere dalle ragioni, ciò che fa la differenza sono gli esiti delle decisioni e delle azioni relative all'impiego del GRU, che di fronte all'opinione pubblica interna e alla Comunità Internazionale hanno sortito l'effetto contrario a quello che verosimilmente il governo russo si era prefissato. Con l'insediamento di Joe Biden alla Casa Bianca ed il profilarsi di un nuovo clima da Guerra Fredda tra la Russia e l'Occidente è prevedibile che il tradizionale impiego del GRU come strumento di una politica estera tendenzialmente aggressiva rimanga inalterato. Nel *targeting* mirato ad obiettivi specifici che, in caso di rivelazione, comporti ulteriori inasprimenti delle sanzioni di cui il popolo russo, in definitiva, subisce le conseguenze, si può prefigurare un "cambio di rotta" da parte del Cremlino. Questo perché nei confronti del mondo esterno il popolo russo è abbastanza coeso e, si potrebbe dire, "culturalmente monolitico" e, pertanto, il crescente dissenso verso il governo può essere alimentato più attraverso il calo del livello di benessere all'interno del Paese, più che dai modelli e dai principi proposti dal sistema occidentale.

Bibliografia

Baud Jacques, *Encyclopédie du renseignement et des services secrets*, Lavauzelle, 2004

Balenko Sergej, *Учебник выживания Спецназа ГРУ. Опыт элитных спецподразделений* (Manuale di sopravvivenza delle forze speciali del GRU. L'esperienza delle forze speciali d'élite), Eksmo, Yauza, 2009.

Balmforth Tom, *Putin Praises Skills of GRU Spy Agency Accused of UK Poison Attack*, Reuters, November 2, 2018.

Balmforth Tom, *Russia Accuses U.S. of Promoting Revolution in Belarus, Toughens Stance*, Reuters, September 16, 2020.

Bartles Charles K. - McDermott Roger, *Russia's Military Operation in Crimea: Road Testing Rapid Reaction Capabilities*, Problems of Post-Communism, vol. 61, no. 6, 2014.

Bellingcat, *305 Car Registrations May Point to Massive GRU Security Breach*, October 4, 2018. https://www.bellingcat.com.

Bellingcat, *FSB's Magnificent Seven: New Links Between Berlin and Istanbul Assassinations*, June 29, 2020. https://www.bellingcat.com.

Bellingcat, *GRU Globetrotters 2: The Spies Who Loved Switzerland*, July 6, 2019. https://www.bellingcat.com.

Bellingcat, *MH17 - Russian GRU Commander 'Orion' Identified as Oleg Ivannikov*, May 25, 2018. https://www.bellingcat.com.

Bellingcat, *Skripal' Poisoner Attended GRU Commander Family Wedding*, October 14, 2019.

Bennet G., *FPS and FAPSI – RIP*, Conflict Studies Research Center, Occasional Paper n. 96.

Bennett C., *Kremlin's Ties to Russian Cyber Gangs Sow US Concerns*, The Hill, October 11, 2015.

Bigg C., *Vostok Battalion, a Powerful New Player in Eastern Ukraine*, RFE/RL, May 30, 2014.

Blank Stephen, «Cyber War and Information War à la Russe», *Understanding Cyber Conflict*, ed. George Perkovich G. and Ariel E. Levite, Georgetown University Press, Washington, DC, 2017.

Bouchet Nicolas, «Russia's "Militarization" of Colour Revolutions», *Policy Perspectives*, vol. 4, no. 2 , Center for Security Studies, January 2016.

Bowen Andrew S., «Russian Private Military Companies (PMCs)», *Congressional Research Service*, In Focus IF11650, September 16, 2020.

Bukkvoll Tor, «Russia's Military Performance in Georgia», *Military Review,* vol. 89, no. 6, 2009, pp. 57-62.

Cheney Kyle, *Wray Says Russia Engaged in "Very Active Efforts" to Interfere in Election, Damage Biden*, Politico, September 17, 2020.

Cohen Ariel – Hamilton Robert E., *The Russian Military and the Georgia War: Lessons and Implications*, Strategic Studies Institute, Carlisle (PA), 2011.

Congressional Research Service (CRS) interview with Mark Galeotti.

Connell Michael –Vogler Sarah, *Russia's Approach to Cyber Warfare*, CNA, March 2017.

Connolly Kate, *Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel*, The Guardian, May 13, 2020

Cristadoro Nicola, *La Dottrina Gerasimov*, La Libellula, Tricase (LE), 2018.

Cristadoro Nicola, *Spetsnaz e corpi paramilitari dei servizi di sicurezza russi. Il contro-terrorismo sui campi di battaglia*, Il Maglio Edizioni, 2018.

Diresta Renee - Grossman Shelby, *Potemkin Pages and Personas: Assessing GRU Online Operations*, 2014-2019, Stanford Internet Observatory Cyber Policy Center, 2019.

Eckel Mike, *More Glimpses of How Russian Intelligence Utilized Hackers Revealed in U.S. Trial*, RFE/RL, March 16, 2020.

Emmott Robin, *EU Imposes Sanctions on Russian Military Intelligence Chief*, Reuters, October 22, 2020.

Fainberg Sarah, «Russian Spetsnaz, Contractors, and Volunteers in the Syrian Conflict», *Russie.nei Visions*, IFRI, December 2017.

Faulconbridge Guy, *What is Russia's GRU military intelligence agency?*, Reuters, 05/10/2018. https://www.reuters.com.

Ferris-Rotman Amie - Nakashima Ellen, *Estonia Knows a Lot About Battling Russian Spies, and the West Is Paying Attention*, Washington Post, November 1, 2018.

Follorou Jacques, *La Haute-Savoie camp de base d'espions russes specialises dans les assassinats cibles*, Le Monde, 04/12/2019.

Free Syrian Army warns on forthcoming attacks on Russian targets in Syria, Department of Monitoring Kavkaz Center, 14/12/2012. http://www.kavkazcenter.com.

Galeotti Mark, *Korabelnikov Leaves Russian Military Intelligence*, In Moscow's Shadows, April 26, 2009.

Galeotti Mark, *Putin's Hydra: Inside Russia's Intelligence Services*, Policy Brief of the European Council for Foreign Relations, May 11. 2016

Galeotti Mark, *Putin's Secret Weapon*, Foreign Policy, July 7, 2014. https://foreignpolicy.com.

Galeotti Mark, *Russia's Military Intelligence Agency Isn't Stupid*, Foreign Policy, September 6, 2018.

Galeotti Mark, *Special Troops of GRU Will Be Growing Headache for the West*, Raamoprusland, September 28, 2018.

Galeotti Mark, *Spetsnaz: Operational Intelligence, Political Warfare and Battlefield Role*, Marshall Center Security Insights, n. 46, February 2020.

Galeotti Mark, *Spetsnaz: Russia's Special Forces*, Osprey Publishing, Oxford, 2015.

Galeotti Mark., *Spooks in the Kremlin*, Foreign Policy, April 27, 2019.

Galeotti Mark, *The Intelligence and Security Services and Strategic Decision-Making*, Marshall Center Security Insights, n. 30, May 2019.

Galeotti Mark, *The Three Faces of Russian Spetsnaz in Syria*, War on the Rocks, March 21, 2016. https://warontherocks.com.

Galeotti Mark, *We Don't Know What to Call Russian Military Intelligence and That May Be a Problem*, War On The Rocks, January 19, 2016.

Garthoff Raymond L., *Soviet Leaders and Intelligence: Assessing the American Adversary During the Cold War*, Georgetown University Press, Washington D.C., 2015.

German Tracey, «Harnessing Protest Potential: Russian Strategic Culture and the Colored Revolutions», *Contemporary Security Policy*, vol. 41, no. 4, 2020.

Gerasimov Valerij V., «Ценность Науки в Предвидении» (Il valore della scienza nella previsione), *Corriere Militare-Industriale*, a cura dell'Accademia Russa di Scienze Militari, 23/02/2013.

Gibbons-Neff Thomas, *How Russian Special Forces Are Shaping the Fight in Syria*, Washington Post, March 29, 2016.

Gioe David V. - Goodman Michael S. - Frey David S., «Unforgiven: Russian Intelligence Vengeance as Political Theater and Strategic Messaging», *Intelligence and National Security*, vol. 34, n. 4, 2019

Ginori Anais, *Breccia russa nell'esercito francese: arrestato un ufficiale di stanza alla Nato in Italia*, La repubblica, 30/08/2020.

Glantz David M., *Soviet Military Intelligence in War*, Frank Cass, New York,1990.

Gorenburg Dmitry, «Countering Color Revolutions: Russia's New Security Strategy and Its Implications for U.S. Policy», *PONARS Eurasia*, no. 342, September 2014.

Government of the Netherlands, *Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW*, press release, October 4, 2018.

Greenberg Andy, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Doubleday, New York, 2019.

Harding Luke, *A Chain of Stupidity: The Skripal' Case and the Decline of Russia's Spy Agencies*, The Guardian, June 23, 2020.

Haslam Jonathan, *Near and Distant Neighbors: A New History of Soviet Intelligence*, Farrar, Straus and Giroux, New York, 2015.

Heickero Roland, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*, Swedish Defense Research Agency (FOI), March 2020.

Jensen Benjamin – Valeriano Brandon –Maness Ryan, «Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist», *Journal of Strategic Studies*, vol. 42, no. 2, 2019.

KATZ Brian –HARRINGTON Nicholas, *The Military Campaign*, in *Moscow's War in Syria*, ed. Seth G. Jones (CSIS, 2020).

KNIGHT Amy, *Spies Without Cloaks: The KGB's Successors*, Princeton University Press, Princeton, 1996.

KNIGHT Amy, *This Russian Spy Agency Is in the Middle of Everything*, Daily Beast, August 10, 2018.

KOESEL Karrie J. –BUNCE Valerie J., «Diffusion Proofing: Russian and Chinese Responses to Waves of Popular Mobilizations Against Authoritarian Rulers», *Perspectives on Politics*, vol. 11. no. 3, 2013.

KOFMAN Michael et al., *Lessons From Russia's Operations in Crimea and Eastern Ukraine*, RAND, 2014.

KOLPAKIDI Alexander, *Империя ГРУ* (L'Impero del GRU) (2 volumi), Olma-Press, 2000.

KRAGH Martin –ASBER Sebastian, «Russia's Strategy for Influence Through Public Diplomacy and Active Measures: The Swedish Case», *Journal of Strategic Studies*, vol. 40, no. 6 , 2017.

LAVROV Anton, «Russian Aerial Operations in the Syrian War», *Russia's War in Syria: Assessing Russian Military Capabilities and Lessons Learned*, ed. Robert E. Hamilton, Chris Miller, Aaron Stein, Philadelphia (PA), Foreign Policy Research Institute, 2020.

LAVROV Anton, «Russian Again: The Military Operation for Crimea», *Brothers Armed: Military Aspects of the Crisis in Ukraine*, East View Press, Minneapolis (MN), 2015.

LEE MYERS Steven, *Qatar Court Convicts 2 Russians in Top Chechen's Death*, New York Times, July 1, 2004.

LEKAREV Stanislav, *Two Types of Russian Intelligence Are Unified*, Nezavisimaya Gazeta, August 31, 2001.

LEONARD Raymond W., «Studying the Kremlin's Secret Soldiers: A Historiographical Essay on the GRU, 1918–1945», *Journal of Military History*, vol. 56, no. 3, 1992, pp. 403–422.

LEONARD Raymond W., *Secret Soldiers of the Revolution: Soviet Military Intelligence, 1918-1933,* Greenwood Press, Westport (CT), 1999.

LILLY Bilyana - CHERAVITCH Joe, «The Past, Present, and Future of Russia's Cyber Strategy and Forces», *12th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre of Excellence, 2020.

LOPEZ-FONSECA Oscar - ABELLAN Lucia - SAHUQUILLO Maria R., *Western Intelligence Services Tracked Russian Spy in Catalonia*, El Pais, November 22, 2019.

MALCANGI Diego, *L'Alta Savoia tra spie e informatori: GRU, ma non solo*, Euronews, 06/12/2019. https://it.euronews.com.

MALLET Victor, *French Military Officer Held on Suspicion of Spying*, Financial Times, August 30, 2020.

Marks Joseph, *Evil Corp Indictments Show Cybercrime Pays—For Those At The Top*, Washington Post, December 6, 2019.

McDermott Roger, «Russian Military Intelligence: Shaken but Not Stirred», *Eurasia Daily Monitor*, Jamestown Foundation, February 7, 2012.

Meakins Joss I., «Squabbling Siloviki: Factionalism Within Russia's Security Services», *International Journal of Intelligence and Counterintelligence*, vol. 31, no. 2, 2018.

Modderkolk Huib, *Dutch agencies provide crucial intel about Russia's interference in US*-elections, de Volkskrant. 25 January 2018.

Nakashima Ellen, *Russian Military was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes*, Washington Post, January 12, 2018.

Nakashima Ellen, *U.S. Sanctions Russian Lab That Built What Experts Say Is Potentially the World's Deadliest Hacking Tool*, Washington Post, October 23, 2020.

NCSC, *Advisory: APT29 targets COVID-19 vaccine development*, 16 July 2020.

Orlova Karina, *Russia's Intelligence Failures*, American Interest, October 10, 2018.

Paton Walsh Nick, *Top Chechen Separatist Dies in Qatar Bomb Blast, Guardian*, February 13, 2002.

Perlroth Nicole – Rosenberg Mattew, *Russian Hacked Ukrainian Gas Company at Center of Impeachment*, New York Times, January 13, 2020.

Pomerantsev Peter, *Russia and the Menace of Unreality*, Atlantic, September 9, 2014.

President of Russia, *President Vladimir Putin visited the new headquarters of the Russian Armed Forces General Staff Chief Intelligence Directorate (GRU)*, press release, November 8, 2006. http://en.kremlin.ru.

Radin Andrew –Demus Alyssa –Marcinek Krystyna, *Understanding Russian Subversion: Patterns, Threats, and Responses*, RAND, February 2020.

Rainsford Sarah, *Convicted Russia Agents "Missing"*, BBC, February 17, 2005.

Rainsford Sarah, *Have Russian Spies Lost Their Touch?*, BBC, October 6, 2018.

Rainsford Sarah – Vernon Will, *Russian Spy Poisoning: Woman 'Identifies' Suspect as Anatoliy Chepiga*, BBC News, September 29, 2018. https://www.bbc.com.

Reddaway Peter, *Russia's Domestic Security Wars: Putin's Use of Divide and Rule Against His Hardline Allies* , Palgrave Pivot, London, 2018.

RFE/RL, *On the Trail of the 12 Indicted Russian Intelligence Officers*, July 19, 2020.

RFE/RL, *Retired Austrian Army Colonel Found Guilty of Spying for Russia*, June 10, 2020.

Rid Thomas, *Active Measures: The Secret History of Disinformation and Political Warfare*, Farrar, Straus and Giroux, New York, 2020.

Rid Thomas, *How Russia Pulled Off the Biggest Election Hack in U.S. History*, Esquire, October 20, 2016.

Romerstein Herbert, «Disinformation as a KGB Weapon in the Cold War», *Journal of Intelligence History*, vol. 1, no. 1 (2001).

ROTH Andrew, *How the GRU Spy Agency Targets the West, from Cyberspace to Salisbury*, The Guardian, August 6, 2018.

ROTH Andrew, *A Separatist Militia in Ukraine with Russian Fighters Holds a Key,* New York Times, June 4, 2014.

SANGER David E. –PERLROTH Nicole –SCHMITT Eric, *Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit*, The New York Times, December 15, 2020.

SAVAGE Charlie - SCHMITT Eric – SCHWIRTZ Michael, *Russia Secretly Offered Afghan Militants Bounties to Kill U.S. Troops, Intelligence Says*, New York Times, June 26, 2020.

SCHWIRTZ Michael, *How a Poisoning in Bulgaria Exposed Russian Assassins in Europe*, The New York Times, December 22, 2019.

SCHWIRTZ Michael, *Top Secret Unit Seeks to Destabilize Europe, Security Officials Say*, The New York Times, October 8, 2019.

SENATE SELECT COMMITTEE ON INTELLIGENCE, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*.

ŠMÍD Tomáš - MAREŠ Miroslav, «Kadyrovtsy: Russia's Counterinsurgency Strategy and the Wars of Paramilitary Clans», *Journal of Strategic Studies*, vol. 38, n. 5, 2015.

SOLDATOV Andrei, *Russian foreign intelligence might be in for a mor prominent political role*, Raamoprusland, May 24, 2019.

SOULEIMANOV Emil A., *An Ethnography of Counterinsurgency: Kadyrovtsy and Russia's Policy of Chechenization*, Post-Soviet Affairs, vol. 31, n. 2, 2015.

STANOVAYA Tatiana, *GRU Exposure: A Sign of Internal Power Struggles?*, Riddle, October 16, 2018.

STANOVAYA Tatiana, *Why the Kremlin Can't Keep Its Chekists in Check*, Riddle, July 25, 2019. https://www.ridl.io.

STUPP Catherine, *Germany Seeks EU Sanctions for 2015 Cyberattack on Its Parliament*, Wall Street Journal, June 11, 2020.

SUVOROV Viktor, *Inside the Aquarium: The Making of a Top Soviet Spy*, MacMillan New York, 1985.

TASS, *First Naval Officer Nominated to Head Russia's GRU*, November 22, 2018.

TAYLOR Brian D., *State Building in Putin's Russia: Policing and Coercion After Communism* Cambridge University Press, Cambridge, 2011.

TELMANOV Denis, *GRU Headed by Igor Sergun*, Izvestia, December 26, 2011.

THOMAS Timothy L., *Russia's Reflexive Control Theory and the Military*, Journal of Slavic Military Studies, vol. 17, no. 2 (2004).

TROIANOVSKI Anton – NAKASHIMA Ellen, *How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels with the West*, Washington Post, December 28, 2018.

TURBIVILLE Graham H., «Organized Crime and the Russian Armed Forces», *Transnational*

Organized Crime vol. 1, n. 4, 1995.

Turovsky Daniil, *It's Our Time to Serve the Motherland: How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers*, Meduza, August 7, 2018.

Turovsky Daniil, *What Is the GRU? Who Gets Recruited to Be a Spy? Why Are They Exposed So Often?*, Meduza, November 6, 2018.

Udmantsev Vadim, «Боевое крещение 'мусульман'» (Battesimo del fuoco 'musulmano'), *ВПК*, n. 50, 29/12/2004. http://vpk-news.ru.

Urban Mike, *The Skripal' Files: The Life and Near Death of a Russian Spy*, Henr, Holt and Company , New York, 2018.

U.S. Congress, Senate Select Committee on Intelligence, *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, 5 vol., 2019-2020.

U.S. Department of Justice, *Former Army Special Forces Officer Charged in Russian Espionage Conspiracy*, press release, August 21, 2020.

U.S. Department of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, press release, October 19, 2020.

U.S. Department of Justice, *U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations*, press release, October 4, 2018.

Välisluureamet (Estonian Foreign Intelligence Service), *International Security and Estonia*, 2018.

Walker Shaun, *Alleged Russian Spies Sentenced to Jail over Montenegro Coup Plot*, The Guardian, May 9, 2019.

Walker Shaun - Georgieva Maria, *'I almost died': arms dealer whose poisoning may be linked to Skripal's'*, The Guardian, February 18, 2019.

Watts Clint, «Russia's Active Measures Architecture: Task and Purpose», *Alliance for Securing Democracy*, May 22, 2018.

Weiss Michael, *Aquarium Leaks. Inside the GRU's Psychological Warfare Program*, Free Russia Foundation, Washington DC, 2020.

Weiss Michael, *The Hero Who Betrayed His Country*, Atlantic, June 26, 2019; Estonian Foreign Intelligence Service, *International Security and Estonia*, Annual Report , 2019.

Whitmore Brian, *Resetting the Siloviki*, RFE/RL Power Vertical, October 21, 2011.

Yapparova Liliya, *The FSB's Personal Hackers*, Meduza, December 12, 2018.

Lieutenant A. FROMENT

L'ESPIONNAGE Militaire

LES FONDS SECRETS DE LA GUERRE ET LE SERVICE DES RENSEIGNEMENTS EN FRANCE ET A L'ÉTRANGER

PARIS
F. JUVEN, ÉDITEUR
10, RUE SAINT-JOSEPH, 10

Intelligence militare, guerra clandestina e Operazioni Speciali

Articles

Reviews