Fecha de recepción: 26/04/2026
Fecha de aceptación: 24/06/2026

La doctrina ciber-cinética rusa en la guerra de sexta generación:

del patrón Tallin-Hostomel al espacio estratégico argentino

The Russian Cyber-Kinetic Doctrine in the Sixth-Generation Warfare:

From the Tallinn-Hostomel Pattern to the Argentine Strategic Space

DIEGO ALEJANDRO DOMÍNGUEZ[1]

Escuela Naval Militar, Facultad de la Armada, Universidad de la Defensa Nacional (UNDEF), Argentina

drdominguez33@gmail.com

1 **Abogado por la Universidad Kennedy (UK), especialista en Ciencias Penales por la Universidad del Salvador (USAL) y magíster en Inteligencia Estratégica Nacional por la Universidad Nacional de la Plata (UNLP). Es docente en la Facultad de la Armada y Escuela Superior de Guerra Naval de la Universidad de la Defensa Nacional (UNDEF).**

Resumen

El presente artículo analiza la adaptación de la nueva doctrina cibercinética rusa como patrón operativo en su estrategia en las guerras de sexta generación (Slipchenko, 2002) recurrente que precede a las acciones convencionales del Kremlin desde 2007 hasta la actualidad, basado ello en la ciberguerra, la guerra electrónica y las acciones de inteligencia. Partiendo de los ataques distribuidos de denegación de servicio contra Estonia (Tallin, 2007), continuando con la guerra ruso-georgiana (Osetia del Sur, 2008), las operaciones contra Chechenia, la anexión de Crimea y el Euromaidán (2014), hasta la invasión a gran escala de Ucrania iniciada el 24 de febrero de 2022, se demuestra la consolidación de un *modus operandi* que combina ataques cibernéticos preparatorios, operaciones de inteligencia humana, sabotaje y guerra electrónica como antesala de la maniobra militar convencional. La reciente exposición pública del Centro 795 (Unidad Militar 75127), unidad ultrasecreta del Estado Mayor ruso revelada en marzo de 2026 por *The Insider* y *Der Spiegel*, ofrece un caso paradigmático para analizar las nuevas capacidades de operaciones encubiertas rusas y sus puntos de vulnerabilidad. Finalmente, se examina la penetración operativa de los servicios rusos en el espacio estratégico argentino –caso "Topos" del SVR (2012-2024), red "La Compañía" vinculada al GRU y al Proyecto Lakhta (2025)– y se proponen lineamientos para el fortalecimiento de las capacidades de ciberdefensa, contrainteligencia y marco normativo en la defensa nacional argentina.

Abstract

This article analyzes the adaptation of Russia's new cyber-kinetic doctrine as a recurring operational pattern within its strategy for sixth-generation warfare (Slipchenko, 2002), one that has preceded conventional Kremlin actions from 2007 to the present, grounded in cyberwarfare, electronic warfare and intelligence operations. Beginning with the distributed denial-of-service attacks against Estonia (Tallinn, 2007), continuing through the Russo-Georgian war (South Ossetia, 2008), operations against Chechnya, the annexation of Crimea and the Euromaidan (2014), and culminating in the full-scale invasion of Ukraine launched on February 24, 2022, the study demonstrates the consolidation of a *modus operandi* that combines preparatory cyberattacks, human intelligence operations, sabotage and electronic warfare as a prelude to conventional military maneuver. The recent public exposure of Center 795 (Military Unit 75127), an ultra-secret unit of the Russian General Staff revealed in March 2026 by The Insider and Der Spiegel, offers a paradigmatic case for examining Russia's new covert operations capabilities and their points of vulnerability. Finally, the article examines the operational penetration of Russian services into the Argentine strategic space

–the SVR “Moles” case (2012–2024), the “Company” network linked to the GRU and Project Lakhta (2025)– and proposes guidelines for strengthening cyberdefense and counterintelligence capabilities and normative framework of the Argentine National Defense.

Palabras clave: inteligencia operativa, ciberdefensa, operaciones encubiertas, Centro 795, defensa argentina

Keywords: sixth-generation warfare, Cyber-kinetic doctrine, Covert operations, Center 795, Argentine defense

Introducción

La guerra ruso-ucraniana iniciada el 24 de febrero de 2022 no inauguró un paradigma; lo confirmó. La integración de operaciones cibernéticas, inteligencia humana (HUMINT), sabotaje y guerra electrónica como antesala de la maniobra cinética convencional es, en rigor, un *modus operandi* consolidado por la Federación Rusa al menos desde el año 2007, cuando los ataques distribuidos de denegación de servicio (DDoS) contra Estonia inauguraron lo que la literatura especializada denominaría "guerra híbrida" o "guerra de zona gris" (Stratcom Centre of Excellence, 2019). La aparente novedad de cada conflicto sucesivo –Georgia 2008, las dos guerras chechenas y sus prolongaciones, Crimea y el Euromaidán 2014, Ucrania 2022– no es sino la repetición refinada de un patrón doctrinario que combina, con creciente sofisticación, los planos no cinéticos y cinéticos de la confrontación.

El presente trabajo se inscribe en la tradición que Heráclito de Éfeso (siglo VI a.C.) condensó en su célebre fragmento DK 22 B 53 sobre el *Pólemos* –el conflicto– como "padre y rey de todas las cosas" (Heráclito, 2007). Si el conflicto es la condición ontológica de las relaciones humanas y de los Estados, su forma contemporánea exige reconceptualizar las categorías clásicas de la inteligencia operativa, la ciberdefensa y las operaciones encubiertas. La sentencia clausewitziana que define a la guerra como "continuación de la política con otros medios" (Clausewitz, 1832/2005, p. 119) conserva plena vigencia, pero reclama una reinterpretación: los *otros medios* contemporáneos incluyen, además del fuego y el acero, los algoritmos de denegación de servicio, las redes botnets distribuidas, los servicios civiles de traducción automática como conducto inadvertido de inteligencia y las operaciones de influencia mediante analistas ficticios y grafitis pagados.

Este artículo persigue un triple objetivo. Primero, demostrar la existencia de una doctrina ciber-cinética rusa como continuum histórico verificable mediante el análisis comparado de cinco escenarios paradigmáticos entre 2007 y 2022. Segundo, analizar la reciente exposición pública del Centro 795 ruso (Unidad Militar 75127) como caso paradigmático del rediseño de las capacidades encubiertas del Kremlin tras los fracasos operacionales de la antigua Unidad 29155 del Glávnoye Razvedyvátelnoye Upravléniye (GRU). Y, tercero, examinar la penetración operativa rusa en el espacio estratégico argentino –documentada en los casos "Topos" del Servicio de Inteligencia Exterior (SVR), la red "La Compañía" vinculada al GRU y al Proyecto Lakhta–, proponiendo lineamientos concretos para el fortalecimiento de las capacidades de ciberdefensa, contrainteligencia y marco normativo en la defensa nacional argentina.

El abordaje es interdisciplinario, combinando las herramientas de la inteligencia estratégica, las relaciones internacionales, el derecho internacional público y la prospectiva estratégica. Se utilizan exclusivamente

fuentes abiertas (OSINT) de calidad verificable sobre investigaciones periodísticas conjuntas de *Der Spiegel* y *The Insider* (Grozev, 2026), análisis del Modern War Institute de la Academia Militar de West Point (Chincharadze, 2025), publicaciones del *Atlantic Council* y del NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), informes del Congressional Research Service de la Biblioteca del Congreso de los Estados Unidos (CRS, 2025) y del George C. Marshall European Center for Security Studies (Galeotti, 2019), entre otros. La metodología se asienta en el análisis cualitativo comparado, complementado con triangulación de fuentes para garantizar el rigor académico exigible a la materia.

La doctrina ciber-cinética rusa: el materialismo histórico dialéctico 2.0 aplicado a la nueva estrategia rusa (2007-2022)

La Informatsionnoye Protivoborstvo ((Информационное противоборство) y Maskirovka en la Era Digital

Para comprender el accionar ruso en el ciberespacio y en el ámbito de las operaciones encubiertas, es imperativo adentrarse en su cosmovisión estratégica. A diferencia de las doctrinas occidentales que tienden a compartimentar las operaciones cibernéticas técnicas de las operaciones de información, el pensamiento militar ruso fusiona ambas dimensiones bajo el concepto unificado de *Informatsionnoye protivoborstvo* (IPb) o "confrontación de la información" (Chincharadze, 2025).

Como señala Chincharadze (2025), esta doctrina, articulada y refinada por estrategas rusos, establece que la información es un arma estratégica que debe ser utilizada tanto en tiempos de paz como de guerra para influir en las creencias y comportamientos del adversario, degradar su cohesión social y neutralizar su infraestructura técnica. La IPb rusa se divide en dos vertientes sinérgicas:

1. Operaciones informático-técnicas: enfocadas en el ataque, explotación y defensa de redes informáticas, abarcando desde ataques de Denegación de Servicio Distribuido (DDoS) hasta el despliegue de *malware* destructivo o *wipers* (Chincharadze, 2025).

2. Operaciones informático-psicológicas**:** destinadas a manipular la cognición de las poblaciones objetivo, los liderazgos políticos y las tropas enemigas, empleando tácticas de desinformación, fábricas de *trolls*, *deep fakes* y narrativas polarizantes (Cariboni, 2026; Chincharadze, 2025).

Esta fusión doctrinal se complementa orgánicamente con la milenaria táctica rusa de la *Maskirovka* (engaño militar). Históricamente utilizada para

ocultar movimientos de tropas o intenciones operativas mediante camuflaje y señuelos físicos, la *Maskirovka* ha mutado hacia el plano cibernético y cognitivo. Hoy en día, implica la ofuscación de la atribución de ciberataques, la negación plausible en operaciones encubiertas y la saturación del ecosistema informativo con versiones contradictorias de un mismo evento para inducir la parálisis decisional en el adversario (Chincharadze, 2025; Domínguez, 2025).

Genealogía de la Doctrina Ciber-Cinética: desde el Cáucaso hasta el Dniéper

El nivel de sofisticación y destructividad que la inteligencia militar rusa exhibe en la actualidad es el resultado de un extenso proceso de aprendizaje empírico. A lo largo de casi dos décadas, Rusia ha utilizado los conflictos periféricos como campos de pruebas iterativos para calibrar la eficacia de sus ciberarmas y operaciones de influencia (Chincharadze, 2025; Domínguez, 2025).

Tallin 2007: el "Soldado de Bronce" y el bautismo de la guerra cibernética interestatal

El 27 de abril de 2007, en respuesta a la decisión del gobierno estonio de reubicar el monumento del Soldado de Bronce –memorial soviético erigido en 1947 en pleno centro de Tallin como tributo a los soldados del Ejército Rojo caídos durante la Segunda Guerra Mundial– desde una plaza céntrica hacia el Cementerio Militar de las Fuerzas de Defensa, comenzó una campaña sostenida de ataques cibernéticos contra los principales sitios web del Estado estonio (CCDCOE, 2008). El monumento poseía una doble carga simbólica de gran densidad: para la mayoría étnica estonia, representaba el recordatorio de la ocupación soviética que había seguido al Pacto Molotov-Ribbentrop; para la minoría rusoparlante (aproximadamente el 25 % de la población), encarnaba la memoria de la victoria sobre el nazismo y la legitimidad histórica de la presencia rusa en el Báltico.

Durante veintidós días, hasta el 18 de mayo de 2007, las páginas del parlamento (*Riigikogu*), los ministerios de Asuntos Exteriores, Defensa y Justicia, los principales bancos comerciales (Hansabank en particular), los medios de comunicación y los proveedores de servicios de internet sufrieron oleadas sucesivas de DDoS coordinados desde botnets globales que en su pico llegaron a comprometer cerca de un millón de computadoras "zombi" distribuidas en más de cincuenta países (Ottis, 2008). Los métodos empleados –*ping flood*, *UDP flood*, *TCP SYN exploit*, *HTTP flood*– evidenciaron una sofisticación técnica creciente conforme avanzaba la campaña, con un punto de inflexión claro el 4 de mayo, cuando comenzó la segunda oleada, esta vez profesionalmente coordinada y dirigida específicamente contra el sistema bancario.

La sofisticación creciente del ataque, que pasó de una primera fase descoordinada y aparentemente "patriótica" a una segunda fase profesional con instrucciones detalladas circulando en foros rusoparlantes y arrendamiento de botnets habitualmente utilizadas para distribución de *spam* comercial, sumada a la negativa rusa a cooperar con la asistencia legal mutua solicitada por Estonia bajo el tratado bilateral vigente (MLAT), sugiere fuertemente la responsabilidad estatal o cuasi-estatal del agresor (Ministerio de Defensa de Estonia, 2008). El 28 de junio de 2007, la Procuraduría Suprema de la Federación Rusa rechazó formalmente la solicitud estonia, alegando que las diligencias procesales propuestas no se encuadraban en el tratado aplicable –argumento técnicamente débil que la mayoría de los observadores interpretó como gesto político de protección a los autores materiales–.

El Kremlin nunca reconoció autoría; alegó que se trataba de "patriotas hacktivistas", actuando espontáneamente en defensa de la memoria de los soldados soviéticos. Pero la coordinación temporal con las protestas de la minoría rusa en Estonia (que dejaron un muerto y más de 150 heridos), el origen rusoparlante mayoritario del tráfico malicioso, las medidas económicas hostiles simultáneas (reducción de exportaciones de petróleo crudo a las refinerías estonias, prohibiciones de importación) y la retórica oficial agresiva del entonces canciller Serguéi Lavrov configuran lo que la literatura especializada denomina "negación plausible" (*plausible deniability*) como técnica deliberada de operación encubierta. Mark Galeotti (2019) caracteriza este fenómeno como propio de la "adhocracia" del aparato de seguridad ruso, donde múltiples actores y agencias generan sus propias iniciativas en busca de favor del Kremlin, configurando una arquitectura de responsabilidad difusa pero estratégicamente coordinada.

Las consecuencias estratégicas fueron monumentales y conformaron, paradójicamente, el mayor fortalecimiento de la ciberdefensa europea de las últimas décadas. En mayo de 2008, la Organización del Tratado del Atlántico Norte (OTAN) creó, en la propia Tallin, el Centro de Excelencia Cooperativo de Ciberdefensa (CCDCOE), institución multinacional dedicada al desarrollo de doctrina, capacitación y cooperación entre Estados aliados. De este centro emanaría posteriormente el *Manual de Tallin sobre Derecho Internacional Aplicable a la Guerra Cibernética*, en sus dos ediciones (2013 y 2017), bajo la dirección del jurista estadounidense Michael Schmitt (2017). El Manual estableció noventa y cinco "reglas en letra negra" sobre la aplicabilidad del derecho internacional al ciberespacio, fijando entre otros aspectos que los Estados poseen soberanía sobre los componentes físicos de la infraestructura informática localizada en su territorio, aun cuando carezcan de soberanía sobre internet en sí. La Cumbre de Varsovia de 2016 consagró formalmente al ciberespacio como dominio operacional de la OTAN, equiparable a tierra, mar, aire y espacio, y reconoció que un ciberataque de gravedad suficiente contra un Estado miembro podría activar la cláusula de defensa colectiva del Artículo

5 del Tratado de Washington (OTAN, 2016).

El caso Tallin estableció además una lección estratégica que excede su contexto báltico. La ambigüedad atribucional –la dificultad técnica y política para asignar responsabilidad estatal a un ataque cibernético– constituye un atributo deliberado, no una limitación accidental, de la nueva doctrina ofensiva.

La capacidad para operar por debajo del umbral del Artículo 5, evitando una respuesta colectiva automática de la alianza, configuró desde 2007 el modelo del *gray zone warfare* o conflicto de zona gris, concepto que Frank Hoffman (2007) había anticipado meses antes en su trabajo seminal sobre las "guerras híbridas" del siglo XXI.

Guerra en Georgia, año 2008: la primera integración ciber-cinética en operaciones combinadas

El 8 de agosto de 2008, mientras los tanques rusos cruzaban el túnel de Roki rumbo a Osetia del Sur en respuesta a la ofensiva georgiana sobre Tsjinvali, los sitios web del gobierno georgiano se encontraban bajo asedio cibernético desde hacía más de dos semanas (Markoff, 2008). La operación combinada constituye, según el Atlantic Council, "el primer caso histórico de ataque cibernético y kinético combinado" (Healey, 2019). Las ofensivas DDoS comenzaron el 19 de julio de 2008, casi tres semanas antes de las hostilidades convencionales, focalizadas inicialmente en la página presidencial georgiana –dominio del presidente Mijeíl Saakashvili–, luego escaladas hacia el parlamento, los ministerios, los principales medios de comunicación y el sistema bancario.

La sofisticación había aumentado significativamente respecto de Tallin. Además de los ataques DDoS (denegación de servicios) por inundación, los atacantes utilizaron inyecciones SQL (*SQL injections*) para penetrar servidores y técnicas de *defacement* (alteración visual de páginas) para fines psicológicos –notoriamente, las páginas del parlamento georgiano y del Ministerio de Relaciones Exteriores fueron alteradas con imágenes que comparaban al presidente Saakashvili con Adolf Hitler (Wentworth, 2008)–.

El sitio "stopgeorgia.ru" funcionaba como portal centralizado de coordinación, ofreciendo listas de objetivos georgianos prevalidados, herramientas de ataque descargables, instrucciones operativas paso a paso y reportes de impacto en tiempo real, evidenciando una arquitectura operacional preestablecida que necesariamente requirió semanas o meses de planificación previa (Tikk, Kaska y Vihul, 2010).

El bloqueo cibernético contra Georgia fue rastreado a cinco sistemas autónomos –cuatro en Rusia y uno en Turquía– controlados por el sindicato criminal Russian Business Network (RBN), una de las principales redes de cibercrimen mundial con sede en San Petersburgo, cuyos vínculos con figuras

políticamente influyentes en Rusia han sido documentados (Markoff, 2008).

El gobierno georgiano, virtualmente "ciberbloqueado" y con dificultades severas para comunicarse internacionalmente –en un momento crítico en que su presidente intentaba contactar a líderes occidentales que se encontraban de vacaciones o asistiendo a la ceremonia inaugural de los Juegos Olímpicos de Pekín–, adoptó una decisión sin precedentes, es decir, relocalizó sus activos digitales oficiales en servidores de Estados Unidos, Estonia y Polonia, sin solicitar autorización previa al gobierno estadounidense, configurando un complejo problema de derecho internacional sobre neutralidad cibernética (Korns y Kastenberg, 2009). Particularmente significativo es el aspecto multi-vector de la campaña rusa contra Georgia, que combinó tres planos coordinados: el ciberataque, la presión energética y el ataque kinético.

El 5 de agosto de 2008, el oleoducto Bakú-Tiflis-Ceyhan (BTC) –pieza clave de la estrategia occidental para diversificar el suministro energético europeo eludiendo el territorio ruso– sufrió una explosión cerca de Refahiye, en territorio turco, atribuida inicialmente al Partido de los Trabajadores del Kurdistán (PKK), pero respecto de la cual existe evidencia circunstancial de un sofisticado ataque informático contra los sistemas de control y seguridad del oleoducto que provocó incremento de presión y la subsiguiente explosión (Robertson y Riley, 2014). Esto sugiere una integración temprana entre ciberataque industrial y geoestrategia energética que precede en años al concepto popularizado de "infraestructura crítica como objetivo estratégico".

El Bumgarner Report de la US Cyber Consequences Unit, publicado en agosto de 2009, concluyó que "los planificadores militares rusos conocían la operación con antelación" y que "la mayoría de las herramientas de ciberataque utilizadas en la campaña parecen haber sido escritas o adaptadas específicamente para la campaña contra Georgia" (Bumgarner y Borg, 2009). La temporalidad –los ataques DDoS preceden por semanas a la operación cinética– configura un patrón doctrinario que se repetirá sistemáticamente. Vemos entonces que el plano cibernético opera como configurador del campo de batalla antes de que se mueva el primer blindado, debilitando la capacidad de respuesta gubernamental, manipulando la percepción pública internacional y aislando comunicacionalmente al Estado víctima en el momento decisivo.

Chechenia y el laboratorio del Cáucaso Norte

Si bien las dos guerras chechenas (1994-1996 y 1999-2009) precedieron la era cibernética madura, constituyeron el laboratorio primario donde la inteligencia rusa refinó técnicas de manipulación informativa, operaciones psicológicas (PSYOPS), sabotaje y eliminación selectiva de líderes opositores. La ejecución selectiva del comandante checheno Abdulvahid Edelguiriev en Estambul en 2015, atribuida a Anatoliy Chepiga –el mismo operador del GRU

vinculado al envenenamiento de Sergei Skripal en Salisbury (2018)– evidencia la continuidad personal y doctrinaria entre los teatros caucásico y europeo (Bellingcat, 2019).

Más relevante aún para el presente análisis es el caso de Denis Alimov, operador del Centro 795 detenido en Bogotá en febrero de 2026, presenta un perfil biográfico anclado en el Cáucaso Norte, con vínculos personales directos con Ramzán Kadírov, líder supremo de Chechenia (*The Insider*, 2026). La proyección de operadores formados en el laboratorio checheno hacia operaciones extraterritoriales en Europa y América Latina constituye uno de los hilos doctrinarios menos estudiados, pero más significativos de la inteligencia rusa contemporánea.

Crimea y Euromaidán 2014: consolidación de la doctrina ciber-cinética rusa como metodología estratégica

El intervalo 2013-2014 representa el momento de madurez doctrinaria. En febrero de 2013, el entonces Jefe del Estado Mayor General Valery Gerasimov publicó en *Voyenno-Promyshlennyi Kuryer* su célebre artículo "El valor de la ciencia en la previsión", texto que la literatura occidental terminaría denominando –no sin imprecisiones– "Doctrina Gerasimov" (McDermott, 2016).

En el escrito, el general reflexiona sobre las "Primaveras Árabes" y las llamadas "revoluciones de colores" (Ucrania 2004, Georgia 2003 y Kirguistán 2005) interpretándolas como resultado de operaciones de injerencia occidental, y propone una concepción no lineal del conflicto donde "las reglas de la guerra han cambiado" y "el rol de medios no militares para alcanzar objetivos políticos y estratégicos ha crecido y, en muchos casos, ha excedido el poder del armamento en su efectividad" (Gerasimov, 2013, p. 24).

La proporción que el general sugiere es de cuatro a uno. La idea central es el uso de medios no militares cuádruples respecto de los militares clásicos, configurando un paradigma operativo donde el conflicto se libra preeminentemente en los planos informativo, cibernético, económico, diplomático y de operaciones especiales encubiertas, dejando al combate convencional como remate final cuando el adversario ya está estructuralmente debilitado.

En medio de las protestas del Euromaidán de noviembre de 2013, que escalaron a la Revolución de la Dignidad de febrero de 2014, Rusia desplegó la denominada "Operación Armagedón" (mediados de 2013), una campaña sostenida de *spear-phishing* contra funcionarios del gobierno, fuerzas de seguridad y militares ucranianos para sustraer información sensible mediante el envío de correos electrónicos personalizados con archivos adjuntos infectados con *malware* (Chincharadze, 2025).

El grupo APT28 (también conocido como *Fancy Bear*, *STRONTIUM*, GRU

Unit 26165) y APT29 (*Cozy Bear*, vinculado al SVR) ejecutaron operaciones complementarias de robo de credenciales, instalación de troyanos persistentes y mapeo de redes informáticas críticas ucranianas con varios meses de antelación a la fase cinética (Mandiant, 2014). Tres días antes del referéndum ilegal en Crimea –el 13 de marzo de 2014– se ejecutó un ataque DDoS de ocho minutos contra las redes informáticas del gobierno ucraniano (CERT-UA, 2014).

La temporalidad ya no es casual: ya es marca doctrinaria. Paralelamente, los célebres "hombrecitos verdes" sin insignias (*little green men*) –operadores de las fuerzas especiales rusas Spetsnaz GRU desplegados con uniformes despojados de identificación– ejecutaron la toma del Parlamento autónomo de Simferópol y de las instalaciones estratégicas de la península el 27 de febrero de 2014, hora de máxima debilidad del aparato estatal ucraniano tras la huida del presidente Víktor Yanukóvich.

Esta operación combinó el control encubierto de instalaciones gubernamentales, neutralización de bases militares ucranianas en territorio de la península de Crimea, en conjunto con la manipulación informativa masiva mediante medios rusoparlantes locales, y referéndum convocado en condiciones que ningún observador internacional independiente certificó como libres y limpias.

El reconocimiento posterior por Vladímir Putin –en su entrevista para el documental *Crimea: Camino a la Patria*, difundido en marzo de 2015– de que se trataba efectivamente de fuerzas regulares rusas, confirmó la deliberada arquitectura de negación inicial.

La "Operación Crimea" configuró el mal definido modelo de "guerra híbrida" que la doctrina occidental terminaría conceptualizando bajo las plumas de figuras como Mark Galeotti, Frank Hoffman y la propia OTAN (Hoffman, 2007; Galeotti, 2016). Conceptualmente, tanto Slipchenko como Gareev y Gerasimov, nunca usaron estos términos, dado que se trata de diferencias de ideas rectoras que se venía desarrollando por parte de OTAN desde las guerras africanas del siglo XX.

En paralelo, en el Donbás, los grupos armados separatistas de las autoproclamadas "República Popular de Donetsk" (RPD) y "República Popular de Lugansk" (RPL) operaron desde abril de 2014 como vehículo de la denominada "guerra por delegación" (*proxy warfare*), con presencia documentada de oficiales del GRU y mercenarios del Grupo Wagner –entonces emergente bajo el mando de Yevgeny Prigozhin y Dmitri Utkin (Marten, 2019)–. El derribo del vuelo MH17 de Malaysia Airlines el 17 de julio de 2014 sobre territorio del Donbás, ejecutado por un sistema de misiles tierra-aire Buk-M1 transportado desde la 53° Brigada Antiaérea de Misiles de Kursk, según establecieron las investigaciones del Joint Investigation Team neerlandés-australiano-belga-ucraniano-malasio, dejó 298 civiles muertos y constituye uno de los crímenes de guerra mejor documentados del conflicto.

La continuidad operativa post 2014 incluyó que el ataque cibernético contra la red eléctrica ucraniana del 23 de diciembre de 2015, ejecutado por GRU Unit 74455 (*Sandworm*), que dejó sin energía a aproximadamente 230.000 personas en la región de Ivano-Frankivsk durante varias horas y constituyó el primer apagón eléctrico documentado del mundo causado por un ciberataque exitoso (CERT-UA, 2016); el ataque similar contra la subestación Pivnichna de Kiev el 17 de diciembre de 2016, que afectó al 20 % del consumo nocturno de la capital; y el devastador ataque NotPetya de junio de 2017, también atribuido a Sandworm, que causó pérdidas globales superiores a los 10.000 millones de dólares estadounidenses según evaluaciones de la Casa Blanca (Greenberg, 2018).

Hostomel y Kiev 2022: el patrón aplicado a escala de invasión total

El 24 de febrero de 2022, exactamente a las 04:00 horas locales –una hora antes del cruce fronterizo terrestre desde Bielorrusia, Rusia y Crimea–, el GRU Unit 74455 (*Sandworm*) ejecutó el ataque cibernético contra la red satelital comercial Viasat KA-SAT, inhabilitando miles de módems en Ucrania y, por efecto de derrame transfronterizo, en Alemania, Francia, Polonia y la República Checa, afectando incluso a 5.800 turbinas eólicas en Alemania que dependían del servicio para mantenimiento remoto (Viasat, 2022). El patrón doctrinario –ciberataque preparatorio + operación encubierta + maniobra cinética– quedaba confirmado a escala de invasión continental, ahora ejecutado con varios años de aprendizaje técnico acumulado.

Horas antes, también se había desplegado un *malware* destructivo denominado FoxBlade contra la infraestructura digital ucraniana, sumándose a las cepas previas HermeticWiper, IsaacWiper y WhisperGate, detectadas en las semanas previas a la invasión (Microsoft Threat Intelligence, 2022).

El propósito doctrinario era evidente, se trataba de degradar la capacidad de mando, control y comunicaciones (C3) ucranianas en el momento crítico, paralizar los sistemas bancarios, desinformar a la población mediante desfiguración de portales oficiales, y crear el caos comunicacional necesario para que la maniobra cinética encontrase un adversario desorganizado.

A las 05:00 horas, mientras misiles balísticos Iskander y de crucero Kalibr golpeaban infraestructura militar y administrativa ucraniana, un asalto aerotransportado del 31° Regimiento de Asalto Aéreo de la Guardia y de la 11° Brigada de Asalto Aéreo de la Guardia, transportadas en una flotilla de helicópteros Ka-52 (apoyo de fuego), Mi-8 (transporte) y Mi-24/35 (escolta), partió desde la base de Pribytki en Bielorrusia con destino al aeropuerto Antonov de Hostomel, apenas 25 kilómetros al noroeste de Kiev (Zabrodskyi *et al*., 2022).

La operación se denominaba “Día Uno” y constituía la pieza maestra del plan ruso original: el aeropuerto debía ser tomado en las primeras horas

para establecer un puente aéreo masivo –utilizando los aviones de carga estratégicos Il-76 disponibles en mayor número– mediante el cual desplegar el grueso de la fuerza aerotransportada VDV en las afueras de Kiev.

La capital sería sitiada en cuestión de tres días, el gobierno de Volodímir Zelenski sería decapitado o forzado a la capitulación, y un gobierno títere sería instalado bajo el modelo aplicado en Praga 1968.

El plan fracasó estrepitosamente, y su fracaso constituye uno de los puntos de inflexión militares más relevantes del siglo XXI.

La defensa ucraniana, organizada por elementos de la 4° Brigada de Reacción Rápida de la Guardia Nacional, la 72° Brigada Mecanizada y unidades del Servicio de Inteligencia Militar (HUR), había sido alertada con suficiente antelación –merced en parte a la inteligencia compartida por Estados Unidos y el Reino Unido durante las semanas previas, y también a las propias capacidades ucranianas refinadas durante ocho años de conflicto en el Donbás– y montó una operación de fuego concentrado de artillería y sistemas antiaéreos portátiles (MANPADS) sobre la pista que impidió la consolidación del aterrizaje (Zabrodskyi *et al*., 2022).

Los Ka-52 sufrieron pérdidas significativas; la 80° Brigada de Asalto Aéreo de la Guardia ucraniana lanzó un contraataque a las pocas horas que terminó retomando el aeropuerto, dejando la pista inutilizable mediante daño deliberado y vehículos calcinados en posición.

La consecuencia operativa fue catastrófica para Rusia, pues sin Hostomel funcional, los Il-76 que despegaron desde Pskov con el grueso de la VDV debieron regresar a sus bases. La columna blindada del 35° Ejército Combinado de Armas que avanzaba desde Bielorrusia por la autopista P-02 hacia Kiev quedó sin punto de unión aerotransportada en la retaguardia ucraniana, y el famoso convoy de 64 kilómetros de longitud quedó atascado durante días en condiciones de pantano primaveral, sufriendo emboscadas con drones Bayraktar TB2 turcos y misiles antitanque Javelin estadounidenses.

La lección operativa de Hostomel-Kiev 2022 es múltiple: primero, la planificación rusa subestimó gravemente la voluntad de combate ucraniana y la calidad de la inteligencia compartida occidental. Segundo: el componente cibernético-electrónico, aun ejecutado conforme al patrón doctrinario probado, no logró degradar suficientemente la capacidad ucraniana de mando y control distribuido, en parte por la ayuda inmediata de servicios civiles como Starlink, desplegado por iniciativa del vice primer ministro Mykhailo Fedorov, mediante solicitud directa a Elon Musk, y operativo en territorio ucraniano apenas 48 horas después del inicio de la invasión (Recalde Melnechenko, 2025). Tercero: la asimetría de información táctica de tiempo real generada por la combinación de drones de reconocimiento + sistemas satelitales civiles + red móvil resiliente + aplicaciones de mensajería cifrada constituye una

novedad operacional que altera la ecuación clásica de superioridad numérica. Por último, cuarto: la doctrina ciber-cinética rusa funciona excepcionalmente cuando el adversario carece de profundidad estratégica, como evidencian los casos Estonia, Georgia y Crimea, pero encuentra sus límites cuando el adversario posee densidad institucional, voluntad política y respaldo internacional consistentes.

La crisis de la Unidad 29155 y el rediseño operacional ruso

Anatomía de un fracaso: del Salisbury al desmantelamiento

Entre 2018 y 2022, la histórica Unidad 29155 del GRU –responsable de operaciones encubiertas en el extranjero desde, al menos, 2008; entre ellas, el envenenamiento de Sergei y Yulia Skripal en Salisbury (Reino Unido, 2018), el intento de golpe en Montenegro (2016), las explosiones en depósitos de munición checos (Vrbětice, 2014), y los presuntos casos del Síndrome de La Habana– sufrió una serie de fracasos operacionales que la convirtieron, en palabras de un evaluador interno ruso citado por *The Insider*, en un "lastre" (Grozev, 2026).

Los errores fueron sorprendentemente básicos para una organización de inteligencia militar de gran potencia, pues pasaportes falsos emitidos en serie con números consecutivos –que permitieron a investigadores como Bellingcat reconstruir redes completas siguiendo la secuencia numérica–, identidades reutilizadas, historiales de viaje inconsistentes, y operadores cuyos datos biométricos quedaron registrados en sistemas migratorios occidentales tras múltiples cruces fronterizos.

Decenas de agentes quedaron expuestos públicamente con nombres, fotografías y datos personales circulando en investigaciones de fuente abierta (*Bellingcat*, 2019; *The Insider*, 2019).

La creación del Centro 795: arquitectura de negación reforzada

En diciembre de 2022, mediante orden directa del Estado Mayor General de las Fuerzas Armadas de la Federación Rusa, bajo el mando del General Gerasimov, se ordenó la creación de la Unidad Militar 75127, conocida internamente como "Centro 795" (Fitsanakis, 2026). Hacia junio de 2023 estaba completamente dotada con aproximadamente 500 oficiales (Grozev, 2026). El diseño persiguió cuatro objetivos doctrinarios: máxima compartimentación operativa; cobertura corporativa civil; ciclo completo de operaciones y reporte directo al núcleo del poder militar.

A diferencia de la 29155, que operaba dentro de la estructura jerárquica tradicional del GRU, el Centro 795 reporta directamente al Jefe del Estado Mayor o a un viceministro de Defensa, evadiendo las cadenas de mando

tradicionales y, con ello, los puntos de filtración burocrática. El comando operacional recae en el Coronel Denis Fisenko, veterano de la Unidad Alfa del Centro de Propósito Especial del FSB, condecorado tres veces con la Orden del Valor y autor de programas de entrenamiento para operaciones especiales (*The Insider*, 2026).

La cobertura corporativa es la innovación más significativa: el Centro 795 está formalmente incrustado dentro del "Concern Kalashnikov", fabricante histórico de armamento ruso integrado al conglomerado estatal Rostec, presidido por Sergey Chemezov –antiguo colega de Vladímir Putin en el KGB durante su servicio en Dresde durante la Guerra Fría (Mezha, 2026)–. El financiamiento adicional proviene del oligarca Andrey Bokarev, copropietario histórico de Kalashnikov.

En consecuencia, los oficiales del Centro 795 figuran formalmente como empleados de una empresa privada del sector defensa, con salarios y contratos justificables como actividad industrial regular. La base operativa se ubica en el Patriot Park de Kúbinka, complejo militar-industrial al oeste de Moscú, donde Kalashnikov mantiene un edificio administrativo de dos plantas –denominado TMU-1– junto al centro de reclutamiento y entrenamiento de la unidad de drones Rubikon (Militarnyi, 2026).

Estructura de ciclo completo: tres direcciones

El Centro 795 está organizado en tres direcciones que materializan el principio de "ciclo completo": Inteligencia, Asalto y Apoyo de Combate.

La Dirección de Inteligencia, la más extensa y compleja, comprende nueve departamentos especializados. El Departamento 11 ejecuta inteligencia de fuentes abiertas (OSINT) mediante explotación de redes sociales, bases de datos públicas e imágenes satelitales comerciales.

El Departamento 12, el más sensible, gestiona redes de agentes humanos (HUMINT) en el extranjero y está integrado mayoritariamente por veteranos de la antigua Unidad 29155 –dirigidos por el oficial Anatoli Kovalev–, lo que evidencia la continuidad operacional pese a la reorganización formal. El Departamento 13 conduce inteligencia de señales (SIGINT) e interceptación electrónica, incluyendo una estación de interceptación satelital. Los Departamentos 14 y 15 operan vehículos aéreos no tripulados (UAVs) Orlán y Eleron para reconocimiento óptico operacional y táctico. Los Departamentos 16, 17 y 18 ejecutan vigilancia terrestre directa para confirmación visual de objetivos. El Departamento 19 agrupa francotiradores cuya integración en la Dirección de Inteligencia –y no en la de Asalto– sugiere que su función primaria es la eliminación selectiva, no el apoyo de combate convencional (*The Insider*, 2026).

La Dirección de Asalto comprende cuatro departamentos integrados cada uno por cuatro grupos de combate autónomos. La compartimentación es

extrema: ningún grupo conoce las operaciones de los otros, garantizando que la captura o filtración de uno no comprometa al resto. Los perfiles incluyen exmiembros de fuerzas especiales, operadores del Servicio Federal de Protección (FSO), especialistas en inserción aérea y operaciones encubiertas. La Dirección de Apoyo de Combate, finalmente, dota al Centro 795 de capacidades militares completas e independientes: blindados (incluidos tanques T-90A), artillería de cohetes múltiples Smerch, obuses D-30, defensa aérea, sistemas antitanque, logística, mantenimiento, fortificación, medicina militar y desactivación de explosivos (EOD). En la práctica, el Centro 795 puede sostener operaciones de alta intensidad sin apoyo externo, configurándose como "ejército en la sombra" autosuficiente (Lounsbury, 2026).

Reclutamiento selectivo y arquitectura bielorrusa

La selección de personal sigue una lógica diferenciada respecto del reclutamiento militar convencional. Aproximadamente un tercio de los candidatos es rechazado, y el énfasis recae sobre experiencia comprobada en operaciones complejas, no en formación académica. Una fracción significativa proviene de unidades de élite del FSB (Alfa y Vympel) y del GRU. Una innovación particularmente relevante consiste en el reclutamiento de veteranos de la Unidad Alfa del KGB bielorruso –notoriamente, el coronel reservista Dmitri Drozdov (jefe de Estado Mayor del Centro 795) y el mayor reservista Sergei Radkevich (jefe de la Dirección de Inteligencia)–, ambos sin antecedentes institucionales rusos (*Reform.news*, 2026).

La lógica debía ser transparente, consistente en que los oficiales sin trayectoria registrada en organismos rusos no atraen el escrutinio de las contrainteligencias occidentales y permiten una capa adicional de negación plausible. Ambos ingresaron al Centro 795 a través de Kalashnikov, sin que su afiliación a servicios militares o de seguridad fuese declarada.

Del error a la paradoja de Google Translate: cuando la ciberdefensa pasiva derrota a la inteligencia ofensiva

El 24 de febrero de 2026, exactamente cuatro años después del cruce fronterizo ruso a Ucrania, Denis Alimov –operador clave del Centro 795– fue detenido en el Aeropuerto Internacional El Dorado de Bogotá por la Oficina Central Nacional de Interpol-Bogotá, integrada en la Policía Nacional de Colombia, tras arribar en un vuelo de Turkish Airlines procedente de Estambul (Fitsanakis, 2026). Su captura derivó en la exposición pública del Centro 795 mediante la investigación conjunta Der Spiegel-The Insider de marzo de 2026.

El mecanismo de la exposición es paradójico y aleccionador. Alimov, exagente de la policía antidisturbios OMON de Stávropol y posteriormente operador de la Unidad Alfa del FSB, había sido encomendado en 2025 con la

organización de una operación de eliminación o secuestro de dos disidentes chechenos miembros de la familia Sakaev –incluido el primer ministro en el exilio de la no reconocida República Chechena de Ichkeria, Ahmed Sakaev–, residentes en Europa Occidental y Estados Unidos (*Insider*, 2026). El presupuesto operativo era considerable: USD 60.000 entregados como adelanto y promesa de hasta USD 1.500.000 por objetivo eliminado.

Alimov dependía de un intermediario en territorio estadounidense: Darko Đurović, ciudadano serbio residente en Nueva York, encargado de coordinar contactos locales y aspectos logísticos. El problema técnico fundamental fue lingüístico: Alimov no hablaba ni inglés ni serbio, y Đurović no hablaba ruso (manejaba inglés deficiente adquirido tras años en Nueva York). Para superar la barrera, ambos recurrieron a un servicio civil de traducción automática: Google Translate. El uso del traductor implicaba que cada instrucción operativa, cada coordenada de objetivo, cada referencia armamentística (Glock 17, 21, 22, adquiribles en Montenegro), cada descripción de víctima ("viven en una villa blanca cerca del mar con cerca blanca y un símbolo islámico en la entrada") quedará registrada en servidores ubicados en jurisdicción estadounidense (Mezha, 2026).

El Buró Federal de Investigaciones (FBI), mediante orden judicial bajo la *Foreign Intelligence Surveillance Act* (FISA), accedió a los registros del proveedor en tiempo real (*intelNews*, 2026). No hubo necesidad de intervención telefónica, instalación de micrófonos ni penetración informática activa: la operación de inteligencia ofensiva más sofisticada del aparato militar ruso quedaba derrotada por una herramienta de uso civil cotidiano cuyos servidores residen en jurisdicción del adversario.

La lección doctrinaria es de profundas implicancias. La ciberdefensa contemporánea ya no se limita a la protección de redes propias; comprende el aprovechamiento estratégico de la dependencia adversaria de infraestructura digital civil controlada por jurisdicciones aliadas. Es lo que la doctrina estadounidense denomina, en el marco de la *Cyberspace Solarium Commission*, "ciberdefensa por densidad infraestructural" (CSC, 2020).

En el caso del Centro 795, la combinación de barrera lingüística y dependencia de servicios civiles destruyó la arquitectura de negación plausible cuidadosamente construida.

Argentina en el tablero del Humint: la penetración operativa de los servicios rusos en el espacio estratégico nacional

La discusión doctrinaria precedente no es un ejercicio abstracto. La proyección operativa rusa hacia América Latina y, específicamente, hacia la República Argentina, está documentada con creciente precisión en investigaciones de fuente abierta y en las actividades públicas del Estado argentino.

Caso "Topos": el SVR en Buenos Aires (2012-2024)

El caso de María Mayer Mishustina y Ludwig Gisch –matrimonio integrado en realidad por Anna Dultseva y Artem Dultsev, oficiales del Servicio de Inteligencia Exterior ruso (SVR), operando bajo identidades argentinas falsas– constituye el ejemplo más documentado de penetración profunda de los servicios rusos en territorio nacional. La pareja se estableció en Buenos Aires en 2012, obtuvo identidades argentinas legítimas mediante manipulación de partidas de nacimiento y documentación falsa, y procreó dos hijos de nacionalidad argentina –Sofía y Daniel, desconocedores tanto del idioma ruso como de la verdadera filiación de sus padres hasta el momento de la detención–, antes de trasladarse a Liubliana, Eslovenia, como base operativa europea (Alconada Mon, 2024).

La operativa argentina del matrimonio Dultsev sigue el patrón clásico del programa de "ilegales" del Departamento S del SVR –heredero directo del Directorio S del Primer Directorio Principal del KGB soviético, conceptualmente fundado por Pavel Sudoplatov en los años cuarenta y operativamente refinado durante la Guerra Fría–, en el cual oficiales rusos se establecen durante años en países de cobertura, adquiriendo lenguaje, profesión, identidad, vínculos sociales y, eventualmente, familia, antes de ser proyectados hacia los teatros operacionales prioritarios. Buenos Aires fue elegida deliberadamente como "fábrica de identidades" por una combinación de factores: porosidad documental relativa del aparato registral argentino, ausencia histórica de capacidades robustas de contrainteligencia específicamente focalizadas en el SVR, presencia de comunidades de origen eslavo que facilitaban inserción social, y carácter de país receptivo de migraciones europeas, lo que normaliza acentos y orígenes que en otros teatros podrían generar alertas.

Detenidos por las autoridades eslovenas en diciembre de 2022, fueron entregados a Moscú en agosto de 2024 en el marco del mayor intercambio de espías entre Occidente y Rusia desde la Guerra Fría –operación que incluyó el regreso del periodista del *Wall Street Journal* Evan Gershkovich y del marino estadounidense Paul Whelan, así como la liberación del asesino del FSB Vadim Krasikov, entonces preso en Alemania por el homicidio del exiliado checheno Zelimján Khangoshvili en el parque Tiergarten de Berlín en 2019 (Universidad de Navarra, 2024)–. El intercambio incluyó dieciséis personas presas en Rusia y Bielorrusia liberadas a cambio de los Dultsev, otros seis espías rusos detenidos en distintos países (incluido el periodista español Pablo González Yagüe), y la familia completa.

El caso Topos no es anecdótico, pues revelan la utilización sistemática del territorio argentino como plataforma de proyección operativa rusa hacia Europa. Los Dultsev no fueron caso aislado; investigaciones posteriores –particularmente el trabajo de Hugo Alconada Mon en *La Nación* y el libro *Topos* (2024)– han documentado, al menos, otros tres casos sospechosos en

el mismo período, sugiriendo que Buenos Aires operó durante más de una década como nodo significativo del programa de ilegales del SVR para el teatro europeo.

La consecuencia para la soberanía argentina es directa: el Estado fue funcionalmente instrumentado como cobertura de operaciones de inteligencia hostiles contra terceros países, sin que el aparato de Defensa Nacional ni los servicios de inteligencia hubieran detectado o neutralizado oportunamente la red.

"La Compañía" y el Proyecto Lakhta: GRU + SVR + Wagner

En octubre de 2025, el portavoz presidencial reveló la desarticulación de un grupo de presuntos espías rusos vinculados al GRU, encabezado por Lev Konstantinovich Andriashvili e Irina Iakovenko, ciudadanos rusos residentes en Argentina (*Buenos Aires Times*, 2025).

El grupo denominado "La Compañía" (*The Company*), y que se vinculaba al Proyecto Lakhta, operación de injerencia rusa supervisada originalmente por Yevgeny Prigozhin –líder del Grupo Wagner, fallecido en agosto de 2023 en el accidente aéreo del avión Embraer Legacy 600, que cayó cerca de Tver dos meses después del fallido motín de junio de 2023– y dirigida desde el exterior contra audiencias en Estados Unidos, Europa, Ucrania y América Latina (*The Record*, 2025).

El Proyecto Lakhta es el mismo aparato que estuvo detrás de la Internet Research Agency (IRA) de San Petersburgo, organización procesada por el Departamento de Justicia de Estados Unidos en febrero de 2018 mediante el *indictment* del fiscal especial Robert Mueller por interferencia en las elecciones presidenciales de 2016.

Las actividades documentadas de "La Compañía" en territorio argentino incluyeron la difusión coordinada de contenidos en redes sociales mediante cuentas falsas y bots, influencia sobre organizaciones de la sociedad civil, fundaciones y organizaciones no gubernamentales receptoras de financiamiento encubierto, conducción de *focus groups* con ciudadanos argentinos para mapear vulnerabilidades narrativas de la opinión pública local, y recolección sistemática de inteligencia política para uso en favor de los intereses del Kremlin (Adorni, 2025). Una investigación de *Open Democracy* publicada en abril de 2026 –en colaboración con *The Continent*, All Eyes on Wagner/INPACT, Forbidden Stories, iStories y el Dossier Center– documentó el encargo de 89 grafitis pintados en la vía pública de Buenos Aires bajo la consigna "Argentina no necesita una guerra ajena", el despliegue de pancartas anti-Ucrania en partidos de fútbol del campeonato local, y la publicación encubierta de artículos firmados por analistas inexistentes –entre ellos, un tal "Gabriel di Taranto", presunto egresado de la Universidad Nacional de Avellaneda, autor de veinte artículos en *Diario Registrado*, C5N y Ámbito– en

medios argentinos de circulación masiva (*OpenDemocracy*, 2026).

Es particularmente significativo que, según la documentación filtrada al consorcio internacional, Andriashvili y Iakovenko abandonaron Argentina rumbo a San Petersburgo días después de que sus nombres fueran expuestos públicamente por el gobierno argentino en octubre de 2025, pero retornaron al país pocas semanas después, según investigación publicada por el *Foro Argentino de Periodismo* en enero de 2026.

Al cierre de la presente investigación, ambos continuaban residiendo en Buenos Aires, lo que evidencia las severas limitaciones del marco normativo argentino para la persecución administrativa o penal de operaciones de injerencia que no configuran tipos penales clásicos de espionaje, pero que erosionan visiblemente la integridad del proceso democrático y la soberanía decisional argentina.

Argentina como nodo logístico: el patrón latinoamericano

Investigación periodística independiente (Rojas, 2026) documenta que las redes de operadores rusos en América Latina utilizan al menos cuatro nodos como rutas de tránsito y bases operativas de Bogotá y Cartagena en Colombia, Buenos Aires en Argentina, Punta Cana en República Dominicana, y Ciudad de México.

Cada caso presenta particularidades adaptadas al entorno local, pero todos comparten la doble función de tránsito hacia objetivos europeos o norteamericanos y de plataforma de operaciones activas en la región. La detención de Alimov en Bogotá no es un episodio aislado: es una pieza del mapa operativo continental.

Implicancias para la defensa nacional argentina

El análisis precedente arroja conclusiones operativas de aplicación inmediata para la defensa nacional argentina. Se proponen cinco ejes de acción interconectados:

Primero: fortalecimiento de la ciberdefensa estatal

La experiencia estonia de 2007 enseña que los Estados con dependencia digital significativa son vulnerables a campañas DDoS coordinadas en momentos de crisis política. Argentina, con un grado creciente de digitalización en banca, administración pública (SUBE, AFIP, sistemas previsionales del ANSES, MiArgentina), salud (historia clínica electrónica nacional, sistemas hospitalarios provinciales), servicios esenciales (red eléctrica interconectada, sistemas de control de oleoductos y gasoductos como el Néstor Kirchner) y telecomunicaciones, debe consolidar capacidades CERT con protocolos

de respuesta inmediata. El modelo del CCDCOE de la OTAN –pese a no ser Argentina miembro de la alianza, condición de "socio" o *partner* sí accesible– ofrece referencias técnicas valiosas, particularmente, el ejercicio anual *Locked Shields* en el que participan más de treinta naciones simulando defensa coordinada ante intrusiones cibernéticas, y el Manual de Tallin como marco de derecho aplicable que el Ministerio de Defensa debería adoptar formalmente como referencia doctrinaria (Schmitt, 2017). La integración del Comando Conjunto de Ciberdefensa con CSIRTs provinciales y sectoriales –banca privada, energía, telecomunicaciones, salud– mediante protocolos de intercambio de indicadores de compromiso (IOC) en tiempo real es, a juicio del autor, una asignatura pendiente del Estado argentino, particularmente urgente dada la documentada presencia operativa rusa en territorio nacional.

Segundo: contrainteligencia frente a operadores ilegales

Los casos Topos y La Compañía evidencian la utilización de Argentina como base de identidades para programas de ilegales del SVR (Departamento S) y como teatro de operaciones del GRU mediante redes de influencia. La Secretaría de Inteligencia (SIDE), reorganizada conforme al Decreto 614/2024, requiere capacidades reforzadas de contrainteligencia específica frente a servicios extranjeros, particularmente en el cruce automatizado de bases de datos migratorias (Migraciones), registros de naturalización (Registro Nacional de las Personas), patrones de tránsito por nodos de cobertura (Aeropuerto Internacional de Ezeiza, Aeroparque Jorge Newbery, paso fronterizo Ciudad del Este), vínculos corporativos con empresas vinculadas al complejo militar-industrial ruso (entidades vinculadas a Rostec, Kalashnikov, RT en Español, Sputnik Mundo) y monitoreo OSINT sobre cuentas de redes sociales que reproducen consistentemente líneas narrativas del Proyecto Lakhta. La cooperación con servicios aliados –dentro del marco constitucional argentino y de las leyes de inteligencia nacional Nº 25.520 y Nº 27.126– resulta inevitable, dado el carácter transnacional del fenómeno; la negativa pretoriana a cooperar bajo argumentos de "soberanía aislacionista" garantizaría únicamente que Argentina permanezca como agujero negro de inteligencia regional, instrumentado por servicios hostiles sin capacidad propia de respuesta.

Tercero: marco normativo de operaciones de influencia y *lawfare* extranjero

El derecho penal argentino, en su redacción actual, presenta zonas grises significativas para perseguir operaciones de injerencia que no configuran tipos penales clásicos del Capítulo VIII del Código Penal (traición a la patria, espionaje en sentido estricto del artículo 222, revelación de secretos militares), pero que erosionan la integridad del proceso democrático y la soberanía decisional.

La experiencia comparada de la Foreign Agents Registration Act (FARA) estadounidense de 1938 –reforzada notablemente desde 2017 frente a operaciones rusas y chinas– y de la Ley de Influencia Extranjera del Reino Unido de 2023, ofrecen modelos parciales adaptables al sistema federal argentino respetando sus propias tradiciones constitucionales.

Una ley de transparencia de injerencia extranjera o un debate serio en base a una nueva ley nacional de inteligencia que obligara a rever el sistema de propaganda y publicidad para evitar operaciones, instruida desde el exterior por gobiernos o entidades vinculadas a gobiernos extranjeros, constituiría una herramienta de defensa democrática proporcional al desafío.

Cuarto: doctrina de operaciones combinadas ciber-cinéticas para las Fuerzas Armadas

El patrón doctrinario ruso 2007-2022 exige que las Fuerzas Armadas argentinas integren componentes cibernéticos y de guerra electrónica en sus planeamientos operacionales convencionales, no como adiciones marginales sino como elemento estructurante de la maniobra. El Comando Conjunto de Ciberdefensa, creado en 2014, requiere recursos materiales y humanos consistentes con la magnitud del desafío, así como un marco doctrinario propio que adapte las experiencias internacionales a la realidad estratégica nacional.

La incorporación sistemática de capacidades C5ISR (Comando, Control, Comunicaciones, Computadoras, Cibernética, Inteligencia, Vigilancia y Reconocimiento) en las Brigadas y Comandos del Ejército Argentino, la modernización de los sistemas de guerra electrónica de la Armada Argentina particularmente en el Comando de la Aviación Naval y los buques de la flota de mar, y el desarrollo de capacidades de defensa aérea contra drones y municiones merodeadoras (*loitering munitions*) por la Fuerza Aérea Argentina –experiencia documentada en Avdiivka, Bakhmut y otros teatros del conflicto ucraniano– constituyen pilares de modernización doctrinaria de aplicación inmediata.

Quinto: dimensión Atlántico Sur y proyección estratégica nacional

El eje Atlántico Sur y Antártida, declarado por el propio Ministerio de Defensa de la Nación como uno de sus núcleos temáticos prioritarios, presenta vulnerabilidades específicas frente al patrón ruso analizado.

La cuestión Malvinas, los espacios marítimos jurisdiccionales argentinos, la presencia de potencias extra-regionales en el Atlántico Sur y la disputa territorial argentina sobre el sector antártico configuran un conjunto de intereses nacionales cuya defensa exige capacidades cibernéticas e inteligencia adecuadas. La operatividad de las redes submarinas de comunicaciones

ópticas que conectan Argentina con el resto del mundo –particularmente los cables del consorcio SAm-1 y Tannat– constituye infraestructura crítica cuya protección, dado el documentado historial ruso de operaciones contra cables submarinos en el Báltico y el Mar del Norte (incidentes Nord Stream 2022, cable C-Lion1 2023, cables Estonia-Finlandia 2024), debe formar parte central del planeamiento de defensa nacional integrado con cooperación de Brasil, Uruguay y otros actores regionales relevantes.

Sexto: educación y construcción de capacidades

La formación de civiles y militares en inteligencia estratégica, ciberdefensa y operaciones encubiertas requiere expansión sostenida y recursos consistentes en el tiempo. La Universidad de la Defensa Nacional (UNDEF), a través de la Escuela Superior de Guerra Conjunta, la Facultad del Ejército, la Facultad de la Armada y la Facultad de la Fuerza Aérea, junto con espacios universitarios civiles como la Maestría en Inteligencia Estratégica Nacional (UNLP), la Maestría en Defensa Nacional (FADENA), y los programas de la Escuela Nacional de Inteligencia (ENI), constituyen la infraestructura académica disponible.

Su consolidación con financiamiento estable, intercambios internacionales con instituciones aliadas (CCDCOE de Tallin, Marshall Center, NPS Monterey, Escuela Superior de Guerra Naval brasileña, IDF Cyber Defense Academy israelí), producción editorial sostenida –de la que la propia Revista Defensa Nacional es ejemplo virtuoso– e incorporación de contenidos sobre operaciones encubiertas contemporáneas, doctrina ciber-cinética rusa, marco jurídico aplicable al ciberespacio y análisis de casos como el Centro 795 son condición *sine qua non* para cualquier estrategia seria de defensa nacional en el siglo XXI.

La experiencia argentina demuestra que cuando esa infraestructura se desarticula –como ocurrió en distintos períodos de la historia institucional reciente– el costo no se paga inmediatamente sino a través del tiempo, en forma de penetración no detectada de servicios extranjeros, captación de funcionarios, manipulación informativa y, eventualmente, debilitamiento de la capacidad decisional autónoma del Estado argentino frente a actores externos.

Consideraciones finales

El *Pólemos* heracliteano –el conflicto como condición ontológica de la civilización, padre y rey de todas las cosas– ha mutado en su forma, pero no en su esencia. La doctrina ciber-cinética rusa que recorre Tallin (2007), Tiflis (2008), las dos Chechenias y sus prolongaciones operacionales, Crimea y el Maidán (2014), y Hostomel-Kiev (2022) evidencia la consolidación de un patrón

operativo que el Centro 795 lleva ahora a sus desarrollos más sofisticados de operaciones encubiertas extraterritoriales. La paradoja de su exposición pública mediante una herramienta civil de traducción automática –Google Translate, jurisdicción servidor estadounidense, orden FISA, captura en El Dorado– señala la complejidad creciente del campo de batalla contemporáneo: ningún diseño operacional, por más compartimentado y refinado en su arquitectura de negación plausible, sobrevive a la densidad infraestructural digital del adversario sin pagar costos significativos. La inteligencia operativa y táctica del siglo XXI opera, así, en una tensión permanente entre la sofisticación de las técnicas ofensivas —reclutamiento selectivo de élites del FSB y del KGB bielorruso, cobertura corporativa Kalashnikov-Rostec, arquitectura de ciclo completo, financiamiento oligárquico en las sombras— y la inexorable porosidad de los servicios civiles digitales que cualquier operador, por más entrenado, termina utilizando.

Para Argentina, la exposición es doble. Por un lado, el país está documentadamente integrado en la geografía operativa rusa global, sea como fábrica de identidades para ilegales del SVR (caso Topos, 2012-2024), sea como teatro de operaciones de influencia del GRU y el aparato Wagner-Lakhta (caso La Compañía, 2025-2026), sea como nodo logístico latinoamericano del Centro 795 dentro del corredor que vincula a Bogotá, Cartagena, Buenos Aires, Punta Cana y Ciudad de México. Por otro lado, el país posee capacidades incipientes pero insuficientes para responder a la magnitud y sofisticación del desafío. La construcción de capacidades de ciberdefensa, contrainteligencia, marco normativo, doctrina militar conjunta y educación estratégica no es un lujo de especialistas: es una necesidad existencial para preservar la soberanía decisional, la integridad democrática y la capacidad de proyección nacional en el escenario multipolar conflictivo del siglo XXI, particularmente respecto del Atlántico Sur, la Antártida y la cuestión Malvinas.

Como advertía Carl von Clausewitz (1832/2005, p. 119), "la guerra es la continuación de la política con otros medios". Los otros medios contemporáneos incluyen, además del fuego y el acero clausewitziano, los bits, los algoritmos, las redes sociales, los traductores automáticos como conducto inadvertido de inteligencia, las identidades civiles fabricadas a lo largo de décadas, los grafitis pagados como instrumento de presión política, los analistas ficticios firmando artículos en medios de circulación masiva. El estratega que ignore esta evolución abdica de su responsabilidad fundamental: pensar el conflicto en sus términos reales, no en sus formas pretéritas. La Defensa Nacional argentina, en el sentido más amplio del concepto –no reducido a sus componentes militares sino comprensivo de la integridad institucional, democrática y soberana del Estado–, exige precisamente esa lucidez doctrinaria. El presente artículo aspira modestamente a contribuir a su construcción.

Bibliografía

Alconada Mon, H. (2024). *Topos: La verdadera historia de los espías rusos en Buenos Aires*. Planeta.

Bellingcat Investigation Team. (2019). *Identifying GRU Officers in Unit 29155*. Disponible en: https://www.bellingcat.com.

Buenos Aires Times. (19 de junio de 2025). Argentina's spies expose alleged Russian disinformation group. Disponible en: https://www.batimes.com.ar.

Bumgarner, J. y Borg, S. (2009). *Overview by the US-CCU of the cyber campaign against Georgia in August of 2008*. United States Cyber Consequences Unit.

CERT-UA. (2014). *Reporte sobre ataques cibernéticos durante el referéndum de Crimea*. Equipo de Respuesta ante Emergencias Informáticas de Ucrania.

CERT-UA. (2016). *Análisis del ciberataque contra la red eléctrica ucraniana del 23 de diciembre de 2015*. Kiev: Equipo de Respuesta ante Emergencias Informáticas de Ucrania.

Cariboni, D. (2 de abril de 2026). Leña al fuego: La campaña rusa para influir en los medios de comunicación de Argentina. *openDemocracy*. Disponible en: https://www.opendemocracy.net/es/argentina-rusia-propaganda-medios-periodismo-milei-ucrania-putin-trump-prigozhin/.
Chincharadze, K. (30 de julio de 2025). From Georgia to Ukraine: Seventeen Years of Russian Cyber Capabilities at War. Modern War Institute at West Point. https://mwi.westpoint.edu/from-georgia-to-ukraine-seventeen-years-of-russian-cyber-capabilities-at-war/.

Clausewitz, C. von. (2005). *De la guerra* (Trad. C. Fortea). La Esfera de los Libros (Trabajo original publicado en 1832).

Congressional Research Service [CRS]. (diciembre de 2025). *Russia's Foreign Intelligence Services* (Informe IF12865). Library of Congress. Disponible en: https://www.congress.gov/crs-product/IF12865

Cyberspace Solarium Commission [CSC]. (2020). *Final Report*. U.S. Cyberspace Solarium Commission.

Domínguez, D. A. (2025). *El rol geopolítico de los recursos naturales y sus implicancias en la seguridad energética: perspectivas empíricas desde Rusia y Europa*. [Tesis de maestría, Universidad Nacional de La Plata (UNLP)]. SEDICI.

Disponible en: https://doi.org/10.35537/10915/183932.

Fitsanakis, J. (16 de marzo de 2026). Investigation uncovers previously unknown Russian covert action unit. *intelNews.org*. Disponible en: https://intelnews.org/2026/03/16/01-3432/

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? *Small Wars & Insurgencies*, *27*(2), 282-301.

Galeotti, M. (2019). *The intelligence and security services and strategic decision-making*. Garmisch-Partenkirchen: George C. Marshall European Center for Security Studies.

Gerasimov, V. (27 de febrero de 2013). Tsennost nauki v predvidenii ["El valor de la ciencia en la previsión"]. *Voyenno-Promyshlennyi Kuryer*, *8*(476), 2-3.

Greenberg, A. (22 de agosto de 2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired Magazine*. Disponible en: https://www.wired.com.

Grozev, C. (13 de marzo de 2026). Lost in translation: How Russia's new elite hit squad was compromised by an idiotic lapse in tradecraft. *The Insider*. Disponible en: https://theins.press/en/inv/290235.

Healey, J. (15 de agosto de 2019). Russian cyber strategy and the war against Georgia. *Atlantic Council*. Disponible en: https://www.atlanticcouncil.org.

Heráclito de Éfeso. (2007). *Fragmentos* (Ed. R. Mondolfo). Siglo XXI.

Hoffman, F. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Potomac Institute for Policy Studies.

Jefatura de Gabinete del PEN (octubre de 2025). Comunicado oficial sobre la desarticulación de la red "La Compañía". Vocería Presidencial de la Nación Argentina, Casa Rosada, Buenos Aires.

Korns, S. W. y Kastenberg, J. E. (2009). Georgia's cyber left hook. *Parameters: U.S. Army War College Quarterly*, *38*(4), 60-76.

Lounsbury, D. (2026). Russia's shadow unit: Inside "Center 795", the Kremlin's new covert warfare command. Disponible en: https://danlounsbury.com/russian-center-795-covert-ops-group/.

Mandiant. (2014). *APT28: A window into Russia's cyber espionage operations?* Mandiant Corporation.

Markoff, J. (12 de agosto de 2008). Before the gunfire, cyberattacks. *The New York Times*.

Marten, K. (2019). Russia's use of semi-state security forces: The case of the Wagner Group. *Post-Soviet Affairs*, *35*(3), 181-204.

McDermott, R. N. (2016). Does Russia have a "Gerasimov doctrine"? *Parameters: U.S. Army War College Quarterly*, *46*(1), 97-105.

Mezha (13 de marzo de 2026). The Insider Exposes Center 795 as secret Russian unit behind assassinations and abductions. Disponible en: https://mezha.net/eng/bukvy/the_insider_exposes_center/.

Microsoft Threat Intelligence Center (2022). *Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine*. Microsoft Corporation.

Militarnyi. (14 de marzo de 2026). New Russian secret special forces unit for high-priority missions Center 795: Structure, command and exposure. Disponible en: https://militarnyi.com.

Ministerio de Defensa de Estonia. (2008). *Cyber security strategy*. Tallinn: Government of Estonia.

NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE]. (2008). *Cyber attacks against Estonia: Legal lessons learned*. Tallinn: CCDCOE.

openDemocracy (9 de abril de 2026). How Russia exploited Argentina's media to run influence operations. Disponible en: https://www.opendemocracy.net. Consultado el 21 de abril de 2026.

Organización del Tratado del Atlántico Norte [OTAN] (2016). *Cumbre de Varsovia: Comunicado de los Jefes de Estado y de Gobierno*. NATO.

Ottis, R. (2008). *Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective*. Tallinn: NATO CCDCOE.

Recalde Melnechenko, F. (2025). Starlink en el escenario bélico: Análisis del impacto de las constelaciones satelitales civiles en la guerra ruso-ucraniana. *Revista Defensa Nacional*, 11, 175-210.

Reform.news (14 de marzo 2026). Belarusian KGB Alpha veterans serve in Russian secret special unit. Disponible en: https://reform.news.

Robertson, J. y Riley, M. (10 de diciembre de 2014). Mysterious '08 Turkey pipeline blast opened new cyberwar era. *Bloomberg News*.

Rojas, J. (2026). *Centro 795 (Unidad 75127): La red de inteligencia militar más secreta de Rusia ha sido expuesta* [Documental audiovisual]. Armapedia. Disponible en: https://www.youtube.com.

Slipchenko, V. (2002). Voyny Novogo Pokoleniya: Distantsionnyye i Bezkontaktnyye (p. 23). ["Wars of the New Generation: Remote and Contactless"]. Olma-Press.

Schmitt, M. N. (Ed.) (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2a ed.). Cambridge University Press.

Stratcom Centre of Excellence. (2019). *Hybrid threats: 2007 cyber attacks on Estonia*. Riga: NATO Strategic Communications Centre of Excellence.

The Insider (2019). *GRU's Unit 29155: An invisible force used by Putin abroad*. Disponible en: https://theins.press. Consultado el 21 de abril de 2026.

The Insider (13 de marzo de 2026). Lost in translation: How Russia's new elite hit squad was compromised. Disponible en: https://theins.press/en/inv/290235.

The Record. (2025, 19 de junio). Argentina uncovers suspected Russian spy ring behind disinformation campaigns. Disponible en: https://therecord.media

Tikk, E., Kaska, K. y Vihul, L. (2010). *International cyber incidents: Legal considerations*. Tallinn: NATO CCDCOE.

Universidad de Navarra (2024). A spy story: Russian moles in Argentina. *Global Affairs and Strategic Studies*. Disponible en: https://en.unav.edu/web/global-affairs.

Viasat (30 de marzo de 2022). *KA-SAT network cyber attack overview*. Carlsbad: Viasat Inc.

Wentworth, T. (12 de agosto de 2008). You've got malice: Russian nationalists waged a cyber war against Georgia. *Newsweek*.

Zabrodskyi, M., Watling, J., Danylyuk, O. y Reynolds, N. (2022). *Preliminary lessons in conventional warfighting from Russia's invasion of Ukraine: February-July 2022*. Royal United Services Institute (RUSI).