

# Control Reflexivo Ruso: teoría militar y aplicaciones

*Russian reflexive control: military theory and applications*

**Resumen:** El desarrollo de la doctrina de la seguridad de la información en la Federación de Rusia ha estado funcionando desde el primer decenio de este siglo. Actualmente, la doctrina se aplica tanto a nivel gubernamental como como instrumento de aplicación del poder militar. Este artículo presenta cómo la Federación Rusa está manejando sus acciones basadas en la Teoría del Control reflexivo (CR). Dado que la teoría implica la comprensión rusa de la información, los datos técnicos, el contenido cognitivo y los "recursos de información" se entienden como tecnológicos y humanos, así como, son empleados por el sistema de Comunicación Estratégica (Relaciones Públicas, Diplomacia Pública y Sistemas de Seguridad de la Información), para un propósito específico. En este trabajo también se describe la interacción de la CR con la doctrina Germazinov, las actividades de guerra de la información, con el uso de medidas no militares, el uso de la guerra cibernética, los medios sociales y las medidas de "caos controlado", todo con el objetivo de garantizar el éxito en el combate y el desarrollo ruso.

**Palabras clave:** Control Reflexivo; Comunicación Estratégica; Guerra Información /Cibernética; Operaciones de influencia y caos controlado.

**Abstract:** The development of information security doctrine in the Russian Federation has been in the works since the first decade of this century. Currently, the doctrine is applied both at the governmental level and as an instrument for the application of military power. The present work presents how the Russian Federation is managing its actions based on the Reflective Control (CR) theory. As the theory involves the Russian understanding of information, technical data, cognitive contents and "information resources" are understood as technological and human, as well as being employed by the Strategic Communication system (Public Relations, Public Diplomacy and Security Systems of the Information), for a specific purpose. This work also describes the interaction of the CR with Doctrina Germazinov, the Information Warfare activities, with the use of non-military measures, the use of Cyber Warfare, social media and the "Controlled Chaos" measures, all with the objective to ensure success in Russian combat and development.

**Keywords:** Reflective Control; Strategic Communication; Cyber/ Information Warfare; Influence Operations and Controlled Chaos.

**João Ricardo da Cunha Croce Lopes**   
Exército Brasileiro. Escola de Comando e  
Estado-Maior do Exército.  
Rio de Janeiro, RJ, Brasil  
ricardo@croce.ggf.br

**Recibido: 19 set. 2021**

**Aprobado: 20 nov. 2021**

**COLEÇÃO MEIRA MATTOS**

**ISSN on-line 2316-4891 / ISSN print 2316-4833**

<http://ebrevistas.eb.mil.br/index.php/RMM/index>



## 1 Introducción

Uno de los principales objetivos del comandante en la guerra es interferir en el proceso de toma de decisiones del enemigo. Este objetivo a menudo se logra a través de la desinformación, el camuflaje u otras estrategias. Para Rusia, uno de estos métodos básicos es el uso de la teoría de control reflexivo, que se define como una forma de transmitir información especialmente preparada a un socio u oponente con el fin de persuadirlos para que tomen una decisión predeterminada, deseable para el iniciador de la acción (ЛЕФЕВР; СМОЛЯН, 2010). Este método se puede utilizar contra "procesadores de toma de decisiones" humanos o máquinas.

A pesar del hecho de que la teoría se ha desarrollado durante mucho tiempo en Rusia, todavía se encuentra en constante actualización en el día de hoy.

En este artículo, se presentará el aspecto militar del concepto ruso de control reflexivo y su papel como arma en la guerra de la información de acuerdo con la doctrina militar de Defensa de la Federación Rusa.

El conocimiento presentado aquí fue el resultado de estudios realizados en Moscú, así como en la profundización llevada a cabo a través de los textos, doctrinas, artículos y conferencias a los que tuve acceso. Aunque hay varios manuales y vasto material, muchos de ellos no fueron puestos a disposición directamente por mis "camaradas". La traducción de términos técnicos también fue un factor de complicación, incluso después de más de 10 (años) de contacto con el idioma ruso. Por estas razones, este artículo tomó mucho tiempo para ser presentado.

## 2 Desarrollo

La naturaleza de la Teoría del Control reflexivo (CR) existe mucho más que conceptos similares de guerra de información y operaciones de información. De hecho, apareció en la literatura militar soviética hace 40 años. Vladimir A. Lefebvre definió el control reflexivo como "un proceso en el que uno de los oponentes transmite las otras razones para la toma de decisiones" (ЛЕФЕВР, 1984, p. 14).

El desarrollo de la Teoría del control reflexivo pasó por cuatro períodos:

- Investigación (desde principios de la década de 1960 hasta finales de la década de 1970);
- Orientado a la práctica (desde finales del decenio de 1970 hasta principios del decenio de 1990);
- Desempeño psicológico / pedagógico (de principios a mediados del decenio de 1990);
- Trabajo psicosocial (desde finales del decenio de 1990).

La Unión Soviética, y después de 1991, las fuerzas armadas rusas han estado explorando durante mucho tiempo las técnicas de uso de la teoría del control reflexivo (*especialmente a nivel táctico y operacional*): como disfraz (*error*), a los efectos de desinformación así como para influir en los procesos de toma de decisiones del enemigo. Por ejemplo, el ejército ruso ya poseía en 1904, la escuela militar de camuflaje. En 1929, esta Escuela sentó las bases para el concepto de camuflaje y creó guías para las generaciones futuras (*Maskarovka*).

El Control Reflexivo también es visto como un medio de guerra de información. Por ejemplo, el General de División N. I. Turko, profesor de la Academia del Estado Mayor de la Federación de Rusia, estableció un vínculo directo entre las guerras de información, las operaciones y las estrategias de control reflexivo. Señaló que la manifestación más destructiva, en la tendencia a confiar en la fuerza militar, se debe al posible impacto del control reflexivo de la parte opuesta, a través del desarrollo adecuado de la teoría y la práctica de la guerra de la información, que es más importante que el uso directo de la fuerza militar.

Turko creía que el control reflexivo es el arma de información más importante para lograr objetivos militares que la "potencia de fuego" tradicional. Este punto de vista fue formado en gran parte por su creencia de que el uso estadounidense de armas de información durante la Guerra Fría hizo mucho más para derrotar a la Unión Soviética que cualquier otra arma, así como fue la fuente que causó el colapso. Por último, Turko mencionó la gobernanza reflexiva como un método para lograr la superioridad geopolítica y como un medio para gestionar las negociaciones militares, un área que debería ser más reconocida por los países que entablan tales negociaciones con los rusos.

Por definición, el control reflexivo ocurre cuando **el órgano de gobierno transmite un sistema controlado de motivos y motivos que servirán como excusa para llegar a una solución deseable, pero las intenciones reales se mantienen en absoluto secreto** (ТУРКО; МОДЕСТОВ, 1996).

"Reflexión" animar ciertos procesos para simular el razonamiento de un enemigo o para simular un posible comportamiento del enemigo, obligándolo a tomar una decisión desfavorable para él. De hecho, el enemigo llega a una solución basada en **representación de la situación que formó**, incluyendo la ubicación de destacamentos y estructuras en el lado opuesto, así como las intenciones conocidas por él de los oponentes.

Las ideas iniciales para la toma de decisiones se forman principalmente sobre la base de la inteligencia, otros datos y factores que se basan en un conjunto sostenible de conceptos, conocimientos, ideas y, finalmente, experiencia. Este conjunto se conoce comúnmente como un "filtro" que ayuda al comandante a separar la información necesaria de los datos inútiles, los datos verdaderos de los falsos, y así sucesivamente.

En los procesos de toma de decisiones militares, el proceso "asistido por hombre-máquina" es más frecuente. Actualmente, los sistemas automatizados de toma de decisiones solo por qué las máquinas aún no están aprobadas (SUTYAGIN, 2015). El adversario puede tratar de influir en el ser humano; y, por otro proceso, el adversario puede tratar de influir en la máquina.

En todos los procesos de toma de decisiones, se enfatiza la importancia de la recolección y evaluación de información recurrente, así como un enfoque integral para permitir a los planificadores crear líneas de acción (LAç) para sus ejecuciones, así como modelos para la LAç de los oponentes. De esta manera, las líneas de acción se basan principalmente en la inteligencia y la información proporcionada por diversos sistemas de conciencia situacional (CS), sistemas de armas y similares. Por lo tanto, los procesos de toma de decisiones dependen en gran medida de la recopilación de datos que sean reales, correctos y oportunos. La información inexacta y / o irrelevante, así como los retrasos en la presentación pueden perjudicar gravemente el proceso de toma de decisiones. En el contexto de la toma de decisiones asistida por máquina, esto significa que se puede introducir información falsa,

irrelevante o prematura al ser humano, a la máquina o a ambos. El CR ruso actúa y ambos procesos 02 (dos) – Humano y Humano asistido por máquina.

La tarea principal del control reflexivo es también explorar, como herramienta, la moralidad, los factores psicológicos y de otro tipo, así como las características personales de los comandantes. En este último caso, los datos biográficos, los hábitos y las diferencias psicológicas pueden utilizarse en actos engañosos. En una guerra donde se utiliza el control reflexivo, el partido con la más alta calidad de "reflexión" (*más capaz de imitar los pensamientos del otro lado o predecir su comportamiento*) tendrá mejores oportunidades de ganar.

La calidad de la "reflexión" depende de un gran número de factores, el más importante de ellos – la habilidad analítica, la erudición general, la esfera del conocimiento sobre el enemigo y la experiencia. El autor militar Coronel S. Leonenko (ЛЕОНЕНКО, 1995) agregó que en el pasado, la estrategia era la principal herramienta de control reflexivo, pero hoy en día los "trucos" y el camuflaje han reemplazado al método.

Aunque la terminología formal del control reflexivo no existía en el pasado, las partes opuestas en realidad la usaron intuitivamente al tratar de identificar y chocar con los pensamientos de los demás, así como planear y cambiar sus impresiones de sí mismos, provocando una decisión equivocada (engañosa).

Si tiene éxito, el CR en el enemigo permite influir en los planes militares y la conciencia de la situación, así como, sus acciones. Así, el control reflexivo se centra más en el elemento subjetivo menos tangible del "arte militar" que en la "Ciencia Militar" más objetiva.

Lograr un Control Reflexivo exitoso **requiere un estudio profundo de la "naturaleza interna" del enemigo, sus ideas y conceptos**; Leonenko los describió como un "filtro" a través del cual pasan todos los datos sobre el mundo exterior. Un control Reflexivo exitoso representa la culminación de una operación de información.

## 2.1 Detalle de Control Reflexivo

La historia del concepto de control reflexivo (CR) se deriva principalmente del trabajo realizado por Vladimir Lefebvre de 1963 a 1967 en la Unión Soviética. Después de la publicación de dos obras *Конфликтующие структуры* (ЛЕФЕВР, 1967) – Estructuras en conflicto and *Алгебра конфликта* (ЛЕФЕВР; СМОЛЯН, 2010) – Álgebra de conflictos, El trabajo de Lefebvre se convirtió en el tema de un informe clasificado de la KGB en 1968. La obra principal de Lefebvre (1984) se titula *Control reflexivo: el concepto soviético de influir en el proceso de toma de decisiones de un oponente* (ЛЕФЕВР, 1984).

Los procesos de control reflexivo se basan en el sistema soviético (y ahora ruso), legados éticos que son muy diferentes de los de Occidente (cristiano), en el que los rusos tienen una comprensión particular de lo que constituye la "verdad".

Según Lefebvre, el concepto de *враню* (вранио-mentira / engaño) se refiere a la "diseminación de falsedades que tienen alguna base en la realidad" (ЛЕФЕВР; СМОЛЯН, 2010) similar a *probabilidad*.

Lefebvre definió el *Control Reflexivo* como "un proceso en el que uno de los oponentes transfiere al otro los fundamentos para la toma de decisiones" (ЛЕФЕВРЕ, 1984, p. 81). En otras palabras, hay una sustitución de los factores motivadores del oponente para alentarlos a tomar decisiones que le son desfavorables.

Por las Fuerzas Armadas de Rusia, **Reflectante control** (CR) es el término utilizado para describir **la práctica de pre-determinar la decisión de un oponente a su favor, cambiar los factores clave en la percepción del mundo del oponente** (ЛЕФЕВРЕ, 1984). El término se encuentra principalmente en la discusión de las técnicas de guerra de la información. En este contexto, la práctica representa un facilitador asimétrico clave para obtener ventajas críticas, neutralizando las fortalezas del oponente, haciéndole elegir cursos de acción dañinos para sí mismo.

Con la exploración de estereotipos morales de comportamiento, factores psicológicos, información personal sobre el comandante (datos biográficos, hábitos, etc.), el CR hace posible aumentar las posibilidades de victoria, sin embargo, se observa que tales tácticas requieren información sobre el enemigo con un alto grado de detalle y calidad!

La manipulación de la opinión pública en Occidente a través de las redes sociales, *trolls* y redes de *bots* mientras conducía anti-estadounidense, anti-OTAN y anti-élite narrativas, son parte de esta política.

La aplicación de Control reflexivo para cambiar el ciclo de toma de decisiones del objeto de control (*publ objetivo / tomador de decisiones / opinión pública*) actúa a través de la influencia de la idea de una situación del objeto de control.

El sujeto de control (*Ruso*) toma medidas para proporcionar al objeto de control información que reflexivamente conduce a la acción en interés del sujeto de control (*Ruso*).

En lugar de negar información por completo, o proporcionar información falsa, la intención del control reflexivo es manipular la información disponible a través de herramientas de información (capacidades relacionadas con sistemas de guerra de información, acciones de inteligencia, espionaje, otras) al objeto de control (*objetivo*) para que utilicen esta información para tomar una decisión reflexiva en interés del sujeto de control.

Ejemplo: **Situación real subject** → **Sujeto de Control X Objeto de control = actitud 01**

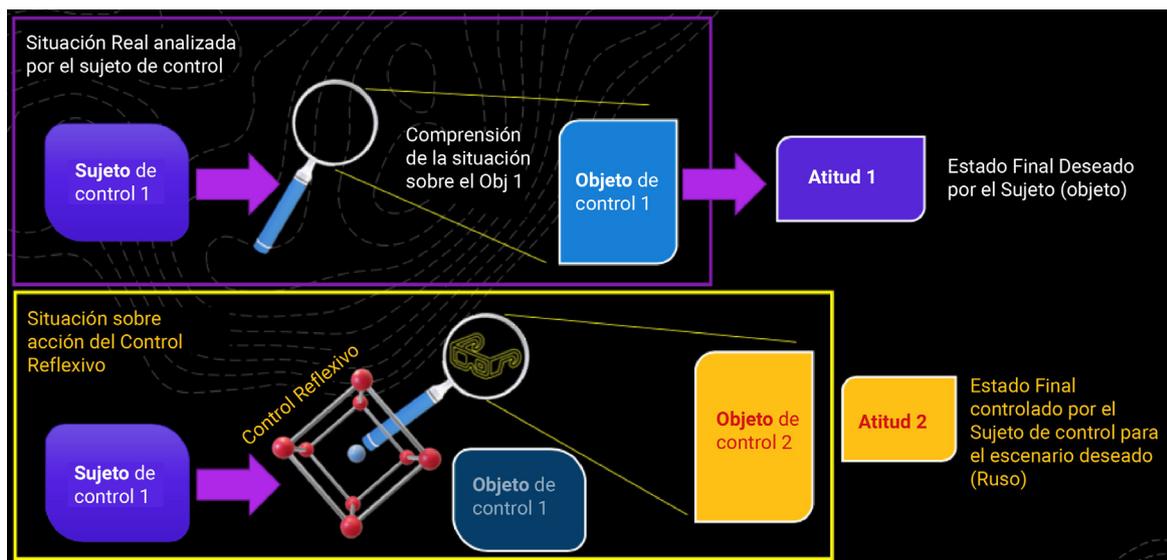
**Situación real + la idea del controlador dirigiendo para cambiar el ciclo de decisión** → **mensajes de influencia para verosimilitud a la situación real.**

**(apuntando al escenario deseable) =**

**Situación real deseada** → **Sujeto de control + Objeto de control = actitud 02.**

Como se mencionó anteriormente, las decisiones se toman a través de un enfoque justo, objetivo y preciso basado en información relevante para la situación, influir en el enfoque la situación cambia.

Figura 1– Esquema de control Reflexivo Ruso



Fuente: Autor (2021).

Se analiza actitudes, conocimientos y habilidades para determinar capacidades de pensamiento crítico, toma de decisiones, juicio predictivo (*y prospectivo*), resolución de problemas, creatividad, apertura a la experiencia y otros comportamientos de liderazgo.

De acuerdo con las actitudes analizadas, se miden (indicadores) las competencias de inferencia, Reconocimiento de supuestos, Deducción, Interpretación y Evaluación de argumentos

Desde el "score" de cada líder y / o objetivo (*publico*), se forma la acción persuasiva del control reflexivo.

## 2.2 Opiniones de los expertos militares: Ionov, Komov y Chausov

Mayor M.D. **Ionov** escribió varios artículos sobre el tema del Control Reflexivo (ИОНОВ, 1994, 1995). Fue uno de los primeros teóricos militares en evaluar la importancia del Control Reflexivo. El concepto de "Control Reflexivo" no estaba en ninguna enciclopedia militar soviética cuando comenzó a escribir en los años 70, por lo que simplemente no podía existir! Como resultado, en sus primeros artículos, Ionov habló de "administrar al enemigo", y no de Control Reflexivo.

Al mismo tiempo, Ionov también entendió la estrecha relación entre la publicidad y el Control reflexivo y la necesidad de combinar el uso de técnicas reflectantes para organizar la gestión del Control Reflexivo (ИОНОВ, 1994).

Ionov identificó cuatro métodos principales para ayudar a transmitir información al enemigo con el fin de facilitar la organización del control sobre él.

**1) Aplicación de presión mediante demostración de fuerza.** Esta demostración de fuerza puede ejercerse de diversas maneras que abarcan diferentes aspectos, desde presiones diplomáticas o económicas, como la amenaza de sanciones económicas, amenazas de acción militar, como el aumento de la preparación para el combate de las Fuerzas Armadas, o provocaciones cercanas a las declaraciones de guerra.

Presión de poder, incluido el uso de fuerza superior, demostración de fuerza, ataques psicológicos, ultimátums, amenazas de sanciones, amenazas de riesgo (manifestadas a través de un enfoque en el comportamiento de liderazgo irracional o la delegación de autoridad a la persona irresponsable), inteligencia militar, maniobras provocativas, pruebas de armas, restricción del acceso enemigo o aislamiento de ciertas áreas, aumento de la preparación para el combate de las Fuerzas Armadas, formación de coaliciones, declaración oficial de guerra, apoyo a la situación desestabilizadora de las fuerzas internas, desactivación y publicidad de la victoria, demostración de acciones despiadadas y muestra misericordia a un aliado enemigo que resistir (ИОНОВ, 1994, p. 45, nuestra traducción).

**2) Proporcionar información falsa.** Este enfoque sugiere el uso del camuflaje, la negación y el engaño "*Maskirovka*" (Doctrina de la ocultación) en todos los niveles con el fin de manipular el anuncio y la recepción de una situación. Esto incluye mostrar una gran fuerza donde hay, de hecho, una debilidad y viceversa, así como el uso de técnicas de caballo de troya.

Métodos para proporcionar información falsa sobre la situación, incluido el camuflaje (mostrar debilidad en un lugar fuerte), crear estructuras falsas (mostrar "fuerza" en un punto débil), dejar una posición para fortalecer otra, dejar objetos peligrosos en esta posición ("caballo de Troya"), ocultar relaciones verdaderas entre unidades o crear falsas, mantener el secreto de nuevas armas, farolear sobre armas, cambiar los métodos de operación o pérdida deliberada de documentos. (ИОНОВ, 1994, p. 46, nuestra traducción).

**3) Afectar el proceso de decisión del oponente.** Tal enfoque incluye el modelado sistemático de procesos, la publicación de doctrinas deliberadamente distorsionadas, así como la presentación de información falsa al sistema del oponente y figuras clave.

Provocar al enemigo a encontrar nuevas direcciones de escalada o poner fin al conflicto: una demostración deliberada de una cadena de Acción Especial, golpear la fortaleza del enemigo cuando no está allí, actividades subversivas y provocaciones, dejando abierta la ruta para que el enemigo abandone el sitio, obligando al enemigo a cometer acciones punitivas que conduzcan al gasto de las Fuerzas Armadas, recursos y tiempo. (ИОНОВ, 1994, p. 46, nuestra traducción).

**4) Que afectan al calendario de la decisión.** Aquí, el elemento sorpresa puede ser empleado por el inicio repentino de una operación militar o inducir al oponente a centrarse en otra área de conflicto para ralentizar la reacción.

El impacto del algoritmo para la decisión a un enemigo, incluyendo la realización del juego sistemático de la divulgación de los planes, el típico, la publicación de la doctrina de deliberadamente distorsionada; el Impacto en los controles e indicadores clave en la transmisión de los datos de la falsa; las Acciones para un camino hasta el acto, con el fin de neutralizar el pensamiento de operar sobre el enemigo, cambiando el tiempo de un juicio que puede ser tomado por un inicio repentino de conflicto armado; informe sobre la situación del conflicto que están trabajando en lo que parece ser un viable y predecible para el enemigo para tomar una decisión, mal considerado, que va a cambiar la forma en y sobre la naturaleza de la operación (ИОНОВ, 1994, P. 47, nuestra traducción).

Segundo **Ionov** (ИОНОВ, 1994), es necesario evaluar los objetivos humanos para el control reflexivo de una persona o grupo, teniendo en cuenta la psicología individual o grupal, la forma de pensar y el nivel profesional de formación.

**Coronel S.A. Komov**, un teórico militar ruso, escribió sobre el impacto informativo del control reflexivo y fue posiblemente el autor más prolífico sobre el tema de las guerras de información en la década de 1990. En las páginas de la revista "pensamiento militar" Komov apoyó el significado dado por Ionov al control reflexivo, dándole otro nombre, métodos "intelectuales" de guerra de información. Enumeró los principales elementos del enfoque "intelectual" de la guerra de la información, que describió como:

- Distracción (desviación de la atención)- crear una amenaza real o imaginaria a una de las dislocaciones vitales del enemigo (flancos, retaguardia, etc.) Durante la fase preparatoria de las hostilidades, obligándole a reconsiderar el sentido común de sus decisiones);
- Sobrecarga (a expensas de grandes cantidades de información conflictiva a menudo enviada al enemigo);
- Parálisis (creación de percepciones de amenazas especiales a intereses vitales o puntos débiles);
- Agotamiento (obligar al enemigo a realizar acciones inútiles y, por lo tanto, agotar a las Fuerzas Armadas);
- Engaño (provocar al enemigo a redespargar sus fuerzas a la región amenazada durante las etapas preparatorias de las hostilidades);
- División (convencer al enemigo de que debe actuar contra los intereses de la coalición);
- Calma (obligar al enemigo a creer que se están entrenando operaciones planificadas previamente en lugar de prepararse para acciones ofensivas-y así reducir su vigilancia);
- Intimidación (creando una percepción irresistible de superioridad);
- Apaciguamiento (disminuyendo la vigilancia y creando la ilusión de llevar a cabo entrenamientos planificados, y no prepararse para acciones ofensivas);
- Provocación (imponer al enemigo datos para que realice acciones beneficiosas de su lado);

- Propuesta (ofrecer información que toque al enemigo legal, moral, ideológicamente o en otras esferas);
- Presión (para ofrecer información que desacredite al gobierno a los ojos de la población) (KOMOB, 1997, p. 18-22, nuestra traducción,).

Finalmente, el artículo del capitán de primer rango **F. Chausov** (ЧАУСОВ, 1999), continúa discutiendo el control reflexivo, que se define como el proceso de transferencia intencional de cierta información a la parte contraria, que tendrá un impacto en la toma de decisiones por esa parte correspondiente a la información transmitida. Chausov formuló los siguientes principios de Control Reflexivo:

- **el principio de propósito** – el proceso debe estar orientado a objetivos, utilizando toda la gama de medidas de Control reflexivo requerir;
- **el principio de actualización** – la planificación debe ser "actualizada", proporcionando una imagen bastante completa del potencial intelectual del comando y el personal, especialmente en situaciones relacionadas con el espacio de información global;
- **el principio de la correspondencia** – la coherencia mutua de objetivos, lugar, tiempo y métodos de Control reflexivo debe ser observado;
- **el principio de modelado** – no debemos olvidar predecir y modelar las acciones y estados del lado opuesto durante la ejecución de Control reflexivo;
- **el principio de anticipación** – los acontecimientos actuales deben ser anticipados y anticipados (ЧАУСОВ, 1999, p. 12, our Griffin, our translation).

También incluye **evaluación del riesgo**, la esencia de lo cual se reduce al peligro de equivocarse en caso de una evaluación incorrecta de las consecuencias. Con este enfoque, el riesgo máximo será si el enemigo desentraña el plan por su cuenta.

### 2.3 EL CR en la Doctrina Militar Rusa – Doctrina Gerasimov

En las dos primeras décadas de este siglo, Rusia llevó a cabo operaciones en varios estados ex soviéticos, con el objetivo de establecer una esfera de influencia en estos países, e impedir que la OTAN y la UE ampliaran sus áreas de influencia, así como para proteger los intereses rusos y las minorías étnicas en el extranjero (ENS Rusa, 2021).

En este mismo período, los análisis occidentales de los conflictos en los que Rusia participó se centraron en las diferentes fuerzas que Rusia utilizó para lograr sus objetivos: fuerzas cibernéticas en Estonia, fuerzas convencionales en Georgia y Fuerzas de Operaciones Especiales (FOpEsp) en el área de Crimea en Ucrania (BERZINS, 2014).

Los especialistas militares occidentales estaban especialmente interesados en las enseñanzas operacionales de las Fuerzas Armadas de la Federación de Rusia y cómo complementaban sus medios militares convencionales con FOpEsp, transporte, infantería naval y fuerzas de reacción rápida. Otros también especularon cómo Rusia usaría los recursos cibernéticos en futuros conflictos. Sin embargo, la mayoría de estos estudios tiene un alcance limitado con solo un enfoque en *hard power* militar. Además, la mayoría de ellos se basan en suposiciones occidentales sobre el modo de guerra ruso, uso

de medios militares dentro de los dominios tradicionales aire, mar y tierra, ampliado con el nuevo dominio cibernético. En realidad, las Fuerzas Armadas de la Federación de Rusia (FAFR) cambiaron su doctrina de guerra en un **concepto operacional** para lograr los objetivos de su política exterior (ПОДБЕРЕЗКИ, 2014; ДОКТРИНА..., 2016; РОССИЯ, 2021; RUSSIAN, 2014).

En 2003, Rusia lanzó un "*white paper*" en apoyo de esta nueva política, que describió un cambio en el pensamiento militar y definió un nuevo concepto operacional basado en la integración de elementos estratégicos, operacionales y tácticos. El concepto se actualizó con las lecciones de los conflictos de Estonia y Georgia. Se caracteriza por el uso de medios no militares y dominios no tradicionales, como los grupos de jóvenes *Partizans* ciberataques, medios de comunicación y fuerzas civiles "*proxy*". Vital para el nuevo concepto operativo es la rápida destrucción, interrupción o control de las comunicaciones, la economía, la infraestructura y las instituciones políticas para interrumpir el comando y control del enemigo, así como el dominio cibernético total.

En esta sección se detalla esta nueva doctrina (NTG), así como, se describe el marco operativo ruso y sus vínculos con las actividades de guerra de información, conceptos militares y posiciones estratégicas, seguido de una breve ejemplificación de la aplicación de la nueva doctrina en el conflicto de Ucrania (Crimea), de 2014.

El objetivo principal es revelar acciones a nivel táctico y operativo (*Comunicación estratégica y actividades de control reflexivo*) de la nueva doctrina (NTG) y los efectos acumulativos y objetivos que estas acciones deben alcanzar para obtener una mejor comprensión del nuevo concepto operativo ruso (DEFENSE INTELLIGENTE AGENCY, 2017).

## 2.4 El enfoque ruso de un conflicto

En febrero de 2014, el jefe del Estado Mayor General de la FAFR, el general Valery Gerasimov, describió en su artículo "El valor de la ciencia en la previsión" (ВАЛЕРИЙ, 2013), el nuevo concepto operacional basado en las lecciones de los conflictos de Estonia y de Georgia.

El general Gerasimov explicó que FAFR ha desarrollado modelos de planificación situacionales únicos para aplicar medios militares y no militares, como FOpEsp, fuerzas "*proxy*", medios civiles y capacidades cibernéticas para influir en todos los actores, interrumpir la comunicación y desestabilizar las regiones con el fin de lograr sus objetivos.

Durante los conflictos de Estonia, Georgia (BARABANOV, 2014), Ucrania (ANÁLISIS..., 2014) (HAINES, 2015) y Siria (SUTYAGIN, 2015), Rusia ha establecido capacidades civiles como grupos juveniles y medios de comunicación estatales y ha movilizado a las minorías étnicas rusas en el extranjero, apelando a sentimientos de marginación, un sentido de autoestima y pertenencia, y una percepción de que la "Madre Rusia" tiene más que ofrecer que el país de origen. Luego Rusia provocó reacciones internacionales y creó una percepción general de desesperación de los líderes militares y políticos de los países objetivo, después de lo cual estos países estaban dispuestos u obligados a aceptar la nueva situación creada por Rusia (FRIDMAN; 2019; GALEOTTI, 2019; LANKINA; WATANABE, 2017; SZOSTEK, 2017).

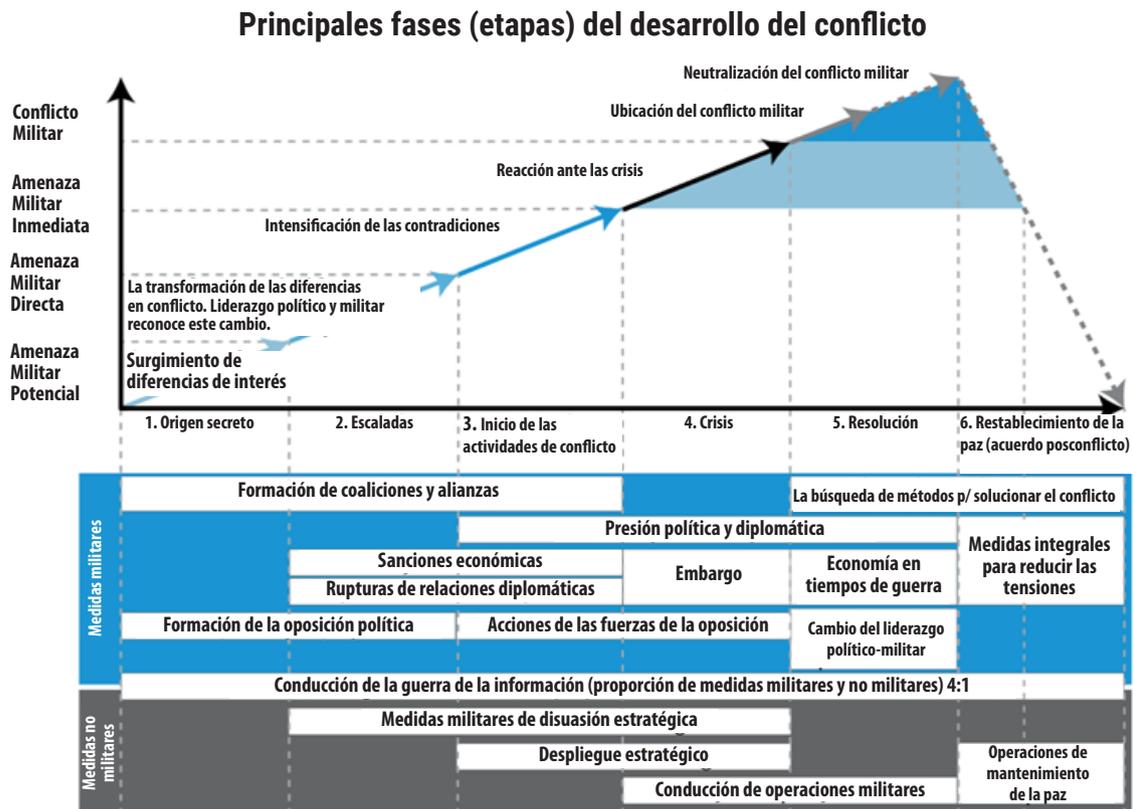
La llamada "Doctrina Gerasimov" es un enfoque de la sociedad que causa un cambio de medios y dominios y plantea un desafío al modo de guerra occidental debido a la infamiliaridad con sus formas, medios, efectos y objetivos.

El general Gerasimov describió el marco actual del concepto operativo ruso como el uso de "todos los métodos no militares para resolver conflictos interestatales"<sup>1</sup>.

Incorpora seis fases, como se muestra en la figura 01: origen secreto, escalada, estallido de la actividad del conflicto, Crisis, Resolución y finalización con el restablecimiento de la paz.

Este concepto operacional es un conjunto de sistemas, métodos y tareas para influir en la percepción (CR) y el comportamiento del enemigo, la población y la comunidad internacional a todos los niveles. Utiliza un enfoque de sistemas basado en el "control reflexivo" (gestión de la percepción) para apuntar al liderazgo enemigo y cambiar su orientación de tal manera que tomen decisiones favorables a Rusia y tomen acciones que lleven a una sensación de desesperación dentro de su liderazgo y establezcan una base para la negociación en términos rusos. Según Ionov, en este caso, el control reflexivo "considera los caracteres psicológicos de los seres humanos e implica una influencia intencional en sus modelos de toma de decisiones" (BARTLES, 2016, p. 31, nuestra traducción).

Figura 2 – El papel de los métodos no militares en la resolución de conflictos interestatales.



Fonte: Adaptado de Герасимов, 2014.

La Nueva Doctrina (NTG) no evolucionó en el vacío durante la última década, sino que es una reacción dual a los eventos que se desarrollaron después del colapso de la Unión Soviética.

1 Ivanovich, Mironov Sergey. Conferencia en la Academia Diplomática del Ministerio de Relaciones Exteriores de Rusia. Tema de la conferencia: "la seguridad y el papel de la fuerza militar en garantizar la seguridad internacional" Curso: "Aspectos político-militares en las relaciones internacionales y el control de armas", 2017. Fuente del autor.

Primero, la evolución es una reacción del liderazgo ruso bajo el presidente Vladimir Putin para combatir el modelo cognitivo que refleja la estructura interna de un sistema de toma de decisiones. Este modelo ofrece un enfoque de mecanismos interrelacionados basados en la historia, las condiciones sociales y la lingüística para engañar, intentar, intimidar o desinformar al enemigo. Los Mecanismos de Control Reflexivo pueden causar efectos psicológicos que van desde la decepción hasta la sugerencia. Si uno de estos mecanismos falla, el enfoque de Control Reflexivo global debe activar otro mecanismo, o sus efectos originales pueden degradarse rápidamente.

Finalmente, el arte operativo ruso se basa en el ocultamiento, también una técnica de control reflexivo, dividida en dos niveles. El ocultamiento a nivel operativo se refiere a medidas "de manera a lograr la sorpresa operativa y está diseñado para desorientar al enemigo con respecto a la naturaleza, el concepto, la escala y el momento de las operaciones de combate inminentes". (ГЕРАСИМОВ, 2014, p. 19) Y el ocultamiento de nivel estratégico son "actividades que preparan subrepticamente una operación estratégica o campaña para desorientar al enemigo sobre las verdaderas intenciones de las acciones". (ГЕРАСИМОВ, 2014, p. 19).

Gen Gerasimov explicó el nuevo concepto operativo con algunos de los mismos principios que Georgi Isserson, uno de los principales pensadores militares soviéticos antes de la Segunda Guerra Mundial. Isserson definió el arte operacional como la capacidad de dirigir y organizar, donde las operaciones son una cadena de esfuerzos en toda la profundidad del área de operación, con principios de choque, rapidez, eficiencia, movilidad, simultaneidad, soporte tecnológico y punto de inflexión en la etapa final. Gerasimov agregó a la noción de Isserson la aplicación de acciones asimétricas e indirectas por parte de componentes civiles/militares, fuerzas de operaciones especiales y armas técnicas (ISSERSON, 2013) para debilitar la economía y destruir las infraestructuras clave en un área potencial de operaciones. Por lo tanto, el nuevo concepto operativo es una mera continuación del arte operativo ruso existente con diferentes medios no solo en el dominio físico sino también en el dominio de la información.

Rusia utiliza "*fuerzas extraterritoriales*", tanto paramilitares como cibernéticas, apoyadas por instituciones y empresas (medios o no), combatientes de Spetsnaz y Cosacos para llevar a cabo diferentes tipos de operaciones, tales como operaciones no convencionales, de información, psicológicas y cibernéticas, así como la asistencia a las fuerzas de seguridad y **comunicación estratégica**. Rusia administra estos medios militares y no militares a través de empresas y organizaciones controladas por el Estado bajo una estructura de mando político centralizada. Esta estructura, junto con el hecho de que las fuerzas empleadas consisten en una mezcla de rusos étnicos y rusos en el extranjero, hacen que Rusia no solo explore las condiciones sociales, sino también los factores culturales y lingüísticos en los antiguos estados soviéticos y en el hogar para crear "*fuerzas extraterritoriales*". Estudios comportamiento, composición étnica y demografía de todos los oponentes potenciales para revelar ventajas que pueden explotar para lograr sus objetivos<sup>2</sup> (АИИЕИКОВ et al, 2006, 2011, 2015).

2 Ivanovich, Mironov Sergey. Conferencia en la Academia Diplomática del Ministerio de Relaciones Exteriores de Rusia. Tema de la conferencia: "la seguridad y el papel de la fuerza militar en garantizar la seguridad internacional" Curso: "Aspectos político-militares en las relaciones internacionales y el control de armas", 2017. Fuente del autor.

**2.5 Detallando el uso de la Doctrina Gerasimov (ASYMMETRIC WARFARE GROUP, 2016; BARTLES, 2016; DEFENSE INTELLIGENCE AGENCY, 2017;) (NTG) (GORENBURG, 2017), con énfasis en la Guerra de la Información y el Control Reflexivo**

Para la comprensión completa de la Doctrina, me acercaré al Arte Operacional en 07 (siete) fases, es decir, 01 (uno) más de lo presentado por el Gen. Gerasimov (ГЕРАСИМОВ, 2014), con el objetivo de presentar las acciones totales de la doctrina de la información (ДОКТРИНА, 2016), con Estrat. / Control Reflexivo NTG.

**El detalle debe ir acompañado del soporte con el documento contenido en el Anexo Nº 01.**

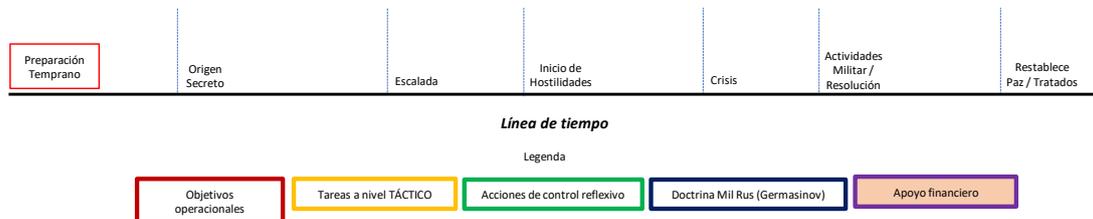
En la línea de base, se encuentra desde el desarrollo del tiempo, de izquierda a derecha.

Verticalmente, 03 (tres) campos de acción están delimitados: medidas militares (en la base), medidas no militares (en el centro) y guerra de la información (en la parte superior).

En la evolución del tiempo, dentro de cada campo de acción, se identifican las acciones de: objetivos operativos, tareas a nivel táctico, acciones de control reflexivo, las acciones de la Doctrina Gerasimov y el apoyo financiero / esfuerzo diplomático necesario.

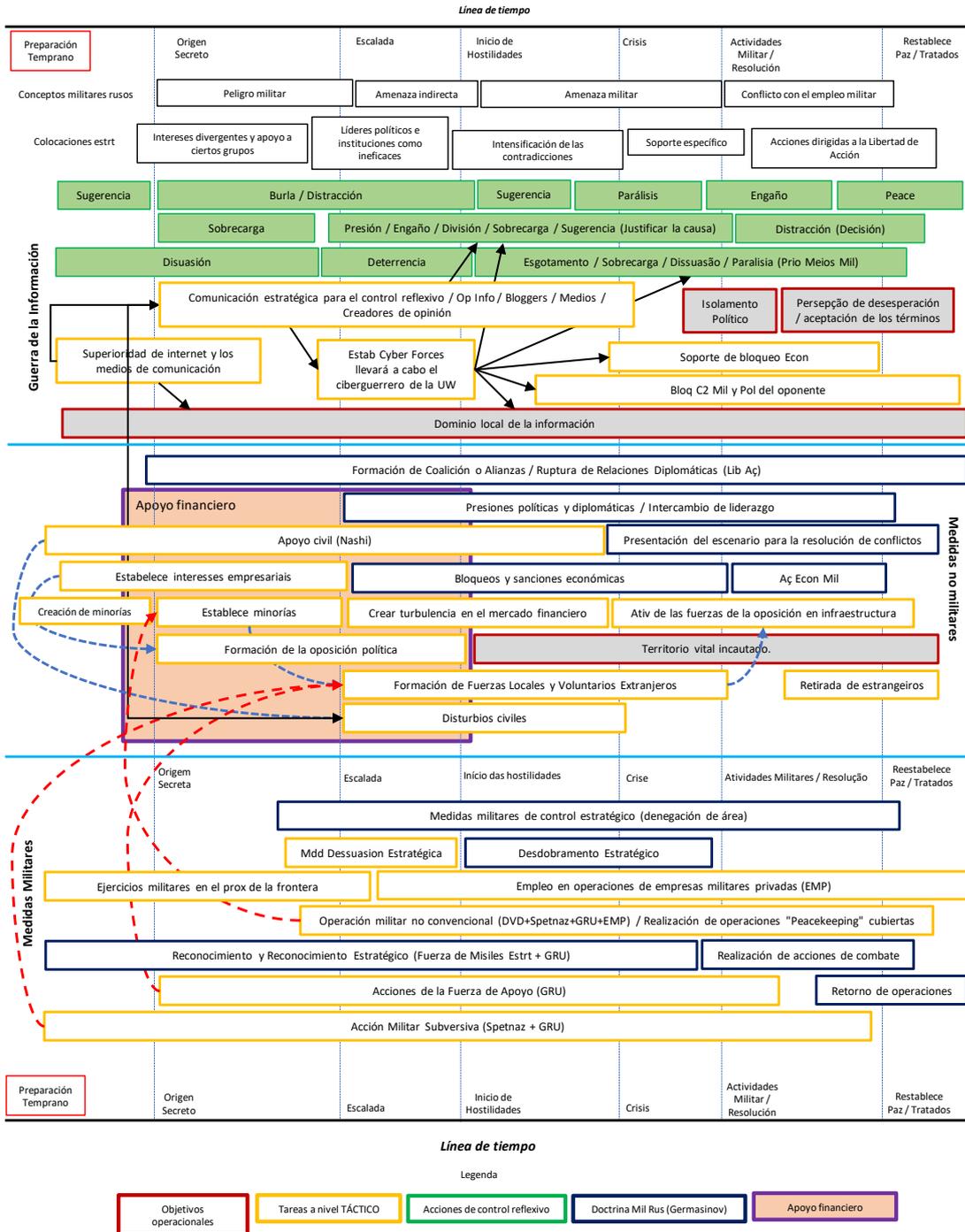
La descripción del detalle se aborda, dentro de la fase temporal, desde la base hasta la parte superior, presentando el desencadenamiento de las acciones dentro de cada campo.

**Figura 3 – Corte de la base del detalle Apéndice 1.**



Fuente: Autor (2021)

**Figura 4 – Estrategia y Arte Operacional de las Fuerzas Armadas de la Federación Rusa**  
**Estrategia y Arte Operacional de las Fuerzas Armadas de la Federación de Rusia**  
*Doy Mil Rus (Gen Gerasimov), con enlaces a las actividades de Com Estrt (Control reflexivo), Negación de área, guerra cibernética, acciones cinéticas (militares) y acciones no militares.*



Autor: Cel Art QEMA Croce

Fuente: Autor (2021)

a) Fase 0 – Preparación anticipada

**Medidas Militares** – Se activan pequeñas infiltraciones de FOpEsp y GRU para llevar a cabo acciones subversivas (soporte) y reconocimiento. Los medios de la Fuerza de Misiles Estratégicos y el GRU realizan actualizaciones semanales de datos Geoint y reconocimiento estratégico detallado. Los mandos militares realizan ejercicios militares dentro de su zona, pero en las proximidades de las fronteras (Rec GE).

**Medidas No Militares** – Las minorías son " activadas " o creadas, también está el desencadenamiento de las " fuerzas Nashi " (DENNING, 2015), partizanos o cosacos, así como el EMP con el objetivo de apoyo futuro. Económicamente, los contratos se llevan a cabo entre empresas interesadas en el área, principalmente empresas de infraestructura, así como, la cooptación de elementos de élite en el área objetivo, a través de la corrupción financiera.

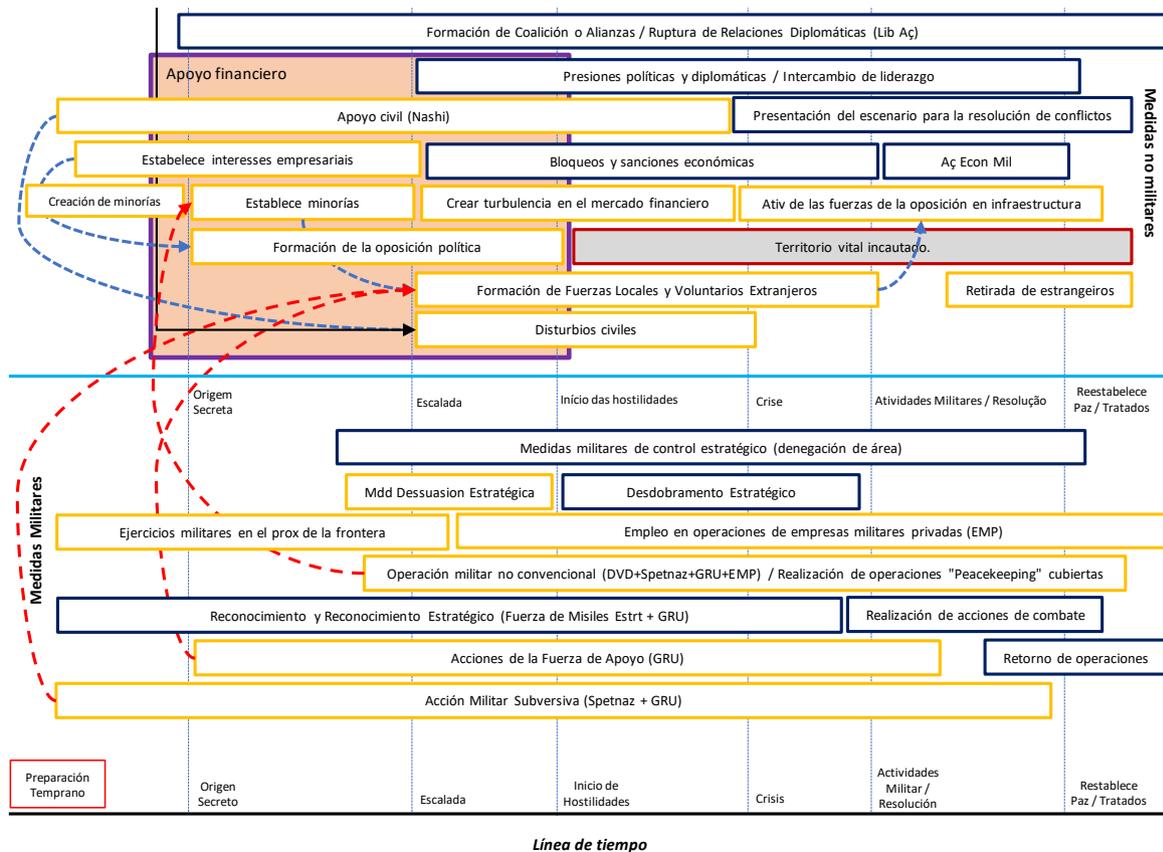
**Guerra de la información** – Se actualizan las redes, "backbones" y la infraestructura cibernética, iniciando acciones para permitir la superioridad de internet y los medios. El objetivo operativo es el dominio local de la información. Las acciones de Com Estr / CR desencadenaron la visión a la sugestión y la disuasión. La sugerencia está dirigida a las minorías y a los errores del gobierno local (generación de enemistades). La disuasión tiene como objetivo ocultar el desplazamiento estratégico, así como transmitir la idea de "Causa Perdida".

A modo de ejemplo, la fase de preparación temprana para los conflictos de Georgia, Ucrania y Estonia comenzó en 1991, cuando todos se convirtieron en estados independientes y separados de la Unión Soviética, centrándose en dos regiones separatistas: Osetia del Sur y Abjasia. Ambas regiones no tenían grandes poblaciones étnicas rusas, pero los habitantes tenían una cultura y un idioma claramente diferentes de la población georgiana, más relacionados con las áreas al norte de ellas, dentro de Rusia. Las tensiones en Ucrania pronto siguieron, en gran parte debido a una minoría étnica rusa en Crimea que deseaba unirse a Rusia. Al mismo tiempo, el gobierno de Estonia aprobó una ley que rechazaba el ruso como idioma oficial, forzando el idioma estonio sobre los rusos étnicos como requisito para obtener la nacionalidad estonia. Rusia vio estos acontecimientos como una marginación de los derechos de los rusos étnicos. En los años siguientes, Moscú emitió pasaportes a los rusos étnicos en los tres países, creando una minoría rusa, que prometió proteger. Las tensiones se intensificaron cuando Estonia se unió a EU y la OTAN en 2004 y posteriormente se negó a construir un oleoducto junto con Rusia. En la mayoría de los casos, Rusia infundió la situación mediante la concesión de la ciudadanía a los rusos étnicos o otros habitantes con quejas, la creación de ciudadanos rusos en los estados vecinos. Uno de los principales objetivos estratégicos de Rusia es proteger a los rusos étnicos dondequiera que se encuentren.

b) Fase 1 – Origen secreto

**Medidas Militares** – En esta fase las fuerzas de apoyo se estructuran, con el apoyo del GRU, con el objetivo de la formación de fuerzas locales, EMP y voluntarios extranjeros (Fuerza Proxy) para la fase de escalada. Se mantienen las actividades de reconocimiento y vigilancia del conocimiento de la situación, y se intensifican los desplazamientos estratégicos y las maniobras militares en la franja fronteriza. A nivel táctico, ya se observa el movimiento de elementos de disuasión estratégica (Def Aae, GE y misiles).

Figura 5 – Recorte de medidas militares y no militares y sus conexiones durante el Origen Secreto (consulte el diagrama completo en el apéndice).



Fuente: Autor (2021)

**Medidas No Militares** – Aumenta-se o apoio financeiros às atividades de cooptação de parceiros “leais à causa”. A partir de la formación de minorías (con descendientes étnicos o no) se activan acciones de formación y establecimiento de áreas de operaciones (incluye el estudio y validación de áreas clave para la “negación de área”). Las acciones de la Nashi (apoyo civil en todos los campos) e intereses comerciales. Se lleva a cabo un fuerte trabajo en la formación de la oposición política. El objetivo operativo es la formación de alianzas y / o una coalición, así como el “debilitamiento” gradual de las relaciones diplomáticas.

**Guerra de la información** – En esta etapa, el concepto operativo ruso, para los medios externos, es el de “Peligro Militar”. Es decir, que las acciones de otros interesados pueden afectar militarmente el área objetivo, con el objetivo de dar libertad de acción para el empleo militar ruso. El posicionamiento estratégico político es la difusión en los medios tradicionales. Las actividades de Com Estrt / CR se intensifican con los objetivos de provocación, distracción, sobrecarga de información en los sistemas internos de la zona objetivo, y aumentar el grado de disuasión.

## c) Fase 2 – Escalada

**Medidas Militares** – Se mantienen los esfuerzos en medidas subversivas, apoyo a las fuerzas de apoyo en la zona objetivo, monitoreo de conciencia situacional (con Prio para Intlg, GE, AAe, Ciber) y los medios de disuasión estratégica ya están posicionados. En esta fase, los primeros EMPs aparecen sobre el terreno, principalmente de logística y apoyo a las actividades civiles (salud y Peacekeeping de la Paz cubierto). El diferencial más identificado es la provisión de recursos militares en DTAs cercanos a la frontera, realizando actividades de mantenimiento para ejercicios militares. La Fuerza de Trens del Min Def se emplea ampliamente para la logística.

**Medidas No Militares** – En esta etapa, se identifican las primeras manifestaciones y acciones de disturbios civiles. La capacitación de las fuerzas no militares locales y de los extranjeros voluntarios ya está en condiciones de empleo. En el mercado financiero, se identifican la fuga de capitales y diversas acciones cibernéticas en el sistema financiero. La formación de la oposición política se siente con el aumento de las cantidades de manifestaciones (planificadas). El soporte de fuerza Nashi es fundamental, junto con las acciones diplomáticas, para asegurar los objetivos estratégico-operacionales del bloqueo y las sanciones económicas, junto con las presiones político-diplomáticas para el intercambio de liderazgo en la zona objetivo.

**Guerra de la información** – El concepto ruso de "amenaza indirecta" está elaborado hasta el agotamiento. Es decir, que las acciones de la población civil deben ser apoyadas y cualquier movimiento de medios militares se considera una amenaza. Frente a la comunidad internacional, la posición estratégica adoptada es dar a conocer la imagen de que los líderes políticos y las instituciones están inoperantes en la zona objetivo, necesitando "ayuda" para controlar el "caos". En esta fase, las fuerzas cibernéticas ya están estructuradas y comienzan actividades en todo el espectro de C2, infraestructura crítica y toma de decisiones. Las acciones de Com Estrt / CR se dirigen principalmente a la presión, el engaño, la División, la sobrecarga y la justificación, con el objetivo de aumentar la libertad de acción y aumentar el caos controlado en el área objetivo. Con el fin de aislar el proceso de toma de decisiones de los dirigentes en la zona objetivo, se llevan a cabo medidas de disuasión (aislamiento de las decisiones y disturbios civiles).

Actividades en el conflicto de Ucrania

La fase de escalada de la crisis comenzó después de que el presidente Yanukovich de Ucrania huyera del país en febrero de 2014 y un gobierno pro-occidental tomara el poder. Según Rusia, el nuevo gobierno actuó contra la seguridad de los rusos dentro de Ucrania. Rusia utilizó el discurso de la intervención humanitaria internacional para proteger a los rusos en el extranjero para justificar una intervención, de nuevo en referencia a los argumentos occidentales para validar la participación de la OTAN en la crisis de Kosovo.

El siguiente paso de la operación rusa fue la campaña mediática para obtener apoyo en Crimea y Rusia y aislar al Gobierno de Ucrania, como se muestra en el centro de la Fase Uno y dos: comunicación estratégica. La televisión e Internet son los medios dominantes en Ucrania. En Crimea, en total, el 95% de la población recogió sus noticias de los canales de televisión, que eran casi todos propiedad del Estado ruso. Alrededor del 50% de la población de Crimea recogió sus noticias de Internet, y el 70% de los usuarios de Internet de Crimea confían en su colección de noticias en los dos principales sitios de redes sociales rusos disponibles. Rusos y ucranianos analizaron la información sobre los sentimientos recogidos de Internet, encontrando una puntuación de 76% para los sentimientos pro-rusos en la región.

Los proveedores de noticias independientes están calificados con una puntuación confiable del 30%, y los proveedores de noticias extranjeros solo tienen una confiabilidad del 5%. En resumen, es razonable afirmar que Rusia estableció el dominio de la información en la primera fase de la nueva doctrina (NTG) – origen oculto – y que utilizó medios adicionales durante la siguiente fase para mantener este dominio descrito como el objetivo de "dominio de información local".

La campaña de información rusa comenzó con la comparación del gobierno ucraniano y sus aliados occidentales con nazis, gays, judíos y otros grupos de personas que Rusia afirmaba ser parte de la comparación del gobierno con la Alemania nazi. Este tema se mantuvo durante todo el conflicto. Rusia también acusó a los medios de comunicación occidentales de simplificar demasiado los mapas demográficos, lo que significa que el este y el sur de Ucrania son los rusos étnicos predominantes. Mientras tanto, los canales diplomáticos y el liderazgo ruso comenzaron a enfatizar los mismos problemas de las minorías rusas marginadas que buscan la reunificación con Rusia.

El 14 de febrero, surgió un ataque cibernético, dirigido a uno de los bancos más grandes de Ucrania, atacado por malware, destinado a apoyar los disturbios en el país y descrito como uno de los medios no militares en el Apéndice 1.

#### d) Fase 3 – Comienzo de las hostilidades

**Medidas Militares** – Se establecen medidas de negación de área (dispersión de medios) y despliegue estratégico dentro del rango operacional. Las actividades de la fase de escalada se mantienen, pero con el objetivo de desencadenar el lado opuesto para que reaccione erróneamente a una acción predeterminada (argumento para la autodefensa). Destacamos las acciones de control del espectro electromagnético y el uso de "drones".

**Medidas No Militares** – Se mantienen las medidas de presión en los ámbitos político, económico, psicosocial y de disturbios civiles. Algunos lugares de la zona objetivo están ahora controlados por fuerzas sustitutivas y designados como territorio vital. Se trata de infraestructura, medios de comunicación, barrios ubicados en las principales DTAS, etc. El "green men" se puede observar, generalmente EMP de seguridad para las ONG partidarias de la ayuda humanitaria.

**Guerra de la información** – El concepto ruso de "amenaza militar" se trabaja con el enfoque en los medios militares de la zona objetivo (*Las Fuerzas de Defensa atacan al pueblo*). Las acciones militares contra la población civil, el apoyo humanitario o algunos medios militares rusos se consideran una amenaza. Frente a la comunidad internacional, la posición estratégica adoptada de difundir la imagen de que los líderes políticos y las instituciones son inoperantes permanece, pero las contradicciones se intensifican, principalmente por medios diplomáticos. Se exacerban los antagonismos, desacuerdos y enemistades internas del área objetivo. Las acciones de Com Estrt / CR en esta fase se dirigen a dos vertientes: la primera, con presión, engaño, División, sobrecarga y sugestión se dirigen a los campos político y económico; y la segunda, con agotamiento, sobrecarga informativa, disuasión y parálisis se dirigen a los campos militar y ciencia y tecnología. Se inician medidas destinadas a bloquear el C2 militar y político (aislar la fuente de poder).

Observación - en el país y en el extranjero, el sistema Com Estrt / CR a menudo opera en una asociación público-privada con oligarcas o empresarios rusos, así como a través de la cooptación de hackers "independientes" por parte de agencias de inteligencia. La estrategia es **alimentar los resentimientos, estereotipos y vulnerabilidades existentes**. Cada actor que debilita los sistemas dominantes y ayuda a socavar la confianza en las democracias de la zona objetivo, es recibido como un socio.

### Actividades en el conflicto de Ucrania

Fuerzas paramilitares locales y cosacos irrumpieron en el parlamento y lo reemplazaron con pro-rusos, liderados por Sergei Aksyonov. Mientras los simpatizantes pro-rusos se apoderaron de más instalaciones clave en Crimea, voluntarios de Rusia acudieron en su ayuda y un fuerte ejército ruso de 40.000 soldados comenzó ejercicios en la frontera entre Ucrania y Rusia. En los días posteriores a la toma, los cosacos permanecieron para proteger los Edificios del Parlamento contra el ejército ucraniano o simpatizantes pro-Ucrania. Desde el 28 de febrero, los militantes ocuparon instalaciones militares, aeródromos, medios de comunicación regionales y centros de telecomunicaciones. Apagaron el teléfono y la comunicación por Internet en Crimea a medida que más aviones con nuevas tropas aterrizaban en los aeródromos incautados. Es esta combinación de guerra no convencional por parte de las fuerzas de Operaciones Especiales y las fuerzas proxy, junto con una fuerza convencional abrumadora que realiza ejercicios en la frontera, lo que conduce a una provocación deseada para una reacción o a la disuasión/pacificación para impedirlo, como se describe en el apéndice 08.

Provocación o la disuasión / pacificación para el trabajo, el gobierno debe ser más o menos aislados, cargado con la desinformación, tal como se representa en el centro del Apéndice 1. Por lo tanto, los militantes bloquearon el tráfico de radio y celular para aislar aún más a Crimea de Ucrania. Los ciberataques coordinados por Rusia comenzaron a principios de marzo y afectaron al gobierno ucraniano, así como a los sitios web de la OTAN. Cyber Berkut, un grupo ucraniano, que puede tener vínculos con los servicios de inteligencia rusos, organizó los ataques. Estos ataques obstaculizaron el liderazgo de la OTAN y Ucrania, pero no llevaron al aislamiento o la sobrecarga. Los Estados Unidos convocaron una misión de la ONU en la región en marzo; Rusia se negó. En cambio, el primer ministro Aksyonov de la República Autónoma de Crimea, junto con el ex presidente ucraniano Yanukovich, pidieron la intervención rusa el 1 de marzo y un referéndum de independencia el 30 de marzo.

#### e) Fase 4 – Crisis

**Medidas Militares** – Se mantienen las mismas medidas que en la etapa del comienzo de las hostilidades. Sin embargo, la logística para los medios militares se incrementan, de acuerdo con la planificación de tiempo de las operaciones. El despliegue estratégico está prácticamente terminado y se inician acciones de reconocimiento "en el límite de la zona de responsabilidad". Tales acciones pueden conducir a pequeños combates en la franja fronteriza (acción y reacción de autodefensa).

**Medidas No Militares** – Las fuerzas sustitutas comienzan sus actividades más notorias con intentos sucesivos de dominar las áreas de interés con el objetivo operacional de controlar el área objetivo. Las acciones subversivas pueden ser disparadas en ciertos lugares (antenas de radio, etc.), pero siempre reconocidas como "actos de sabotaje" por los partizanos (KPEIЦYJI, 2015). En el área política, se presentan escenarios comerciales. Sin embargo, con EFD objetivo.

**Guerra de la información** – Al comienzo de esta fase se activan acciones para el aislamiento económico del oponente. Se mantienen las medidas de Com Estrt / CR de la fase anterior, pero el enfoque se dirige a la parálisis política del oponente, apuntando al objetivo operacional que debe sentirse hasta la fase del conflicto armado.

### Actividades en el conflicto de Ucrania

Con el gobierno de Crimea prácticamente eliminado, los efectos del control reflexivo como la distracción, la presión, la sugerencia y el aislamiento (*local*) tuvieron éxito. Rusia nunca fue capaz de aislar completamente al gobierno ucraniano, sin embargo, como apoyo occidental a este gobierno disminuir durante el conflicto y el EFD se logró.

#### f) Fase 5 – Actividades militares (conflicto armado)

**Medidas Militares** – Se aplica la doctrina del empleo militar ruso, con negación de área y empleo masivo de medios blindados. Las acciones se llevan a cabo con la máxima velocidad y dispersión.

**Medidas No Militares** – Las acciones en las infraestructuras del oponente se intensifican por Fuerzas proxy. El objetivo operacional perseguido es el control del territorio vital. Las acciones de la economía militar (bloqueo de importaciones, incumplimiento de contratos, etc.) se desencadenan con el objetivo de reemplazar al MEM opositor. En el ámbito diplomático, persisten las presiones para la validación del escenario previsto. Denuncias de corrupción, degradación de imagen, descrédito, etc. son algunas de las actividades desarrolladas con objetivos diplomáticos. Algunas empresas ya están presentes en áreas "libres de combate" proporcionando infraestructura y apoyo logístico. Se firman los contratos de los contratistas para la reconstrucción.

**Guerra de la información** – El posicionamiento estratégico buscado está dirigido a aumentar cualquier libertad de acción. Los objetivos operacionales del aislamiento político, la percepción de desesperación y la aceptación de las condiciones se persiguen sin cesar. En el Com Estrt / CR se mantiene el lado militar y el lado político se dirige hacia el engaño y la distracción del proceso de toma de decisiones. Antes de que la opinión pública se presenta el escenario propuesto y trabajó fuertemente su aceptación. El mensaje de la reestructuración de la zona con el empleo de las empresas y el apoyo a la población local es el foco. Se plantean temas como la protección del medio ambiente y la protección del patrimonio cultural local. Se solicita el desempeño de los empresarios en el área de comunicación. Sin embargo, en las zonas de combate, todo acceso físico o informativo, de cualquier medio, está controlado. El monitoreo del tema en las redes sociales está fuertemente ejecutado. Así como, el control de la opinión pública se acompaña.

### Actividades en el conflicto de Ucrania

Luego, en el enfoque ruso estaban las tareas que llevarían a provocaciones (una segunda vez como último recurso) o agotamiento y parálisis del gobierno ucraniano en Kiev. Aunque el gobierno ucraniano decidió no ser provocado estratégicamente, el resultado a nivel operativo fue devastador. Las acciones combinadas llevaron a la ruptura de la moral de las fuerzas ucranianas en Crimea, a través de una combinación de los mecanismos de control reflexivo de agotamiento y sugerencia, ya que entregaron sus bases, en muchos casos para unirse a las fuerzas rusas. Los "Little Green Men" aislaron a las fuerzas ucranianas en sus bases, y luego utilizaron Internet y los medios locales para iniciar operaciones de apoyo a la información militar, campañas en los medios e intimidación en combinación con soborno.

Para el 2 de marzo, los militantes ya habían cortado las líneas eléctricas en el cuartel general de la Armada de Ucrania en Sevastopol, seguido de la toma de las instalaciones de comunicación de las Fuerzas Navales Ucranianas y el sabotaje de todas las líneas de comunicación. No se produjo un ataque cibernético en la zona de Crimea. Una de las razones de la ausencia puede ser que Crimea es una pequeña zona con un solo centro de Internet, que ya estaba en manos de las tropas "desconocidas".

El gobierno de Kiev admitió que la policía local y las fuerzas armadas en Crimea eran corruptas, simpatizaban con el levantamiento o tenían baja moral. Entonces los agentes de influencia rusos penetraron en las fuerzas de inteligencia y seguridad locales. En conjunto, la falta de comunicaciones y apoyo de la base llevó al aislamiento táctico y finalmente operacional de las fuerzas ucranianas en Crimea y su percepción de desesperación.

g) Fase 6 – Restablecimiento de la paz y firma de tratados

**Medidas Militares** – Comienza la retirada de parte de las fuerzas empleadas, dejando en la zona objetivo EMP para la formación de las fuerzas de autodefensa. Destacan las tropas de la Policía Militar, DQBRN, GRU, FOpEsp, FSB y Def AAe. Posteriormente, en caso de anexión, se desplegarán efectivos de las FAFR.

**Medidas No Militares** – Se realizan acciones de retirada de extranjeros y catalogación de la población. Comienzan las actividades las asociaciones civil-militares para la reconstrucción. Se elaboran la organización política y los servicios esenciales y se apoyan las actividades rutinarias.

**Guerra de la información** – El posicionamiento estratégico buscado es mantener toda la libertad de acción para la aceptación de los términos. Los objetivos operacionales del aislamiento político, la percepción de desesperación y la aceptación de las condiciones se persiguen sin cesar. Se trabajan temas de pacificación de hostilidades y retorno de actividades económicas. El Com Estrt / CR está dirigido a la pacificación del área objetivo, con la apertura de lugares para visitas, inauguración de desarrollos de muebles y en el fomento del turismo cultural.

#### Actividades en el conflicto de Ucrania

En abril de 2014, Rusia admitió que los "Little Green Men" eran, de hecho, tropas del fafr Spetznaz y aerotransportadas. El 16 de marzo, Crimea celebró el referéndum por la independencia antes de lo previsto, y el 96,77% votó a favor de la reunificación con Rusia (la participación fue del 83,1%). A Dumas Rusia (parlamento) firmó un tratado el 18 de marzo incorporando formalmente a Crimea en Rusia, iniciando la sexta fase, la restauración de la paz. El conflicto sigue congelado (ØSTENSEN, Å.; BUKKVOLL, Ø. 2018).

### 3 Conclusión

El actual concepto operacional ruso utiliza medios militares y no militares de manera simultánea y rápida en todos los ámbitos físicos y de información, mediante la aplicación de acciones asimétricas e indirectas. Rusia mitiga las capacidades de los oponentes, crea caos, toma terreno vital y aísla al liderazgo enemigo. Aunque Rusia utiliza una fuerza convencional en su concepto operacional superior y con la que la victoria es casi segura, no quiere emplear fuerzas militares como tales para su política exterior.

La gran pelea es una escalada no deseada, ya que Rusia busca una victoria psicológica, no física. En lugar de una acción militar, Rusia quiere dejar que el Sistema de Comunicación Estratégica extienda el control reflexivo. Los efectos psicológicos culminantes del enfoque de control reflexivo, como la desorientación, la sugestión y el ocultamiento, deben superar la provocación. Al final, causará agotamiento, parálisis y percepción de desesperación entre los líderes políticos y militares de los opositores. Estas percepciones plausibles y percepciones erróneas crean el liderazgo para la fase final de la nueva doctrina (NTG): **resolución no combatiente**.

La evolución de la nueva doctrina (NTG) y su marco no ha terminado, ya que el marco operativo ruso es cualquier cosa menos un conjunto fijo de medios y estrategias. El liderazgo ruso puede desarrollar y emplear nuevos tipos de medios asimétricos, dependiendo de la situación en cuestión.

En opinión del General Gerasimov, cada conflicto tiene su propio conjunto de reglas y, por lo tanto, requiere formas y medios únicos. Por otra parte, los efectos a lograr deben estar relacionados con fases y objetivos. Por lo tanto, la lección para posibles conflictos futuros no es simplemente fijarse en los medios físicos de Rusia, sino, lo que es más importante, reconocer las fases discutidas y predecir los efectos deseados por el oponente.

Encontramos que la "Doctrina Gerasimov" probó su estructura durante los conflictos de Estonia, Georgia y Ucrania, y en todos ellos se logró el Estado final deseado.

Estudios sobre el uso de la Comunicación Estratégica aliada al control reflexivo deben ser desarrollados para identificar sus efectos, es decir, nosotros como objetivo, con el fin de que las medidas de protección puedan ser tomadas de manera oportuna. En vista de las últimas actividades de las empresas Cambridge Analytica, SCL Group (defensas) and Psy-Group in the democracies of Australia, India, Philippines, Kenya, Malta, Malaysia, Romania, Trinidad and Tobago, Nigeria, United States and UK - case Leave.EU (BORSHCHEVSKAYA, 2019; Universidad de Defensa Nacional, 2020. CSIS, 2020 y Congressional Research Service, 2021), que tienen características modernas del uso del control reflexivo, pero no por los rusos.

Nigeria, Estados Unidos e UK - caso Leave. EU (BORSHCHEVSKAYA, 2019; National Defense University, 2020. CSIS, 2020 e Congressional Research Service, 2021), as quais apresentam características modernas do emprego do controle reflexivo, mas não pelos russos.

## Referencias

АННЕНКОВ, В. И. et al. **Международная безопасность: геополитические и военно-политические аспекты современности.** Под общей редакцией проф. Анненкова В.И. Москва: РУСАВИА, 2015. 512 с.

АННЕНКОВ, В.И. et al. **Военная сила в международных отношениях.** Наставнический. Москва: КНОРУС, 2011. 496 с.

АННЕНКОВ, В.И. et al. **Безопасность России: геополитические и военно-политические аспекты.** Москва, 2006.

ANALYSIS: Russian military manpower – strengths, weaknesses, Ukraine standoff. **Caversham BBC Monitoring**, [London], May 15, 2014.

ASYMMETRIC WARFARE GROUP. **Russian new generation warfare handbook.** [S. l.]: Asymmetric Warfare Group, Dec 2016. p. 68. Disponible en: <https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf>. Acceso el: 18 nov. 2021.

ВАЛЕРИЙ, Г. Ценность науки в ожидании: Новые вызовы требуют переосмыслить формы и способы ведения боевых действий. **Военно-промышленный курьер**, 26 февраля 2013. Disponible en: <http://www.vpk-news.ru/articles/14632>. Acceso el: 26 jul. 2017.

BARABANOV, M. Hard Lessons Learned: Russian Military Reform up to the Georgian Conflict. In: HOWARD, C.; PUKHNOV, R. **Brothers armed: military aspects of the crisis in Ukraine.** Minneapolis: East View Press, 2014. p. 80-81.

BARTLES, C. K. Getting Gerasimov Right. **Military Review**, Fort Leavenworth, Kansas, v. 96, n. 1, p. 30-38, Jan/Feb 2016. Disponible en: [https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview\\_20160228\\_art009.pdf](https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf). Acceso el: 19 nov. 2021.

BERZINS, J. **Russia's new generation warfare in Ukraine: implications for Latvian Defense Policy.** Latvia: National Defence Academy of Latvia, Apr 2014.p. 3-6. (Policy Paper, n. 2). Disponible en: <https://sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf>. Acceso el: 19 nov. 2021.

BIKKENIN, R. Questions of theory: information conflict in the military sphere: basic elements and concepts. **Information Conflict in Military Sphere**, [s. l.], p. 38-40, Sep 18, 2003.

BOLDYREVA, Elena, Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. 2018/12/31 pg. 102. DO - 10.15405/epsbs.2018.12.02.10 Disponible en: [https://www.researchgate.net/publication/330032180\\_Cambridge\\_Analytica\\_Ethics\\_And\\_Online\\_Manipulation\\_With\\_Decision-Making\\_Process](https://www.researchgate.net/publication/330032180_Cambridge_Analytica_Ethics_And_Online_Manipulation_With_Decision-Making_Process). Acessado em 19 Nov 21.

BORSHCHEVSKAYA, Anna. **Russian Private Military Companies: Continuity and Evolution of the Model**. Russia Foreign Policy Papers, Dec 2019. p. 21. Disponible en: <https://www.fpri.org/wp-content/uploads/2019/12/rfp4-borshchevskaya-final.pdf>. Acessado em 19 Nov 21.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. **Not so private military and security companies: Wagner Group and Russian Prosecution of Great Power Politics**. Washington, D.C.: CSIS, Sept25, 2020. Disponible en: <https://www.csis.org/blogs/post-soviet-post/not-so-private-military-and-security-companies>. Acceso el: 1 oct. 2020.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES. **Moscow's Mercenary Wars**. Washington, D.C.: CSIS, Sept 2020. Disponible en: <https://russianpmcs.csis.org/>. Acessado em 19 Nov 21.

CONGRESSIONAL RESEARCH SERVICE. Sept 16, 2020. **Russian Private Military Companies (PMCs)** Disponible en: <https://crsreports.congress.gov/product/pdf/IF/IF11650>. Acessado em 19 Nov 21.

ЧАУСОВ, Ф. Основы рефлексивного управления противником. **Морской сборник**, [s.l.], n.1, 1999.

DENNING, D. The rise of hacktivism. **Georgetown Journal of International Affairs**, Washington, D.C, Sep 8, 2015. Disponible en: <https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism>. Acceso el: 19 nov. 2021.

DEFENSE INTELLIGENCE AGENCY (United States). **Russia military power: building a military to support great power aspirations**. [Washington, D.C.]: DIA, 2017. p. 116.

ПОДБЕРЕЗКИН, А. **Анализ, стратегический прогноз и планирование в военно-политической области**. 2014. Центр военно-политических исследований, Московский государственный институт международных отношений, Университет МИД России, Московский, 2014. Disponible en: <https://docplayer.com/64510400-Analiz-strategicheskiy-prognoz-i-planirovanie-v-voenno-politicheskoy-oblasti.html>. Acceso el: 22 nov. 2021.

ДОКТРИНА информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от.п. 646, 5 декабря 2016 г. Disponible en: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. Acceso el: 22 nov. 2021.

ГЕРАСИМОВ, В. В. Доклад начальника штаба Вооруженных Сил Российской Федерации: роль государства оборонной организации страны в соответствии с новым положением о штабе, утвержденным Президентом Российской Федерации. **Вестник Академии военных наук**, [s. l.], tom 1, n. 46, с. 14-22, 2014. Disponible en: <http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/639-vestnik-avn-1-2014> .Acceso el: 5 abr. 2018.

FRIDMAN, O. On the "Gerasimov Doctrine": why the West Fails to beat Russia to the punch. **PRISM**, [Washington, D.C], v. 8, n. 2, p. 100-113, 2019. Disponible en: [https://www.jstor.org/stable/26803233?seq=1#metadata\\_info\\_tab\\_contents](https://www.jstor.org/stable/26803233?seq=1#metadata_info_tab_contents). Acceso el: 18 nov. 2021.

GALEOTTI, M. **Moscow's mercenaries reveal the privatisation of Russian geopolitics**. In: OPENDEMOCRACY. London: open Democracy, Aug 29, 2017. Disponible en: <https://www.opendemocracy.net/en/odr/chvk-wagner-and-privatisation-of-russian-geopolitics/> Acceso el: 29 ago. 2017.

GALEOTTI, M. The mythical 'Gerasimov Doctrine' and the language of threat. **Critical Studies on Security**, London, v. 7, n. 2, p. 157-161, 2019. Disponible en: <https://www.tandfonline.com/doi/abs/10.1080/21624887.2018.1441623?journalCode=rscs20>. Acceso el: 18 nov. 2021.

GORENBURG, D. **Russia's military modernization plans: 2018-2027**. In: GORENBURG, D. Russian Military Reform. Cambridge, Nov 27, 2017. Disponible en: <https://russiamil.wordpress.com/2017/11/27/russias-military-modernization-plans-2018-2027/>. Acceso el: 27 nov. 2017.

HAINES, J. R. Russia's use of disinformation in the Ukraine Conflict - analysis. **EurasiaReview**, [s. l.], 18 Feb 2015. Disponible en <http://www.eurasiareview.com/18022015-russias-use-of-disinformation-in-the-ukraine-conflict-analysis/>. Acceso el: 30 mayo 2021.

IBS Center for Management Research. Facebook–Cambridge Analytica Data Scandal. Disponible en: <https://www.icmrindia.org/casestudies/catalogue/Business%20Ethics/BECG160.htm> .Acessado em 19 Nov 21.

Institute For National Strategic Studies (NATIONAL DEFENCE UNIVERSITY), Nov 24, 2020. **Russia's Escalating use of Private Military Companies in Africa**. Disponible en: <https://inss.ndu.edu/Media/News/Article/2425797/russias-escalating-use-of-private-military-companies-in-africa/> . Acessado em 19 Nov 21.

ИОНОВ, М. Д. Психологические аспекты управления противником в антагонистических конфликтах (рефлексивное управление). **Прикладная эргономика**, [s. l.], Специальный выпуск. n. 1, 1994.

ИОНОВ, М. Д. Управление противником. *Морской сборник*, n. 7, 1995.

ISSERSON, G. S. **The evolution of operational**. Translated by Bruce W. Menning. Fort Leavenworth, Kansas: U.S. Army Combined Arms Center's, 2013. Disponible en: <https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/OperationalArt.pdf>. Acceso el: 19 nov. 2017.

ЛЕФЕВР, В. А. Конфликтующие структуры. Москва: Высшая школа, 1967.

ЛЕФЕВР, В. А. Рефлексивный контроль: советская концепция влияния на процесс принятия решений противником. Москва: Научные приложения, 1984.

ЛЕФЕВР, В. А.; СМОЛЯН, Г. Л. **Алгебра конфликта**. 4 е. изд. Москва: Книжный дом, Либроком, 2010.

ЛЕОНЕНКО, С. Рефлексивное управление противником. *Армейский сборник*, [s. l.], n. 8, 1995.

КОМОВ, С. А. Оспособахведенияинформационнойборьбы. *Военнаямысль*, том 4, n. 7-8, с. 18-22, 1997.

КОНОНОВ Д.А., Кульба В.В., Шубин А.Н. **Информационное управление: принципы моделирования и области использования** //Труды ИПУ РАН. Т. XXIII. - М.: ИПУ РАН. 2005. С. 5-29. Kononov D.A., Kulba V.V., Shubin A.N. *Gestão da informação: princípios de modelagem e áreas de uso* // Procedimentos de IPU RAS. T. XXSH. - M.: IPU RAN. 2005.S. 5-29.

КРЕЦУЛ, Р. Россия закрывает «черную дыру» на границе с Украиной. *ВЗГЛЯД.РУ*, Москва, 1 июня 2015. Disponible en: <https://vz.ru/society/2015/6/1/748541.html>. Acceso em: 30 mayo 2021.

LANKINA, T.; WATANABE, K. 'Russian Spring' or 'Spring Betrayal'? The media as a mirror of Putin's evolving strategy in Ukraine. *Europe-AsiaStudies*, [London], v. 69, n. 10, p. 1526-1556, Dec 2017. Disponible en: <https://www.tandfonline.com/doi/full/10.1080/09668136.2017.1397603>. Acceso el: 18 nov. 2021.

ØSTENSEN, Å.; BUKKVOLL, Ø. **Russian use of private military and security companies - the implications for European and Norwegian Security**. Oslo: Chr. Michelsens Institutt, 2018. (FFI-RAPPORT, n. 18/01300). Disponible en: <https://www.cmi.no/publications/6637-russian-use-of-private-military-and-security>. Acceso el: 23 nov. 2021.

РОССИЯ. Президента. Стратегия национальной безопасности Российской Федерации, Москва, n. 400, 2 июля 2021 года. Disponible en: <http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZmR5cER0g5tZC.pdf>. Acceso el: 22 nov. 2021.

RUSSIAN. President of the Russian Federation. Military Doctrine of the Russian Federation, approved by Russian Federation President V. Putin. In: RUSSIAN FEDERATION PRESIDENT. [Moscow], Dec 31, 2014. Disponible en: <http://www.kremlin.ru>. Acceso el: 30 mayo 2021.

RUSSIA'S new maritime doctrine. **Jane's Defense Weekly**, [s. l.], p. 4, Aug 14, 2015.

SUTYAGIN, I. Detailing Russian Forces in Syria. In: THE ROYAL UNITED SERVICES INSTITUTE. **Defense Systems**. London: RUSI, Nov 13, 2015. Disponible en: <https://rusi.org/explore-our-research/publications/rusi-defence-systems/detailing-russian-forces-in-syria>. Acceso el: 30 mayo 2021.

ТУРКО, Н.И.; МОДЕСТОВ, С.А. **Рефлексивное управление развитием стратегических сил как механизм современной геополитики: Системный анализ на пороге 21 века**||: теория и практика» Москва, февраль 1996 г. с. 366.

SZOSTEK, J. The power and limits of Russia's strategic narrative in Ukraine: the role of linkage. **Perspectives on Politics**, Cambridge, v. 15, n. 2, p. 379-395, 2017. Disponible en: <https://eprints.gla.ac.uk/167897/> Acceso el: 18 nov. 2021.

