Revista del Instituto Español de Estudios Estratégicos
ISSN-e: 2255-3479

Pau Muñoz Pairet
Ingeniero informático y politólogo. Doctorado en estudios estratégicos por la Universidad de Salamanca. Analista de inteligencia

Correo electrónico: munyoz.15@gmail.com

La doctrina de las grandes potencias en la guerra de la información

The doctrine of the great powers in information warfare

Resumen

La guerra de la información es un tipo de conflicto que trasciende el ámbito tradicional del enfrentamiento armado. La lucha por el control y a través de la información ha estado presente a lo largo de toda la historia humana, evolucionando con cada avance en las tecnologías de gestión de la información, del pergamino a internet. A través de un análisis comparativo, el presente artículo se centra en la visión y enfoque doctrinal de las tres grandes potencias actuales: Estados Unidos, China y Rusia. Dadas sus avanzadas capacidades mediáticas y tecnológicas, estas potencias se erigen como protagonistas dominantes en este escenario de confrontación informativa. Del mismo modo, su estatus en el sistema internacional, del que se deriva una gran amalgama de intereses contrapuestos, las sitúa en un escenario de conflicto latente permanente. Por ello, ofrecen la mayor base de ejemplos y recursos para el estudio de dicho fenómeno. Al examinar su historia reciente, así como sus documentos doctrinales y principales aportes académicos, se alcanza a entender no solo sus estrategias y tácticas, sino también las

dinámicas de competencia y la evolución de la guerra de la información en el contexto contemporáneo.

Palabras clave

Guerra cognitiva, Ciberguerra, Propaganda, Realismo, Política exterior.

Abstract

Information warfare is a type of conflict that transcends the traditional realm of armed confrontation. The struggle within the information domain has persisted throughout human history, evolving with every advancement in information management technologies, from parchment to the internet. Through a comparative analysis, this paper focuses on the doctrinal vision and approach of the three current major powers: the United States, China, and Russia. Given their advanced media and technological capabilities, these powers emerge as dominant protagonists in this informational confrontation arena. Similarly, their status in the international system, from which a vast array of opposing interests arises, places them in a perpetually latent conflict scenario. Hence, they provide the most substantial base of examples and resources for the study of this phenomenon. By examining their recent history, as well as their doctrinal documents and primary academic contributions, we come to understand not only their strategies and tactics but also the dynamics of competition and the evolution of information warfare in the contemporary context.

Keywords

Cognitive warfare, Cyberwarfare, Propaganda, Realism, Foreign policy.

Citar este artículo:

Muñoz Pairet, P. (2024). La doctrina de las grandes potencias en la Guerra de la Información. *Revista del Instituto Español de Estudios Estratégicos*. N.º 23, pp. 85-118.

1. Introducción

La premisa «La información es poder» ha resonado de manera constante en la historia de la humanidad. A lo largo de los distintos periodos de la historia humana, el manejo de la información ha dominado la dinámica política en numerosos escenarios: influenciando tácticas, operaciones y estrategias en todo el mundo. Su influencia histórica ha sido y es transversal, se ha manifestado tanto en tiempos de conflicto como en tiempos de paz. Durante periodos de guerra, la información se ha constituido doblemente como arma y campo de batalla, siendo empleada para el engaño, la implementación de camuflajes o señuelos, la difusión de rumores y la interceptación de comunicaciones enemigas. En tiempos de paz, ha representado la piedra angular del espionaje, herramienta clave para la manipulación política en sus diversas formas. En este aspecto, el control de la información ha sido empleado tanto de manera defensiva como ofensiva.

La competencia por controlar el dominio de la información no es un fenómeno reciente. De hecho, ha sido objeto de análisis y documentación en múltiples culturas a lo largo de la historia; desde las enseñanzas de Sun Tzu en China y Kautiliya en la India, hasta las reflexiones de Jenofonte y Tucídides en la Grecia clásica. La misma importancia se observa en Roma, en el *Stratagemata* de Frontino y, siglos más tarde, en *El Príncipe* de Maquiavelo. Estas obras, entre muchas otras, subrayaron el valor intrínseco de la información y cómo su dominio y manejo han influenciado la cultura estratégica de las distintas naciones a lo largo del tiempo (Gilpin, 1984).

A medida que la tecnología avanzaba, su impacto en la gestión de la información se hacía evidente. Desde la invención de la imprenta, pasando por la llegada de la radio y más recientemente, la proliferación de internet, cada innovación técnica fue adoptada y adaptada rápido para servir en la guerra de la información. No solo las innovaciones tecnológicas, sino también los avances sociales, en particular la Revolución Industrial, han jugado un papel fundamental en la estructuración y desarrollo de las estrategias y tácticas de este tipo de conflicto. Estos avances motivaron a Ejércitos y servicios de inteligencia de diversas naciones a desarrollar y fortalecer sus capacidades en la guerra de la información. Como resultado, estos métodos y técnicas no solo se emplean en conflictos armados, sino que también son fundamentales en acciones encubiertas y en la diseminación de propaganda estatal.

La guerra de la información contemporánea, se encuentra en una fase de consolidación. Desde la Segunda Guerra Mundial (IIGM) ha experimentado un fuerte desarrollo, incrementado en las últimas décadas, hasta ser reconocida en la actualidad como una forma autónoma de conflicto, merecedora de estudio y análisis en sí misma. Su relevancia es tal que, en muchas ocasiones, se convierte en el núcleo de las operaciones militares y es esencial en las modernas estrategias de proyección de poder político.

Si bien la guerra de la información es un fenómeno global en el que intervienen múltiples actores estatales y no estatales, son las grandes potencias las que, en la

actualidad, dominan con mayor intensidad este escenario. Naturalmente, la guerra de la información es un fenómeno complejo, el cual requiere tanto de sistemas de inteligencia sólidos, una particular capacidad de influencia global y un sector tecnológico muy desarrollado. Así, el dominio de las grandes potencias sobre este modo de guerra se debe en gran parte a sus avanzados sectores mediáticos y tecnológicos. Estas potencias no solo tienen las capacidades, sino también intereses enfrentados que les impulsan a competir en este ámbito, con el objetivo primordial de ampliar su influencia a nivel mundial.

Este artículo se centra en el estudio de la guerra de la información desde la perspectiva de las tres grandes potencias del sistema internacional: Estados Unidos, China y Rusia. A través de un análisis comparativo, se examinan sus enfoques doctrinales. Más allá de entender sus capacidades y potencialidades en el ámbito de la guerra de la información, esta investigación permite estudiar sus dinámicas de competencia, así como la evolución este modo de guerra a lo largo de la historia reciente.

Para llevar a cabo el análisis, se han tomado en consideración los principales documentos doctrinales disponibles en publicaciones oficiales. Del mismo modo, se han tenido en cuenta las contribuciones y análisis de destacados intelectuales y centros de pensamiento militar de cada una de estas naciones.

2. La guerra en el dominio de la información

La guerra de la información se define como un modo de guerra que implica la manipulación, distribución y, en ocasiones, negación de información. Su propósito principal es lograr una ventaja competitiva sobre el adversario, protegiendo simultáneamente los propios sistemas de información (Libicki, 1995). La finalidad es influir en las decisiones, comportamientos, percepciones y capacidades del adversario. Para lograrlo, se emplea un amplio espectro de herramientas y tácticas, que abarcan desde las tradicionales, como la propaganda y la desinformación, hasta las más contemporáneas, como las operaciones cibernéticas y la guerra electrónica (Libicki, 2017).

La definición comprende tanto los métodos tradicionales de la guerra de la información, fundamentalmente basados en el aspecto cognitivo, como la propaganda, como los más recientes, tales como las operaciones técnicas en el ciberespacio. Este modo de guerra puede manifestarse en diversos contextos, ya sea en tiempos de paz o durante un conflicto armado, y puede ser ejecutada por actores estatales y no estatales.

El conflicto en el espacio de la información es transversal a todo lo referente al manejo de la información. No solo se centra en los canales de comunicación, sino también en quienes emiten y reciben la información, así como en el contenido del mensaje en sí. Dentro de este enfoque, se reconoce al ser humano como un actor vital, desempeñando de forma simultánea los roles de emisor y receptor dentro del vasto ecosistema de la información. Por ende, cuando se habla de la guerra de la información, se hace referencia tanto a operaciones que atacan o defienden el aspecto cognitivo de la

información —por ejemplo, la desinformación y la propaganda— como a aquellas que se centran en su dimensión tecnológica, como la guerra electrónica, el ciberespionaje y la ciberguerra (Aro, 2016; Robinson, 2015; Sampanis, 2024).

Más allá del empleo de innovaciones tecnológicas, este modo de combatir se caracteriza por su versatilidad y adaptabilidad. Así, puede manifestarse sutilmente en tiempos de paz entre naciones, evidenciándose a través de actividades como el espionaje o la influencia política. En un contexto de guerra abierta, tiene la capacidad de intensificarse y adaptarse rápido a contextos más beligerantes. En este tipo de escenarios de conflicto abierto, puede escalar hacia tácticas más agresivas, como la guerra electrónica, la diseminación masiva de desinformación o incluso ciberataques con objetivos de puro sabotaje. Todas son operaciones que se intensifican a partir de una base preexistente construida antes de la guerra convencional, sobre tácticas ya establecidas.

Una vez que el conflicto ha cesado, las operaciones en el ámbito de la guerra de la información pueden disminuir en intensidad, adaptándose al nuevo escenario de posguerra. Sin embargo, estas operaciones nunca desaparecen por completo; sino que se transforman y se adaptan según las circunstancias.

Así, este enfoque adaptable de la guerra de la información la convierte en una de las principales herramientas al servicio de las operaciones de guerra híbrida, modo de guerra que combina tácticas convencionales y no convencionales en un mismo escenario militar (Hoffman, 2007). En este contexto, la guerra de la información se alinea perfectamente con el concepto de acciones en zona gris, operaciones que se sitúan entre la paz y el conflicto declarado y que buscan explotar las ambigüedades y vacíos en las reglas y normas internacionales (Votel, 2016; Liu, 2024).

3. Las grandes potencias en la guerra de la información

Para comprender de manera cabal las dinámicas en el sistema internacional, caracterizado por su habitual naturaleza anárquica, se recurre a las principales teorías que han intentado explicar este tipo de relaciones. Entre las múltiples corrientes existentes, la perspectiva realista emerge como la predominante en el estudio contemporáneo de las Relaciones Internacionales (RR. II). El realismo no es monolítico y presenta subcorrientes significativas, entre las que se puede identificar el realismo neoclásico, el realismo estructuralista —conocido también como defensivo, representado por teóricos como Waltz— y el realismo ofensivo, cuya principal figura es Mearsheimer (Waltz, 2018; Mearsheimer, 2001).

La óptica del realismo ofensivo destaca por ofrecer una herramienta conceptual y muy enriquecedora en cuanto al abordaje de la guerra de la información entre las grandes potencias. Bajo este prisma, tal guerra no es una anomalía, sino un componente inevitable y persistente del juego de poder internacional.

Dentro de este marco teórico y respaldado por el consenso en el campo de las RR. II, Mearsheimer conceptualiza a las grandes potencias como aquellos Estados dotados de fuerzas militares lo suficientemente robustas como para no solo defender su territorio sino también proyectar poder más allá de sus fronteras (Mearsheimer, 2001). Estos cuentan con capacidades nucleares y un avanzado entorno tecnológico. Además, sus recursos y fortaleza económica les otorgan una notable autosuficiencia. Asimismo, estas potencias se caracterizan por mantener un alto grado de autonomía política y poseen sistemas políticos y culturales distintivos que tienen la potencia de ser promovidos o defendidos internacionalmente como herramientas de influencia. Naturalmente, esta conjunción de factores alimenta su ambición geopolítica.

En esta misma línea, es preciso subrayar que, si alguna de estas grandes potencias logra consolidar una hegemonía a nivel regional, puede ser categorizada como una superpotencia o potencia hegemónica. Esta designación tiene implicaciones profundas en el equilibrio del sistema internacional y en cómo estas entidades interactúan con sus contrapartes.

Actualmente, Rusia, China y Estados Unidos dominan el escenario global en calidad de grandes potencias. El país americano, a su vez, ostenta un papel de liderazgo en el sistema, establecida como la única superpotencia en el sistema internacional. A pesar de la actual hegemonía regional estadounidense, no se puede obviar la ascendente presencia de China en el sistema y su manifiesta intención de alcanzar una posición semejante en los próximos años.

Así pues, el enfoque del realismo ofensivo, como esboza Mearsheimer, postula que, en un sistema internacional anárquico, estas grandes potencias, en su afán por garantizar su propia seguridad, se inclinan a maximizar su poder (Mearsheimer, 2001). Esta expansión de poder, si las condiciones son propicias, puede materializarse mediante la intervención militar directa. La lógica subyacente sugiere que, en el largo plazo, el conflicto entre estas potencias se vuelve más probable, en especial cuando halla en un contexto de multipolaridad desequilibrada[1]. El reciente crecimiento de China señala que el sistema internacional está en transición hacia este tipo de configuración (Mearsheimer, 2021). En este sentido Estados Unidos, acorde a los postulados de este enfoque en RR. II, se encuentra en proceso de adaptación de su política exterior, para hacer frente a la competición de poder en el Indo-Pacífico (Perez, 2023).

En la pugna por la hegemonía global, el enfrentamiento entre las grandes potencias es un hecho prácticamente asegurado. El establecimiento y consolidación de la hegemonía no solo implica un predominio militar o económico, sino también una influencia política y cultural decisiva en el resto del sistema. Por ello, es común que estas potencias entren en colisión al intentar ejercer su influencia en regiones similares o al intentar socavar el dominio regional de sus rivales. La guerra de la información emerge, en este contexto, como una herramienta estratégica esencial. Su ventaja radica

1 La multipolaridad desequilibrada hace referencia a una situación caracterizada por la presencia de varias grandes potencias, pero sin un líder claro o indiscutible.

en que suele acarrear costos políticos mínimos, pero con la capacidad de escalar hacia operaciones más agresivas y extensas en caso de desembocar en un enfrentamiento militar tradicional (Harknett, 1996). Dadas estas dinámicas, la guerra de la información no solo es probable, sino inevitable en la arena global. La relevancia de examinar este fenómeno desde la perspectiva de las grandes potencias es indiscutible. Estas naciones, dada su vasta reserva de recursos, intereses estratégicos y capacidad de autosuficiencia, están en una posición inigualable para formular y dictar doctrinas específicas. Además, poseen la capacidad y los medios para desarrollar técnicas y estrategias nítidas en el ámbito de la guerra de la información, reflejando así un estilo distintivo y característico.

Para poder investigar este fenómeno, resulta esencial abordarlo mediante el análisis doctrinal de estas potencias preponderantes. Una metodología efectiva para este estudio implica el examen detenido de documentos oficiales emitidos por dichas potencias.

Para estudiar de manera práctica la doctrina de un país alrededor de la guerra de la información se partir del análisis de los principales documentos oficiales en una estrategia multinivel combinando el análisis del contexto histórico, con el legal y el relativo a la doctrina militar.

Antes de iniciar el análisis doctrinal, es importante tener presente el contexto histórico del país, tanto en lo relativo a su política interna como en cuanto a su interacción con el resto de las potencias, pues sus hechos históricos, leyendas y mitos podrán ser con frecuencia instrumentalizados en la guerra de la información, su tendencia histórica naturalmente dará una idea general sobre su modo de actuar. A la hora de analizar la doctrina de un país, se debe prestar atención, en primer lugar, en los documentos doctrinales oficiales al respecto, emitidos por el respectivo Ministerio de Defensa, Consejo de Seguridad Nacional u organización de alto nivel equivalente. Dichos documentos no serán sino la conjugación del contexto histórico del país, su idiosincrasia política, su interés nacional y sus capacidades. En el caso de disponer de documentos doctrinales oficiales para el periodo de estudio en particular, el análisis podrá emanar en gran medida de estos. A la hora de estudiar la doctrina estadounidense se analizarán los documentos *Joint Doctrine Publications* y las distintas iteraciones de la *National Security Strategy*, documento que, o bien cubren la visión estadounidense oficial en materias específicas de este fenómeno como la guerra psicológica o la ciberguerra, o cubren la estrategia general del país en el que se incluyen dichos aspectos. En cuanto al estudio de China se pondrá el foco en los distintos libros b lancos, en su discusión sobre la Defensa Nacional, los documentos de la Política de Defensa, así como los distintos manuales militares específicos relativos a dichas materias. Por último, en el caso ruso, se estudiará la Doctrina Militar de la Federación Rusa las distintas iteraciones del Concepto de Seguridad Nacional, complementándolas con las Estrategias de Seguridad Nacional y Política Exterior lanzadas de forma periódica por la oficina del presidente.

En el segundo nivel de análisis se encuentra el conjunto de instrumentos legales y resoluciones ejecutivas relativas a los distintos subdominios de la guerra de la información. Si bien dichos documentos no establecen una doctrina tras su publicación, ya que las resoluciones afectan a desarrollos parciales y las leyes pueden

ser interpretadas o aplicadas de distintos modos, sí permiten establecer las capacidades y posibilidades del país a la hora de confrontar en dicho dominio.

El tercer nivel del análisis estará compuesto por el compendio de publicaciones emitidas en los principales centros de pensamiento del país en materia militar, de seguridad o estudios estratégicos en general. Si bien los documentos publicados en dichos foros pavimentan el terreno para el establecimiento de doctrinas formales, su naturaleza académica y prospectiva hace que el trabajo en su seno suela estar notablemente más avanzado a la realidad práctica del país. Resulta pues, muy habitual ver como trabajos de análisis y reflexión sobre materias relativas a la guerra de la información publicados en las principales revistas y foros estratégicos terminen dando pie al establecimiento o simple formalización de las propias doctrinas nacionales. En Estados Unidos se pone el foco, en gran medida, en el trabajo publicado en instituciones como la Rand Corporation o el Military Review. En Rusia se analiza el contenido de publicaciones como *Военное Обозрение* (Revisión Militar) y *Военно-промышленный курьер* (Correo militar-industrial). En China se explora el 解放军报 (*Diario del EPL*), así como el 中国国防报 (*Periódico de Defensa Nacional*).

Por último, se puede complementar el análisis con el estudio de las operaciones de información conocidas, la estructura de las fuerzas armadas y las principales corrientes ideológicas en política internacional en los respectivos países, así como se debe tener en cuenta la propia posición del país en el sistema internacional y su estado en cuanto al desarrollo de sus sistemas mediático y científico-técnico, pues a través de dichos sistemas podrá construir sus capacidades.

A la hora de llevar a cabo este análisis, se ha tenido como base el estudio de dichos documentos, a través de la metodología presentada.

3.1. La doctrina estadounidense

La guerra de la información, tal como se conoce actualmente, se originó como un término empleado en los círculos militares de los Estados Unidos durante los años 80. No obstante, su esencia y aplicación práctica se remontan todavía más atrás en el tiempo. Fue tras guerra del Golfo, cuando este término adquirió la importancia esencial que hoy en día mantiene, destacando la relevancia de la información y la desinformación en el teatro de operaciones.

Si se rastrean los orígenes de la implementación organizada de tácticas de guerra de la información por parte de los Estados Unidos, se encuentra con que estas se remontan a las primeras décadas del siglo pasado. Fue durante dicho periodo cuando teóricos como Lasswell y Lippman comenzaron a desarrollar conceptos y estrategias alrededor del poder de la información (Laswell, 1948; Lippman, 1946). Su trabajo construyó las bases para establecer un marco teórico y práctico en el cual los Estados Unidos podrían comenzar a operar. El propio Lippman tuvo un rol central al participar en la fundación y dirección del comité de opinión pública, articulando gran parte de la propaganda de

guerra estadounidense en la IIGM, alrededor de conceptos innovadores, desde la radio hasta el empleo de viñetas humorísticas (Ruiz, 2018).

A nivel militar, se pueden trasladar los esfuerzos iniciales en la guerra de la información estadounidense a la Segunda Guerra Mundial. Tanto en este conflicto como en la Guerra Fría, Estados Unidos intensificó sus tácticas en la guerra de la información. Durante estos tiempos, incorporó tácticas y estrategias específicas para dominar el ámbito informativo. Hollywood produjo películas que favorecían los valores estadounidenses y combatían la propaganda adversaria, mientras que el gobierno estadounidense impulsó esfuerzos propagandísticos a través de agencias como el Comité de Opinión Pública y la creación de agentes propagandísticos como los Four minute men[2].

Más allá de la mera propaganda interna, las tácticas militares de la época incorporaron elementos de engaño y camuflaje, alcanzando nuevas cotas de complejidad. Ejemplos notables incluyen el uso de tanques hinchables, hogueras o altavoces, así como otras simulaciones para engañar al enemigo sobre la ubicación y la magnitud de las fuerzas aliadas. La conocida operación Mincemeat a su vez, constituye otro ejemplo clásico de engaño estratégico donde el cuerpo de un hombre muerto fue empleado para transmitir información falsa a los nazis.

El ámbito de la guerra electrónica experimento una gran revolución durante dicho período. Las unidades de Beach Jumpers fueron establecidas por la marina de Estados Unidos para llevar a cabo operaciones de engaño, basadas sobre todo en el *jamming* y el despliegue de señuelos electrónicos. Del mismo modo, la interceptación y protección de la información también se convirtieron en áreas clave, tal como se apreció en la colaboración entre los aliados para descifrar códigos nazis y en el uso del Navajo en las comunicaciones, un idioma indígena utilizado como un código casi indescifrable en la época.

Durante el avance de la Guerra Fría en los años sesenta y setenta, la guerra de la Información fue central entre EE. UU. y la URSS enfocándose en espionaje e ideología. EE. UU. y sus aliados debatían ideológicamente contra la URSS y el comunismo, buscando promover valores democráticos y capitalistas. Para ello, EE. UU. usó medios de comunicación, programas educativos y apoyo a organizaciones prodemocracia, actuando de forma abierta y encubierta. Iniciativas como La Voz de América y Radio Free Europe/Radio Liberty difundieron noticias en zonas con censura, mientras que documentos como el informe Church revelaron tácticas encubiertas de la Agencia Central de Inteligencia (CIA) en la guerra de la información. En el ámbito educativo, programas como Fullbright, centrado en intercambios educativos y culturales, buscaban proyectar valores y prácticas democráticas en el extranjero garantizando la influencia estadounidense a través del poder blando (Nye, 1990).

2 Los Four minute men eran los encargados de lanzar discursos por la radio, buscando maximizar el apoyo de la población a la participación en el conflicto.

Sin embargo, no todo estaba dirigido hacia el exterior; la operación CHAOS, bajo el mandato del presidente Johnson, nació en el contexto de la guerra en Vietnam con el objetivo monitorear a grupos domésticos antiguerra, reflejando la creciente preocupación por los efectos de la guerra de la información dentro de las propias fronteras del país. Esta preocupación también fue palpable durante la propia guerra contra el Viet Cong[3], donde operaciones psicológicas, como la Wandering Soul, se basaban en un profundo entendimiento de la cultura vietnamita y existía un intento constante por manejar y controlar la narrativa presentada por la prensa.

En la década de los 80, con Ronald Reagan como presidente, EE. UU. intensificó su postura ideológica. En 1982, la administración Reagan buscó fortalecer la infraestructura de la democracia, invirtiendo más en medios y organizaciones prodemocráticos. En 1983, se fundó la Fundación Nacional para la Democracia (*National Endowment for Democracy*, NED) con 31.3 millones de dólares de presupuesto inicial, destinada a apoyar la democracia, la libertad de prensa y derechos humanos en áreas influenciadas por el comunismo.

A su vez, durante este período, la guerra de la información tomó un carácter más estratégico. La Iniciativa de Defensa Estratégica[4] desmoralizó a la URSS, etiquetada como el imperio del mal por Reagan, en su competencia con la Organización del Tratado del Atlántico Norte. En América Latina, se crearon Radio y Televisión Martí en 1985 y 1990 para influir en Cuba y EE. UU. apoyó a los Contras en Nicaragua, reafirmando su postura anticomunista, mostrando que, en la guerra de la información, las batallas ideológicas influían en la historia tanto como el poder militar.

Las décadas de 1990 y 2000 trajeron consigo nuevos desafíos derivados de la sofisticación técnica y profesional que permitió la puesta en marcha de canales de noticias en veintiocuatro horas y la posterior emergencia de la comunicación en internet. Durante los años noventa, el efecto *CNN* y la guerra televisada demostraron el poder de los medios a la hora de influir en una opinión pública esencial para justificar la política exterior estadounidense (Robinson, 1999). Esto quedaría especialmente patente durante la guerra del golfo y las sucesivas guerras balcánicas, donde la propia opinión pública del país tuvo un papel clave a la hora de facilitar la intervención militar. Así pues, en respuesta a la creciente importancia de la percepción pública en el contexto internacional, las sucesivas administraciones estadounidenses empezaron a moverse de la acción psicológica a la comunicación estratégica. Se observó un enfoque en la manipulación directa o la influencia de la opinión pública para obtener apoyo a acciones militares y políticas en el extranjero. Este enfoque integró los medios de comunicación como herramientas esenciales en la guerra de la información, utilizando coberturas en tiempo real y reportajes intensivos para fomentar narrativas que alinearan a la opinión pública con los objetivos de política exterior del gobierno (Robinson, 1999).

3 Viet Cong: contracción de Việt Nam Cộng-sản (comunista vietnamita).

4 La Iniciativa de Defensa Estratégica era popularmente conocida como iniciativa «star wars».

A su vez, la transición tecnológica, representada por la expansión del internet y la digitalización, demandó un replanteamiento de la seguridad de la información. Las administraciones de Bush y Clinton iniciaron esfuerzos tanto defensivos como ofensivos en el ciberespacio. Con resoluciones, como la Directiva de Seguridad Nacional 42 y la formación de grupos de trabajo, Estados Unidos buscó fortalecer su infraestructura de información. En medio de estos avances técnicos, hubo un reconocimiento de la necesidad de un marco teórico más coherente. Libicki (1995) y Johnson (2004), entre otros, trabajaron en la desambiguación y estructuración del concepto de guerra de la información, generando un marco de comprensión integral, no solo desde un ángulo técnico, sino también cognitivo y psicológico.

Así pues, el cambio de milenio vio una rápida formalización de estas ideas. Documentos como *Joint Vision 2010* y la Doctrina Conjunta para Operaciones de Información surgieron como puntos de referencia en la guerra de la información. Además, la serie de *Joint Publications* detalló operaciones específicas, desde la guerra electrónica hasta las operaciones en el ciberespacio.

Los ataques del 11 de septiembre de 2001 reconfiguraron la percepción de seguridad en Estados Unidos. Las tácticas de guerra de la información ya no eran solo herramientas en la pugna de los Estados-nación, sino también de actores no estatales (Soriano, 2018). En el escenario contemporáneo, post-2018, el Departamento de Defensa de EE. UU. ha reconocido la importancia de la guerra cognitiva. El énfasis actual está en la comunicación estratégica (STRATCOM), alejándose de la manipulación psicológica pura hacia un intento de influencia positiva y explicativa, donde la justificación de las acciones militares se coloca en el centro del escenario.

En la actualidad, en cuanto a la guerra de la información, si bien no existe una definición oficial del gobierno de los EE. UU., los principales analistas militares y oficiales la solían conceptualizar como una estrategia o un proceso de planificación para alcanzar objetivos y metas de interés nacional, para el uso y la gestión de la información con el objetivo de obtener una ventaja competitiva, incluyendo operaciones tanto defensivas como ofensivas. Al respecto de esto, las operaciones (de información), desarrolladas extensivamente en las décadas anteriores, representan el eslabón que conecta los objetivos estratégicos con tácticas, técnicas y procedimientos. Más allá de la falta de una definición unificada, cabe destacar que diversos organismos y expertos del país han aportado sus propias perspectivas al respecto y las mantienen como marco doctrinal de trabajo, siendo el Departamento de Defensa (*Department of Defense* DoD) la organización más relevante. Así pues, el DoD ha conceptualizado la Guerra de la Información desde principios del siglo como una interrelación entre los sistemas de información físicos y la información en sí misma (*Understanding Gray zone warfare from multiple perspectives*, 2023). La guerra de la información se centraría en afectar el proceso (militar) de toma de decisiones mediante el ataque a los sistemas físicos de información o a la información en sí.

Es importante entender que, según el enfoque de la doctrina estadounidense, estas actividades se desarrollan dentro del dominio de la información, el cual

comprende tres dimensiones principales: física, comunicativa o información y cognitiva. En la era digital actual todos los instrumentos del poder nacional pueden proyectarse y emplearse en este nuevo entorno, incluso por elementos no militares del gobierno, respondiendo a una estrategia común (*The White House*, 2022). En cuanto al aspecto de la guerra de la información basada en el aspecto cognitivo, en EE. UU. se identifican tres categorías principales, es decir, tres formas en las que la información puede ser manipulada o sesgada, a saber, propaganda, información errónea (*misinformation*) centrada en confundir al enemigo y desinformación o información sesgada con partes, posiblemente falsas centrada en buscar el engaño y la manipulación (ODNI, 2023).

El enfoque estratégico actual de los EE. UU. al respecto, se centra en la difusión de información precisa y veraz combinada con el empleo de la propaganda para influir en la opinión pública en las sociedades enemigas (USA-JCS, 2022). Para ello, el gobierno estadounidense, a través de varias iniciativas nacionales, patrocina de manera habitual tecnologías de identificación de información falsa, agencias de verificación de noticias y entidades similares. Este *modus operandi* se aplica tanto de manera interna en el país, a modo defensivo, como en el exterior, buscando neutralizar narrativas enemigas, sustituyéndolas por la propia propaganda, a través de medios favorables y medios oficiales como la *Voz de América* y similares.

No obstante, a diferencia de las potencias autocráticas, analizadas más adelante, EE. UU. se esfuerza por aplicar las tácticas de guerra de la información de una manera ofensiva, pero también defensiva, donde la ética es importante y debe respetarse la libertad de prensa. Del mismo modo, la compleja red de agencias y unidades vinculadas a la guerra de la información en los EE. UU. así como la naturaleza democrática del país, hace especialmente difícil la realización de según qué tipo de acciones de manera coordinada y efectiva, algo de lo que no adolecen las potencias autocráticas.

En cuanto a las acciones en el ciberespacio, la estrategia estadounidense presenta enormes ventajas en comparación con sus adversarios, debido a la fortaleza y la sofisticación científico-técnica del complejo militar industrial, así como la posibilidad de establecer acuerdos y vínculos con empresas estratégicas de la talla de Google, Microsoft o entidades certificadoras vinculadas a sistemas de cifrado.

Así pues, las capacidades en guerra de la información de los EE. UU. se encuentran organizadas a través de una compleja red de agencias gubernamentales, unidades de las Fuerzas Armadas y el apoyo indispensable de centros de pensamiento y el complejo militar-industrial. Si bien en los EE. UU., las acciones de influencia y la propaganda a favor de su política exterior puede realizarse a través de una red en la que ONG, empresas estratégicas e incluso individuales pueden operar de una manera más o menos coordinada con los intereses del gobierno, las principales capacidades en esta materia se encuentran repartidas entre los Servicios de Inteligencia, las Fuerzas Armadas y el Departamento de Estado (ODNI, 2023).

3.2. La doctrina rusa

La aproximación rusa a la Guerra de la Información, si bien no se aleja del planteamiento general del concepto, tiene raíces profundas en su historia. Cabe recordar pues, que la relación de Rusia con el control de la información y la propaganda en los tiempos modernos es tan antigua como la propia Revolución Rusa. Fue durante dicho período, cuando el manejo de la información cobró especial relevancia, convirtiéndose tanto en arma como en campo de batalla, en un escenario en el que las líneas entre política y guerra se volvían cada vez más borrosas. El auge del partido comunista y el triunfo de la Revolución de Octubre marcarían el inicio de una tradición histórica en la guerra de la información, permitiendo el desarrollo de un enfoque único.

Tras la Revolución de Octubre de 1917, la propaganda se convirtió en una de las principales armas en el arsenal bolchevique, siendo empleada para legitimarse, ampliar el apoyo popular y consolidar su poder a través del espacio informativo. Se difundían carteles, folletos y periódicos con mensajes probolcheviques. Durante la Guerra Civil rusa (1918-1922), la propaganda buscaba desestabilizar a opositores tanto dentro como fuera de Rusia. El fervor revolucionario trascendió las fronteras rusas, influyendo en Europa, con el respaldo del Partido Comunista.

Tras alcanzar victorias militares en la guerra y consolidar su poder, el Partido Comunista, consciente de su valor, comenzó a articular una estrategia amplia para el control absoluto del dominio de la información. En el plano oficial, los bolcheviques comenzaron consolidando su control sobre el espacio de los medios de comunicación. Así, poco después de la Revolución de Octubre, emitieron el Decreto sobre la Prensa, estableciendo restricciones sobre la prensa no socialista, asegurando así un dominio casi total sobre el discurso público. Paralelamente, se creó la Cheka[5], la policía secreta bolchevique. Más allá de su labor en inteligencia, desempeñó un papel esencial en la difusión del mensaje bolchevique, en especial, en la represión de cualquier forma de disidencia.

En cuanto al manejo de la guerra de la información, de manera transversal, un pilar central en este aparato propagandístico fue la Agitprop[6], establecida en 1920 (Mally, 2003). Como brazo propagandístico principal del partido, desempeñó un papel crucial en la promoción de la ideología comunista, tanto dentro como fuera de la URSS. Dicho comité destacó por su gran manejo del espacio informativo, poniendo la creatividad y las tecnologías de la época al servicio de la propaganda. Aparecen ejemplos claros de esto en los posters rosta, una serie de carteles propagandísticos creados por la agencia de noticias oficial Rosta entre 1919 y 1922. Estos carteles fueron pioneros en la estrategia propagandística rusa y serían empleados por parte del partido a lo largo de

5 La Cheka fue una comisión extraordinaria panrusa (*Всероссийская Чрезвычáйная Комиссия*).

6 La Agitprop fue un departamento para la agitación y propaganda, integrado en los Comités Central y regionales del Partido Comunista de la URSS.

toda la Guerra Fría, siendo equivalentes a los actuales memes tan relevantes en las redes sociales en línea. Del mismo modo, estaciones como Radio Moscú, se convirtieron en los primeros instrumentos de proyección de influencia internacional en el país.

La Internacional Comunista, o Comintern, surgió en 1919 para propagar la revolución comunista de forma global, reflejando la estrategia rusa de ganar aliados ideológicos contra influencias capitalistas. Esta organización, activa desde 1920 hasta 1943, puso la ideología al servicio de la propaganda y estrategia de la URSS. Sus acciones se basaron en documentos doctrinales, como las «21 Condiciones» de 1920, que enfatizaban la lealtad a Moscú y la revolución violenta. El Programa del Comintern de 1928 reafirmó estos objetivos, promoviendo la dictadura del proletariado global.

Desde sus primeros días, el Comintern fue resuelto en su misión. Su mandato, de combatir a organizaciones burguesas y de luchar por una república soviética internacional, puso de manifiesto su objetivo revolucionario global. Sin embargo, sus esfuerzos por catalizar revoluciones comunistas en Europa, post-Primera Guerra Mundial, aunque apasionados, tuvieron un éxito limitado. Trataron de capitalizar el descontento en países como Alemania, sobre todo en la frágil República de Weimar y Hungría, donde brevemente surgió una república soviética en 1919. Sin embargo, las circunstancias políticas y sociales no siempre favorecieron el surgimiento de regímenes comunistas duraderos. En muchos de los escenarios de conflicto, la ideología comunista tuvo que luchar contra movimientos reaccionarios y el nacionalismo local.

Tras constatar como los resultados del Comintern en Europa no eran del todo favorables, la organización desplazó su mirada hacia Asia. Siendo un continente con vastos territorios y poblaciones y donde el descontento colonial y postcolonial ofrecía oportunidades para el comunismo. Así, su apoyo fue fundamental en la fundación del Partido Comunista chino en 1921, que se convertiría en una de las fuerzas comunistas más poderosas del mundo.

La década de 1930 presentaría nuevos desafíos para la acción de influencia soviética en Europa debido al auge del fascismo en el continente. En respuesta, el Comintern adoptó una firme postura antifascista, instando a los partidos comunistas a formar alianzas, conocidas como frentes populares, con otros grupos de izquierda para contrarrestar la amenaza. Pero la geopolítica es siempre compleja y durante el Pacto Molotov-Ribbentrop entre 1939 y 1941, el Comintern tuvo que adoptar una postura de neutralidad hacia la Alemania nazi. Esta posición cambiaría de forma drástica con la invasión alemana de la URSS en 1941, haciendo volver al Comintern al apoyo aguerrido de la resistencia antinazi en Europa. No obstante, la realidad geoestratégica soviética en el contexto de la Segunda Guerra Mundial exigía una flexibilidad política que el Comintern no podía gestionar. En 1943, Stalin disolvió el Comintern, en parte como un gesto hacia sus nuevos aliados occidentales. Argumentó que el Comintern había cumplido su función y ya no era necesario en la nueva etapa de la política global.

Si bien el Comintern fue disuelto, esto no significó la pérdida de capacidades de la URSS en guerra de la información, más al contrario. En paralelo a iniciativas ideológicas como dicha organización, la Unión Soviética fortaleció sus capacidades de

inteligencia y espionaje. Organizaciones como el Comisariado del Pueblo para Asuntos Internos de la Unión Soviética (*Народный комиссариат внутренних дел* СССР, NKVD) y el Departamento Central de Inteligencia de las Fuerzas Aradas (*Главное Разведывательное Управление*, GRU) se establecieron y durante los años veinte y treinta Moscú creó escuelas especializadas para formar agentes en técnicas de espionaje, contrainteligencia y propaganda. Estos agentes, una vez capacitados, fueron desplegados en todo el mundo, convirtiéndose en los ojos y oídos del Estado soviético, antes, durante y (especialmente) después de la guerra. Más adelante, el NKVD evolucionaría consolidándose como principal órgano de inteligencia en el Comité para la seguridad del Estado (*Комите́т Госуда́рственной Безопа́сности*, KGB). En este sentido, la Segunda Guerra Mundial, daría paso a la Guerra Fría, un período marcado por la guerra de la información entre los dos grandes bloques.

En lo militar, el manejo de la información influyó de manera decisiva en la victoria soviética en el este. Sería durante dicho período donde la doctrina militar soviética integraría el empleo del engaño a todos los niveles, dando lugar al término de la *maskirovka* como enfoque doctrinal (Keating, 1981), cabe decir, recuperado tras el resurgimiento ruso de la mano de Putin (Staun, 2023).

Durante la extensa época de la Guerra Fría, la URSS se centró en su enfrentamiento con el bloque occidental. Al ser una lucha no solo militar sino también ideológica y política, las tácticas de la URSS abarcaban desde la propaganda hasta la inteligencia encubierta. Las estaciones de radio como Radio Moscú y la Voz de Rusia eran vitales en este sentido, transmitiendo propaganda soviética a audiencias globales en varios idiomas y presentando a menudo el mundo desde una perspectiva prosoviética y antioccidental. En el terreno de las operaciones encubiertas, los servicios de inteligencia soviéticos llevaron a cabo maniobras muy relevantes como la Operación *INFEKTION* en la década de 1980, que difundió el infundado rumor de que el virus del VIH/SIDA había sido una creación del gobierno de Estados Unidos (Bates, 2010). También, patrocinaron revistas como *New Times* y *World Marxist Review* para difundir su perspectiva ideológica. Durante la década de 1980, en medio de tensiones crecientes, la URSS inició campañas de desinformación que retrataban a Estados Unidos como el principal impedimento para la paz mundial, mientras se esforzaban en promover iniciativas de desarme que favorecieran sus propios intereses. Estas operaciones, denominadas en la doctrina del KGB como medidas activas, abarcaban una amplia gama de tácticas destinadas a influir en la política y la opinión pública de otros países. Estas no se limitaron solo a la desinformación. La estrategia soviética fue más amplia, centrada en buscar el cambio en el sistema político. En este sentido la URSS proporcionó financiamiento, armas, entrenamiento y propaganda para apoyar a partidos comunistas y movimientos de liberación en diferentes partes del mundo, colisionando con los EE. UU. (Brantly, 2020).

En este contexto el KGB, se erigió como columna vertebral de estas estrategias, siendo el responsable principal de las operaciones antes detalladas, desarrolló numerosos manuales que se constituyeron en doctrina. Si bien buena parte fueron clasificados como secreto, ejemplos filtrados como *La Ciencia de la Desinformación*

(Bittman, 1985) en la década de 1980, detallaban técnicas y tácticas para operaciones de desinformación. Estas se basaban principalmente en la creación de historias falsas, la utilización de documentos fabricados, la infiltración de medios de comunicación y la cooperación con simpatizantes y agentes en el extranjero (Darczewska, 2015).

Del mismo modo, instituciones especializadas fueron creadas y se encargaron de formar a agentes en estas técnicas, convirtiéndose en expertos en guerra de información. Con el tiempo, la doctrina militar soviética, reflejada en conceptos como la guerra profunda y *maskirovka*[7], subrayó la necesidad de utilizar desinformación y engaño como herramientas cruciales, tanto en el ámbito informativo, como también en el campo de batalla.

Al desintegrarse la URSS en 1991, el KGB dio paso a nuevos servicios de inteligencia en Rusia, como el Servicio Federal de Seguridad de la Federación de Rusia (*Федеральная служба безопасности Российской Федерации,* FSB) y el Servicio de Inteligencia Exterior (*Служба Внешней Разведки*, SVR), continuando con operaciones similares en línea con la política exterior rusa, heredando su enfoque del soviético. Del mismo modo el GRU siguió con sus actividades, responsable de inteligencia militar y operaciones de sabotaje. En la actualidad, estos tres organismos son fundamentales en cuanto al diseño y ejecución de las principales operaciones de guerra de información de Rusia.

La desintegración de la Unión Soviética en 1991 marcó un punto de inflexión en el panorama geopolítico mundial. Rusia, el estado sucesor más grande de la URSS, se vio sumida en una profunda crisis política, económica y social. Esta situación interna tuvo consecuencias directas sobre su presencia y su influencia en los asuntos globales. Durante los años inmediatamente posteriores a la desintegración, Rusia estuvo centrada sobre todo en sus asuntos internos, esforzándose por garantizar una mínima estabilidad en un país que atravesaba transformaciones radicales.

Esta introspección rusa, de alguna manera, dejó en segundo plano a sus operaciones en el ámbito de la guerra de la información. Durante la década de los 90, Rusia enfrentó serias limitaciones financieras que afectaron a muchos sectores, incluido el de esta guerra. Se vio una reducción significativa en el financiamiento y la priorización de este tipo de operaciones, resultando en una virtual parálisis de los esfuerzos en este dominio durante buena parte de esa década. Sin embargo, la entrada en el caos de los 90 no solo repercutió en la capacidad de Rusia para emprender operaciones de guerra de la información, sino que también sentó las bases para una transformación del sistema que más tarde daría lugar a esfuerzos renovados en este ámbito en el nuevo milenio. Es esencial comprender dos aspectos cruciales que surgieron en este contexto.

En primer lugar, el colapso de la URSS generó vacíos de poder en Rusia. Estos, combinados con la emergencia económica y el proceso de privatización acelerada, facilitaron la aparición y consolidación de distintos actores no estatales con gran poder

7 *Maskirovka*: modo de guerra basado en el engaño militar operacional.

e influencia. En este grupo se destacan los conocidos oligarcas, magnates que amasaron enormes fortunas durante este periodo y que, con el tiempo, se convirtieron en actores políticos de primer orden. Aunque estos oligarcas operaban en ocasiones al margen del Estado, poseían significativa capacidad económica y política. Como derivada de su situación comenzaron a mantener un conjunto de intereses que a veces trascendían y hasta han podido llegar a contradecir la política exterior oficial de Rusia.

En segundo lugar, la fragilidad temporal del Estado ruso en esa década dejó una puerta abierta a la influencia extranjera, especialmente en los sectores cultural, político y de telecomunicaciones entre otros. Al respecto de las telecomunicaciones, algunas empresas extranjeras comenzaron a operar para conectar a Rusia a la red global, marcando el inicio de la era de internet en el país. A diferencia de lo que sucedió en naciones como China, donde pronto se establecieron mecanismos de control y regulación de la red, Rusia, en su aspiración a democratizarse y bajo la influencia occidental, no implementó marcos legales ni capacidades técnicas rigurosas para regular las telecomunicaciones hasta mucho más tarde. Esta falta de regulación dio lugar al florecimiento de una comunidad de hackers y comentaristas políticos (Woolley, 2018), que en los años subsiguientes jugarían un papel clave en la evolución de la guerra de la información desde el enfoque ruso.

De igual modo, la fragilidad percibida del recién formado Estado ruso en la década de 1990 no solo expuso al país a la influencia extranjera, sino que también sentó las bases para el surgimiento de nuevos actores políticos. Estos últimos veían en el acercamiento a Occidente una oportunidad para consolidar su posición y éxito político. Este contexto geopolítico propició una serie de movimientos y revueltas en todo el espacio postsoviético más conocidas como las revoluciones de colores en las primeras décadas del siglo XXI. Dichas revoluciones de colores se refieren a una serie de movimientos políticos que tuvieron lugar en varios países postsoviéticos, como Ucrania, Georgia y Kirguistán, donde las protestas masivas y, en su mayoría pacíficas, llevaron a la destitución de gobiernos considerados autoritarios o corruptos y a su reemplazo por regímenes más prooccidentales.

Para las élites rusas, estos movimientos no solo representaban un desafío a su esfera de influencia tradicional, sino que también despertaron profundas preocupaciones sobre posibles interferencias extranjeras y la exportación de revoluciones a la propia Rusia. Este contexto de revoluciones y los cambios geopolíticos que traían consigo, generó un sentimiento de alarma y desconfianza entre las autoridades rusas, quienes interpretaron estas revoluciones como parte de una estrategia de guerra híbrida impulsada por Occidente (Guerasimov, 2013).

Ante este sentimiento general de alarma, la respuesta sistemática de las élites rusas se articuló en torno al blindaje del espacio de información nacional a través, no solo de un refuerzo en la censura y el fortalecimiento de capacidades, sino también a nivel moral e ideológico. Así pues, mediante el establecimiento de un nuevo relato nacional reforzado por la propaganda capaz de unificar ideológicamente al país, este se blindaría en mayor medida contra las distintas campañas de influencia extranjera, cualesquiera que fuesen. Las élites encontraron pues en corrientes como el eurasianismo de

Aleksander Duguin una base ideológica sobre la que construir una narrativa nacional y, por ende, justificar su política exterior o incluso llegar a pugnar por la hegemonía del relato en contra de la democracia liberal. El propio Duguin destacaría el rol de la propaganda y el establecimiento de narrativas nacionales alternativas al atlantismo en una de sus principales obras, *Proyecto Eurasia*, destacaba la necesidad de «establecer un ecosistema de comunicación alternativo al atlantismo dominante» (Duguin, 1999).

Precisamente, las ideas de pensadores como Duguin comenzarían a tomar forma a partir de 2005 mediante el progresivo establecimiento de todo un ecosistema de comunicación internacional ruso. Dicho sistema estaría encabezado por la cadena Rusia Today, establecida ese mismo año junto con otros canales y agencias como Sputnik y, a su vez, estaría respaldado por una amplia red de medios *proxy* vinculados a extremismos de todo tipo, comunicadores alternativos y medios sociales (Galán, 2023). La aplicación de estas nuevas capacidades permitiría al Kremlin comenzar a disputar el relato occidental alrededor del mundo con especial éxito en regiones con corrientes y sentimientos antiimperialista latentes como Iberoamérica (Miles, 2021). Dicha batalla narrativa se iniciaría de forma progresiva con la puesta en marcha de medios como RT y se intensificaría poco a poco tras eventos como el Euromaidán o el propio inicio de la Operación Militar Especial en Ucrania (Darczewska, 2014).

Del mismo modo, este temor, junto con la revolución tecnológica que estaba redefiniendo los medios de comunicación, aceleró el interés de Rusia en desarrollar y consolidar una doctrina propia en el campo de la guerra de la información. Además, sirvió de incentivo para trabajar en capacidades específicas tales como unidades militares en forma de tropas de información o nuevos medios de guerra cibernética y electrónica (Gerasimov, 2016; Lysenko, 2018). Esta transformación nutrida del pensamiento de académicos y militares rusos se tradujo en una serie de directrices y estrategias que fueron incorporadas en la doctrina oficial del Ejército ruso (Rumer, 2019).

Una vez identificada la problemática en el dominio de la información y construidas las primeras capacidades en el sector mediático, las élites rusas procedieron a trasladar este nuevo escenario a una doctrina formal. A medida que avanzaba el siglo XXI, bajo la administración de Vladimir Putin, esta doctrina fue tanto plasmada en diversos documentos estratégicos oficiales como materializada en la construcción y aplicación de capacidades, consolidando así la visión rusa sobre la guerra de la información como respuesta a los desafíos que esta presentaba en el ámbito internacional.

La postura contemporánea de Rusia en la guerra de la información se encuentra arraigada en diversos documentos estratégicos esenciales. La Doctrina Militar de la Federación de Rusia, actualizada en 2014 (Kremlin.ru, 2010, 2014), aunque se centra primordialmente en temas de defensa militar tradicional, destaca la trascendencia de la información y subraya la necesidad de salvaguardar la soberanía informativa del país frente a amenazas externas que buscan desestabilizar su integridad territorial. En 2016, se aprobó la Estrategia de Seguridad de la Información de la Federación de Rusia (рф, 2016), que prioriza la seguridad informativa, identifica amenazas en el ámbito digital y establece un marco para preservar la integridad informativa nacional. Ese mismo año, el Concepto de Política Exterior de la Federación de Rusia enfatizó la necesidad

de emplear herramientas informativas para alcanzar objetivos de política exterior, reconociendo los conflictos que se proyectan en el espacio informacional (*pcф*, 2015-2021) y en su versión de 2023 incide todavía más en la defensa contra la «desinformación y la influencia de actores externos», entendiendo la defensa del espacio informativo interior del país como un elemento central en la seguridad nacional y habilitante de la política exterior (kremlin.ru, 2023). Por otro lado, aunque la Estrategia Nacional de Contraterrorismo de la Federación de Rusia tiene su foco en el terrorismo, no pasa por alto la imperativa lucha contra la propagación de ideologías extremistas en el ámbito informativo.

Este marco doctrinal refleja la concepción rusa de la guerra de la información como un fenómeno multifacético, articulado a través del Ejército, los servicios de inteligencia y los medios oficiales y abarcando dimensiones tanto cognitivas como técnicas (Darczewska, 2015). Ejemplos notorios de esta postura son las acciones rusas que integran técnicas de hackeo, filtraciones, desinformación y propaganda, evidenciadas en eventos como la intervención en Estonia en 2007 (Ottis, 2008; Sanger, 2016) y la supuesta injerencia en las elecciones estadounidenses de 2016. Rusia, reconociéndose como un blanco persistente de esta guerra informativa por parte de Occidente, adopta una postura defensiva que frecuentemente se manifiesta en contraataques, explicando su comportamiento y perspectiva en el escenario global actual.

3.3. La doctrina china

China emerge como actor en la guerra de la información con un desarrollo doctrinal menos sofisticado que el realizado en Estados Unidos, pero con una doctrina informal sólidamente integrada en su pensamiento estratégico y militar. Si bien el valor del control de la información se reconoce desde tiempos antiguos en China, ha sido durante las últimas tres décadas cuando el país ha vivido una revolución doctrinal, en especial después de la guerra del Golfo (Cheng, 2011).

El control y la manipulación de la información han sido fundamentales para las estrategias chinas desde los tiempos de Sun Tzu, como se ilustra en el *Arte de la Guerra*, un tratado que enfatiza la importancia de la estrategia, la inteligencia y la astucia en el combate (Ota, 2014). No obstante, para entender la doctrina moderna de la guerra de la información china, es necesario volver a la segunda mitad del siglo XX y la instauración del comunismo en el país.

Así pues, con la llegada de la revolución comunista de 1949 y la instauración de la República Popular China, la importancia del control informativo se elevó a niveles sin precedentes. En este contexto, la propaganda se convirtió en una herramienta crucial para la promoción y consolidación de la ideología comunista. Sin embargo, debido a las limitaciones tecnológicas y económicas del país en ese momento, la faceta tecnológica de la guerra de la información en China no se desarrolló hasta mucho más tarde. Durante este periodo inicial, se establecieron las bases de la maquinaria

informativa del país, con entidades como la agencia de noticias *Xinhua* y el *Diario del Pueblo* desempeñando roles clave que aún mantienen.

La siguiente etapa crítica en la evolución de la guerra de la información en China fue la Revolución Cultural (1966-1976). Esta década fue testigo de una intensificación de la propaganda, donde su objetivo principal era consolidar el poder del Partido Comunista de China (PCCh) Durante este tiempo, la propaganda no solo era omnipresente, sino también extremadamente política. La movilización masiva y la propaganda alcanzaron niveles desenfrenados, con campañas ideológicas intensas que apuntaban a la eliminación de contrarrevolucionarios y otros enemigos del Estado. Estas campañas se manifestaban en sesiones de estudio, infiltración en todos los sectores de la sociedad, activación de grupos de jóvenes, distribución de material escrito y emisiones de radio (Mittler, 2014). El fin de esta era vino con la ascensión de Deng Xiaoping, quien inició una fase de apertura y reforma en China.

Tras la era de la Revolución Cultural, con la llegada de Deng Xiaoping, China adoptó una postura de apertura al mundo, priorizando su desarrollo económico a través del comercio internacional. Durante esta fase, China moderó sus actividades en la guerra de la información, limitándolas principalmente a la gestión de la información interna para asegurar la estabilidad del régimen, sin mostrarse demasiado ambiciosa en el ámbito internacional. Sin embargo, este periodo también vio el nacimiento de las primeras conceptualizaciones doctrinales sobre la guerra de la información en China. El Dr. Shen Weiguang, en 1985, es reconocido como el padre del concepto en China y definió la guerra de la información como «el intento de ambos bandos de obtener la iniciativa de la batalla a través de su control sobre la información y el flujo de inteligencia» (Weiguang, 1985).

El conflicto de la guerra del Golfo en 1991 sería un punto de inflexión para China. Observando la supremacía de los EE. UU. en el dominio de la información y su capacidad para utilizar armas de precisión e inteligencia contra el adversario, China reconoció la necesidad de invertir y adaptarse. En este período postguerra del Golfo la tecnología y la digitalización comenzaron a desempeñar un papel más prominente en la estrategia china, inspirada en parte por los avances de Estados Unidos (Cheng, 2011). Durante los años 90, figuras militares como el general Wan Pufeng (Pufeng, 1995) y los coroneles Wang Baocun y Li Fei enriquecieron y expandieron la conceptualización china de la guerra de la información (Neilson, 1997). Wang Pufeng lo vinculó con la guerra en red, destacando la relevancia de la tecnología de la información, mientras que Wang Baocun y Li Fei dieron un enfoque más tecnológico, relacionando la guerra de la información con la tecnología de red y la «sensorización» en el campo de batalla.

Liang Zhenxing y el general Yan Banggen, por su parte, propusieron una definición más amplia y holística que abarca no solo el aspecto militar, sino también la lucha más amplia por la supremacía en la adquisición, control y uso de la información en todos los ámbitos de la sociedad (Zhenxing, 1997). De este modo, revolucionó su comprensión y aplicación de la guerra de la información desde sus raíces históricas hasta las concepciones más modernas, integrándola en su política exterior, tanto en lo civil como en lo militar.

En este sentido, la doctrina china de las tres guerras (三战), establecida en el Reglamento de Trabajo Político del Ejército Popular de Liberación en 2003 (PCCh, 2003), es una clara manifestación de cómo el PCCh y el Ejército Popular de Liberación (EPL) siguió conceptualizando y adaptando sus enfoques hacia la guerra en la era de la información. En este contexto, las tres guerras se refieren a:

– Guerra psicológica (心理战)

  Su objetivo es influir y socavar la moral del oponente, ya sea la población en general, la estructura de liderazgo, o las fuerzas armadas. Busca establecer o promover narrativas que favorezcan la posición de China, mientras se socavan las posiciones y perspectivas adversarias.

– Guerra de medios (舆论战)

  Esta guerra se centra en la batalla de las narrativas en el espacio de la información pública, sobre todo a través de medios de comunicación. Su objetivo es dominar el discurso y asegurarse de que la perspectiva china sea la dominante o, al menos, esté ampliamente representada y aceptada.

– Guerra legal (法律战)

  Conocida también como *lawfare*, esta estrategia implica el uso de leyes internacionales y nacionales para lograr objetivos estratégicos. China ha utilizado argumentos legales, por ejemplo, para justificar sus reivindicaciones territoriales en el mar del Sur de China.

Estas tres guerras demuestran cómo China ha conceptualizado el conflicto en el espacio de la información, más allá del campo de la guerra convencional y hacia el ámbito cognitivo, aprovechando todos los mecanismos en el espacio de información a su favor. Este enfoque se ha incrementado progresivamente tras el ascenso de Xi Jinping al poder y el giro de la política exterior china hacia una posición más asertiva en los asuntos internacionales.

En cuanto a su aplicación en la actualidad, la doctrina china de guerra de la información, si bien no queda solo recogida en una serie de documentos oficiales, emana de las distintas publicaciones históricas por parte de su élite intelectual, así como de la Doctrina General de las Fuerzas Armadas y los libros blancos de defensa. Esta, hace hincapié en la búsqueda de la informatización total de sus fuerzas armadas, el desarrollo tecnológico y de ciberfuerzas, así como la aplicación del marco de las tres guerras dentro de un escenario bélico por todos los medios, lo que los coroneles Liang y XIangsui definieron en su visión doctrinal como «guerra sin restricciones» (Liang, 1999; Chew, 2018).

Así, la doctrina de guerra de la información de China ha evolucionado, incorporando una mezcla de elementos prestados de la doctrina estadounidense, así como su herencia soviética con elementos propios históricos como el concepto de guerra popular, la concentración en los puntos débiles o los ataques de engaño y falsa bandera[8] (Charon, 2021).

8 También llamados ataques con espada prestada por Sun Tzu.

Del libro blanco de defensa de China, en su edición de 2015 (China, gov.cn, 2015), se puede apreciar como el Ejército Popular de Liberación (EPL) ha dedicado y se encuentra dedicando recursos muy significativos a la informatización de sus fuerzas. Este proceso no se limita a garantizar el acceso a las operaciones de inteligencia y engaño militar al EPL, sino comprender el control de las entradas y salidas de información en todos los elementos militares como componente crítico para la seguridad nacional. Dicho enfoque quedó confirmado y ampliado en la edición de 2019 de la misma publicación titulada *La Defensa Nacional de China en la Nueva Era* (China, gov.cn). El documento amplió el dominio de la información identificando tres espacios globales de especial interés para su seguridad, el espacio ultraterrestre, el nuclear y el ciberespacio. Incluyendo el ciberespacio como dominio de especial interés, así como el ultraterrestre, el cual depende del manejo de la información, China consolidó su enfoque doctrinal vinculado a la informatización de la guerra.

En el ámbito cibernético del EPL, la ciber guerra es vital para la guerra de la información, enfocándose en acceder y en ocasiones dañar sistemas enemigos. Estas operaciones buscan fortalecer el poder del país, complementar la recopilación de información, mapear redes extranjeras y mejorar capacidades defensivas. A su vez, China mantiene la guerra psicológica, empleando propaganda en la guerra de la información para influir en la opinión pública exterior. Para ello emplea activistas locales vinculados al gobierno para modular la opinión en redes sociales y medios asiáticos. Estos activistas patrióticos[9], alineados con la guerra popular del país, pueden ser empleados para alterar la opinión pública en línea. A su vez, el control del discurso interno protege su retaguardia informativa.

A efectos prácticos, esta consolidación doctrinal se materializó en el establecimiento en 2015 de la Fuerza de apoyo Estratégico (FAE) del EPL, centralizando las misiones espaciales, cibernéticas, de guerra electrónica y de guerra psicológica bajo una sola organización, absorbiendo progresivamente las capacidades del tercer y cuarto departamentos del EPL (Costello, 2018). La puesta en marcha de la FAE fue un hecho de especial relevancia en tanto que materializó la toma de conciencia por parte de las autoridades del PCCh del enorme valor estratégico del dominio de la información y su transversalidad como potenciador o incluso habilitador de operaciones completas en el resto de los dominios convencionales. Del mismo modo, la FAE también serviría como centro de desarrollo de capacidades permitiendo al EPL profesionalizarse en los distintos subdominios en la Guerra de la Información.

Junto con la reestructuración de las fuerzas armadas, el PCCh comenzó a adaptar su arquitectura legal a la guerra de Información moderna. El 1 de julio de 2015 se aprobó la Ley de Seguridad Nacional de la República Popular China (China, ilo.org, 2015), cubriendo una multitud de áreas relacionadas con la seguridad del Estado, pensada para gestionar las amenazas de seguridad en China tanto internas como externas. La

9 Llamado ejército de los cincuenta centavos por analistas occidentales, debido a un supuesto sistema de contraprestaciones a los activistas a cambio de su intervención en las redes sociales. Cabe recalcar, que no existen evidencias claras de este esquema de pagos pero sí de la manipulación política masiva por parte de activistas.

ley, vigente en la actualidad se compone de 84 artículos distribuidos en diez capítulos en los que aborda aspectos variados como la seguridad política, territorial, militar, económica, cultural o la seguridad social y tecnológica. Al respecto de la tecnología, la ley destaca por su especial atención al dominio del ciberespacio. A grandes rasgos subraya la centralidad del liderazgo del PCCh y la necesidad de salvaguardar la estabilidad política en el país, permitiendo tomar medidas enérgicas contra la disidencia política bajo la justificación del concepto de seguridad política.

El enfoque cibernético enfatiza la soberanía cibernética del país, promoviendo el control de internet, censura y vigilancia. El artículo 11 establece que todos en China deben cooperar en la seguridad del Estado según la ley. Aunque es ambiguo, sugiere que deben asistir al Estado si se solicita información o ayuda relacionada con la seguridad nacional, o podrían ser acusados de traición[10]. La Ley de Seguridad Cibernética de 2017 exige que las empresas del sector TIC colaboren con las investigaciones gubernamentales y almacenen datos de usuarios chinos dentro del país.

El siguiente y último paso en la materialización de las capacidades chinas al respecto de la guerra de la información se encuentra en la partición de la FAE en tres nuevas agencias dedicadas, resaltando todavía más la importancia del dominio informativo.

Estas agencias, colocadas directamente bajo la supervisión directa de la Comisión Militar Central del PCCh, incluyen la Fuerza de Apoyo a la Información (heredera directa de la FAE) complementada con la Fuerza de Ciberespacio y la Fuerza Militar Espacial. Cada una de estas nuevas entidades absorbe una de las dimensiones específicas de la guerra de la información, quedando todas ellas coordinadas por la máxima autoridad de las fuerzas armadas del país, Xi Jinping (Singer, 2024).

Así pues, el actual enfoque chino en la guerra de la información se articula a través de dos principales vías, la informatización total de los sistemas militares y la lucha técnica en dicho dominio y el empleo de los medios y sistemas de comunicación para llevar a cabo campañas de influencia global. Para ejecutar dicha estrategia el Partido Comunista chino pone a su servicio todos los mecanismos del Estado en un enfoque sistémico de guerra popular.

3.4. Análisis comparativo

La guerra de la información es un fenómeno transversal, en ella participan todos los Estados, así como un notable número de actores no estatales. Las grandes potencias, debido a su posición y sus intereses en permanente conflicto, aplican este marco de conflicto para obtener ventajas estratégicas sin recurrir a las armas. En la actualidad, los EE. UU., La República Popular China y Rusia son los principales actores en el conflicto, por su desarrollo tecnológico y social, por su tradición política-militar y por sus intereses globales.

10 Mediante los artículos 102,103 y 104 del código penal chino.

En este sentido, Estados Unidos destaca por una sofisticada y estructurada doctrina en cuanto a la defensa que se traslada al ámbito de la guerra de la información. Así, el establecimiento de una doctrina clara y su difusión abierta es en gran medida resultado de su sistema democrático, el cual promueve una comunicación abierta y transparente en cuanto a su política exterior y de defensa. En términos militares su doctrina se encuentra detallada en las *Joint Publications* del Departamento de Defensa, mientras que, a grandes rasgos, las intenciones estratégicas y movimientos del país se ven plasmados en los documentos del Consejo de Seguridad Nacional.

En su aproximación moderna a la guerra, Estados Unidos ha adoptado una estrategia basada en la integración multidominio, posicionando gradualmente a la información como el núcleo central del campo de batalla. Desde una perspectiva cognitiva, ha habido un notable cambio en el enfoque estadounidense: la nación ha evolucionado hacia la STRATCOM, dejando atrás las operaciones psicológicas tradicionales, que ahora son manejadas en secreto por sus servicios de inteligencia.

La influencia global de Estados Unidos se extiende más allá de la fuerza militar. Gracias a su dominante industria audiovisual y cultural y su centralidad en los medios de comunicación occidentales, Estados Unidos ejerce una poderosa influencia —o *soft power*— sobre Occidente y gran parte del mundo. Esta posición es reforzada por programas educativos y de ayuda, lo que les permite evitar conflictos directos en el ámbito digital, reservando dichas tácticas para situaciones muy específicas.

Además, en respuesta a los desafíos planteados por otras grandes potencias en el escenario de la desinformación, Estados Unidos ha invertido considerablemente en iniciativas de alfabetización mediática y en campañas contra la desinformación. Organizaciones como el USAGM y la reciente agencia FMIC, que opera bajo la oficina del director nacional de Inteligencia, son claros ejemplos de estos esfuerzos. Del mismo modo Estados Unidos es reconocido por su notable sofisticación y precisión en las operaciones militares y de inteligencia. Esta destreza es el producto directo de su robusto complejo militar-industrial, una característica que se diferencia de manera drástica del enfoque adoptado por Rusia. La meticulosidad y eficiencia de Estados Unidos en el ámbito militar ha sido evidenciada en operaciones estratégicas de alto calibre como *Olympic Games* (Kamiński, 2020), dirigida contra el programa nuclear iraní y la más reciente *Operation Triangulation* (Kucheryn, 2023), que tuvo como objetivo la interceptación selectiva de comunicaciones en territorio ruso.

No obstante, a pesar de su liderazgo en el dominio de la información, Estados Unidos enfrenta vulnerabilidades considerables en este escenario de conflicto. Una de las principales debilidades radica en la extensa y enmarañada red de servicios de inteligencia y militares del país. Esta infraestructura, densamente burocratizada, a menudo resulta lenta, presentando desafíos en términos de comunicación y coordinación efectiva. De forma paralela, el firme compromiso del sistema democrático estadounidense con la libertad individual y su resistencia natural hacia la censura, aunque virtuoso, puede actuar como un doble filo. El respeto hacia estos principios puede complicar la toma rápida de decisiones y, en ciertas circunstancias, dar ventaja a adversarios que operen con menos restricciones.

A diferencia de Estados Unidos, Rusia no posee un esquema doctrinal amplio y estructurado en relación con la guerra de la información; la información pública al respecto es escasa. Así, partiendo de la escasa documentación oficial, limitada sobre todo a las perspectivas de seguridad nacional emitidas por el gobierno, la estrategia rusa en este ámbito se puede discernir a través de sus acciones concretas en el escenario internacional. En este sentido, Rusia adopta un enfoque de guerrilla. A pesar de carecer de la sofisticación técnica de otras potencias y enfrentarse a un aislamiento internacional, compensa estas debilidades con una estrategia coste-efectiva y extremadamente ágil. Este enfoque tiene sus raíces en la era soviética, caracterizada por técnicas de infiltración y manipulación en los sistemas políticos de naciones objetivo, adaptadas ahora al (nuevo) entorno digital.

La transición tumultuosa de Rusia a la sociedad de la información, tras el colapso de la URSS, influenció mucho su enfoque en la guerra de la información. Mientras el Kremlin y los oligarcas mantienen un control férreo sobre los medios tradicionales, la desregulación de internet ha permitido el surgimiento de una cultura hacker distintiva. Esta cultura, que incluye a blogueros y usuarios activos y politizados, eventualmente evolucionó hacia figuras como los *hackers* patrióticos y los *trolls* profesionales.

Desde la llegada del nuevo milenio, Rusia ha fortalecido tanto sus capacidades en ciberguerra y ciberespionaje como en la manipulación del dominio cognitivo. Su habilidad para integrar operaciones en ambos dominios es evidente, como se vio en los ciberataques a Estonia, los ataques al Comité Nacional Demócrata en Estados Unidos y las incursiones constantes en la infraestructura crítica de Ucrania, todos acompañados de campañas de desinformación y propaganda.

La agilidad de Rusia en estas operaciones se deriva de un enfoque que otorga a las diferentes agencias de inteligencia una gran autonomía, hasta el punto de competir entre ellas. Además, el empleo frecuente de actores no estatales, como el grupo Wagner, permite a Rusia desplegar operaciones rápidas, económicas y escalables a nivel global, aunque esto conlleva sus propios desafíos y problemas asociados.

China se ha consolidado rápidamente como una potencia emergente, posicionándose cerca del liderazgo en la guerra de la información. A partir de finales de los años noventa, las élites intelectuales militares chinas comenzaron a desarrollar su propia doctrina en este ámbito, influidas en gran medida por los acontecimientos de la guerra del Golfo. Esta evolución llevó a China a comprender la importancia crucial del dominio de la información. A diferencia de otras naciones, China no distingue entre los aspectos cibernéticos y psicológicos de la guerra de la información. En su visión, la información es un dominio estratégico en sí mismo.

La doctrina china en esta guerra a su vez ha experimentado una metamorfosis significativa a lo largo de los años. En un principio influenciada por la herencia soviética, que priorizaba la propaganda y la instrumentalización de la ideología comunista, China ha adaptado su enfoque hacia una guerra de la información más integral. Esta adaptación se basa en combinar tecnología, operaciones psicológicas y manipulación mediática internacional. Es digno de nota que, en su evolución, China

tomó inspiración de la doctrina estadounidense, pero la adaptó según su contexto y legado soviético.

Hoy en día, China se esfuerza por una total integración de la información en el contexto bélico. En su perspectiva, toda guerra es, en esencia, una guerra de la información. Este concepto es el pilar de las fuerzas armadas chinas en su proceso de modernización. Además, la guerra de la información en China tiene un enfoque transversal, involucrando a todos los actores de la sociedad. Siguiendo la herencia comunista del país, la guerra popular se mantiene como una estrategia central, siendo el Partido Comunista el máximo responsable en la gestión y dirección de estas operaciones.

A nivel estratégico, la República Popular China ha incorporado la guerra de la información en su doctrina de las tres guerras: mediática, legal y psicológica. Mediante estas, busca ejercer una presión política, diplomática y comunicativa, escalando gradualmente y utilizando todos los recursos disponibles en el espacio informativo. El objetivo primordial es construir un escenario internacional que favorezca la política exterior china. Esto se logra a través de la manipulación mediática, la reinterpretación de las leyes internacionales en su beneficio y tácticas agresivas de manipulación que van desde la intimidación militar (como en el caso de Taiwán) hasta campañas de desinformación y hostigamiento *online*, ejemplificado en tácticas como la diplomacia del lobo guerrero.

Internamente, el Estado chino ha instaurado un control estricto sobre el flujo de información. Este control se materializa a través de varios mecanismos: una constante propaganda orientada a la población, sistemas de vigilancia tecnológica avanzada como el Escudo Dorado y, por supuesto, la omnipresencia del Partido Comunista que monitorea y guía todos los aspectos de la sociedad. De hecho, la guerra de la información en China no es solo una estrategia de las altas esferas gubernamentales; es un enfoque que se entrelaza de forma transversal en toda la sociedad, implicando tanto a individuos como a entidades corporativas.

En este contexto, las empresas estratégicas chinas, que abarcan desde grandes operadoras de telecomunicaciones hasta gigantes de las redes sociales, desempeñan un papel crucial. Según la ley de seguridad nacional, estas compañías pueden ser movilizadas para contribuir a los esfuerzos de guerra de la información del país. Esta integración de las empresas en las estrategias nacionales de información es notablemente más sistemática y estructurada que en países como Rusia. Además, la posición de China como potencia tecnológica y económica global le confiere una sofisticación que supera la aproximación rusa y presenta una agilidad que, en muchos aspectos, desafía incluso a Estados Unidos.

Desde una perspectiva militar, esta doctrina de la guerra de la información ha llevado a reorganizaciones significativas dentro del EPL. Un hito relevante en este proceso fue la creación de la Fuerza de Apoyo Estratégico en 2015 como fuerza de integración y desarrollo para las distintas capacidades de guerra de la información en el país y su posterior expansión hacia tres agencias específicas en los subdominios comunicativo, cibernético y espacial bajo el mando directo de la Comisión Militar Central en 2024.

4. Conclusiones

Desde los albores de la civilización, grupos organizados de todo tipo han buscado la supremacía en el dominio de la información, para garantizar o respaldar su control en el territorio físico. Sin embargo, la verdadera transformación en esta lucha a lo largo de los años se ha dado a través de los avances tecnológicos y sociales, los cuales han redefinido tanto las estrategias como las tácticas, técnicas y procedimientos de los actores implicados. La consolidación de la guerra de la información como un modo de combate relevante se afianza en el siglo XX, en especial con el auge de las TIC en el nuevo milenio. Este enfoque contemporáneo se bifurca en dos dominios: el cognitivo, en el que la propaganda, el engaño y la desinformación son las armas principales y el tecnológico, dominado por la ciberguerra, la guerra electrónica y el ciberespionaje.

Para comprender las complejidades actuales de la guerra de la información, resulta esencial analizarla a través del prisma de las operaciones de las tres grandes potencias: EE. UU., Rusia y China. Cada una de estas potencias aborda este conflicto con un enfoque propio aunque, más allá de su modo de actuar, todas comparten un objetivo común: consolidar y expandir su influencia en el sistema internacional. El realismo ofensivo ofrece una perspectiva clara para entender este fenómeno. En su esencia, las grandes potencias, en su búsqueda de hegemonía, están destinadas al choque y al conflicto. Este choque no se manifiesta solo en enfrentamientos militares convencionales, sino también en la arena de la información. La guerra de la información, por su bajo costo político y su fácil escalabilidad, se convierte en una herramienta primordial, irrenunciable para dichas potencias. La lucha por la influencia política y cultural sobre el sistema internacional se traduce en una batalla constante en el dominio de la información.

Así, en este nuevo escenario global, la guerra de la información no es solo una posibilidad, resulta un fenómeno inevitable. Las grandes potencias, mediante sus vastos recursos y capacidades, se encuentran inmersas en una lucha constante para definir y redefinir la realidad, influir en las percepciones y controlar el flujo de información en un mundo cada vez más conectado.

El dominio de la información se ha convertido, sin lugar a duda, en uno de los principales teatros de conflicto en la política internacional contemporánea. El estudio doctrinal de la guerra de la información a través de las grandes potencias permite una comprensión profunda del fenómeno. Dada su capacidad de innovación y liderazgo en operaciones a gran escala, estas naciones no solo establecen pautas, sino que también influyen en la orientación y posición que toman otras potencias en este ámbito, a menudo generando alianzas y frentes comunes.

A pesar de compartir ciertas similitudes, especialmente en su interés creciente en la competencia en este dominio desde la Segunda Guerra Mundial, las realidades tecnopolíticas de estas potencias las han llevado por rutas distintas. China y Rusia, bajo el paraguas ideológico del comunismo, han adoptado la guerra de la información con un enfoque de influencia política. En particular, Rusia, fortalecida por las tensiones de

la Guerra Fría, invirtió mucho en el sabotaje y manipulación de la información, lo que ha caracterizado su enfoque agresivo, ahora bien, adaptado al ámbito digital.

Por otro lado, Estados Unidos ha adaptado su estrategia de defensa de la democracia utilizando avanzada tecnología, ciberarmas y operaciones en el ciberespacio, respaldando su posición internacional. China a su vez, combinando experiencias de EE. UU. y su herencia soviética, ha creado una estrategia centrada en la información, fusionando esfuerzos civiles y militares bajo el Partido Comunista.

Este panorama actual sugiere una intensificación de la guerra de la información en los años venideros. Las potencias avanzarán en sus doctrinas, buscando una mayor sofisticación e integración. Aunque el poderío militar convencional sigue dominando las dinámicas de conflicto internacionales, la guerra moderna tiende cada vez más hacia la guerra de la información. El objetivo será desestabilizar y romper las capacidades de comando y control del enemigo en todos los niveles, desde influenciar la percepción pública hasta interrumpir sistemas de telecomunicaciones vitales. En definitiva, ya sea en las llanuras de Europa del Este, en la isla de Formosa o incluso dentro de las democracias occidentales, la información será la clave del poder. Su control y manipulación decidirán el resultado de los enfrentamientos, tanto en el ámbito político internacional como en el militar.

Tal como se analiza en este trabajo, la guerra de la información es un fenómeno tan permanente como inevitable. Debido a sus intereses globales, así como la amplitud y complejidad social de sus territorios, las grandes potencias se ven forzadas a injerir en el dominio de la información, sea para coordinar la acción colectiva de sus vastos recursos humanos, para facilitar la cooperación con poblaciones lejanas o para obtener información estratégica. La guerra de la información entre dichas potencias es inevitable, tal como se ha visto en los casos ruso y chino, precisamente al alcanzar (o recuperar) el estatus de gran potencia el país se ve forzado de manera natural a competir en dicho dominio, sea mediante la lucha por el relato o ampliando y sofisticando sus capacidades en materia de inteligencia y sabotaje.

El reconocimiento y el estudio de dicho modo de guerra resulta más que imperativo para líderes y estrategas, tanto en dichos países como en potencias de rango medio y menor entre las cuales, por ejemplo, se encontraría a España. Dichas potencias, por su menor capacidad de influencia, frecuentemente limitada a su entorno geográfico más cercano se ven muy influenciadas, tanto por los desarrollos doctrinales, como por las acciones de las grandes potencias. Al disponer de un peso menor en el sistema internacional, dependiendo de alianzas políticas, económicas y militares dominadas por las grandes potencias, estos Estados pasan a constituirse como campo de batalla donde las grandes potencias luchan por la influencia. Debido a esto, suelen ser víctimas de campañas de espionaje digital o convencional, acciones de influencia, injerencia y maniobras políticas de todo tipo. Este hecho ya puede observarse hoy en regiones de Iberoamérica y, en menor medida, en la Europa Occidental. Incluso potencias tradicionalmente influyentes como Israel, capaces de defenderse de forma técnica y narrativa, se ven a menudo implicadas en las dinámicas de poder de las grandes potencias a través del dominio de la información.

Ante este escenario, resulta imperativo que dichas potencias desarrollen capacidades propias en guerra de la información, en especial aquellas con sistemas basados en la democracia liberal, mucho más vulnerables a la acción desestabilizadora proveniente de potencias con regímenes autocráticos. Por ende, resulta primordial reforzar de manera legal estas capacidades a través de leyes que regulen la actividad de agentes extranjeros, sean servicios de inteligencia o grupos políticos vinculados a poderes extranjeros. La primacía de las leyes de agentes extranjeros tales como la existente en Estados Unidos sobre las recientemente discutidas leyes antidesinformación sitúa el foco en la injerencia extranjera más allá del contenido, garantizando la protección del Estado a la par que el derecho a la libertad de expresión frente a la censura política. Del mismo modo, resulta esencial aumentar las capacidades en contrainteligencia y ciberinteligencia, tanto a nivel humano como a nivel tecnológico, fomentando a su vez una mayor comunicación y transparencia hacia la sociedad para reforzar la confianza en estos organismos tal como ha sido señalado por Maddox *et al.* (2021). En lo militar, se debe reconocer la transversalidad del fenómeno y establecer mecanismos robustos de comunicación en la cadena de mando y, en particular, unidades especializadas, capaces de manejar el ciclo completo de la guerra de la información, integrando tanto capacidades técnicas como capacidades en comunicación. En cuanto a la formación, las academias y centros de pensamiento militares deberían ser capaces de formar a las nuevas generaciones de los cuadros militares en perfiles específicos de este fenómeno, desde la psicología hasta la ciberseguridad. La aplicación de dichas medidas garantizará una defensa más eficiente y adaptada a los desafíos contemporáneos del entorno geopolítico global.

Bibliografía

Aro, J. (2016). The cyberspace war: propaganda and trolling as warfare tools. *European view*. 15, 1, pp. 121-132.

Ateş, A. (2020). The Transformation of Russian Intelligence Community After the Cold War (1991-1993). *Karadeniz Araştırmaları*. 66, pp. 321-332.

Azad, T. M. (2023). Understanding Gray zone warfare from multiple perspectives. *World Affairs*. 186, 1.

Bates, S. (2010). Disinforming the world: Operation INFEKTION. *The Wilson Quarterly*. 34, 2.

Bittman, L. (1985). *The KGB and Soviet disinformation: an insider's view*. Pergamon.

Brantly, A. F. (2020). A brief history of fake: Surveying Russian disinformation from the Russian Empire through the Cold War and to the present. En: Whyte, C. *Information warfare in the age of cyber conflict*.

Bruzesse, M. y Singer, P. (2024). Farewell to China's Strategic Support Force. Let's meet its replacements [en línea]. *Defense One*. [Consulta: 2024].

Charon, P. y Jeangène VIlmer, J. B. (2021). *Chinese influence operations. A Machiavellian moment*. París, Institut de Recherche Stratégique de l'Ecole Militaire.

Cheng, D. (2011). Chinese lessons from the Gulf Wars. En: Scobell, A., Lai, D. y Kamphausen, R. *Chinese lessons from other peoples' wars*. ISBN: 1-58487-511-9

Chew, J. (2018). *How China Applies its «Principles of Unrestricted Warfare» in the 21st Century*. Raportti, Galisteo Consulting Group. Haettu 30.

China, T. S. (s. f.). China's National Defense in the New Era [en línea]. *gov.cn*. [Consulta: 2024].

—. (2015a). China's Military Strategy [en línea]. *The State Council The People's Republic of China*. [Consulta: 2024]. Disponible en: https://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm

—. (2015b). National Security Law of the People's Republic of China [en línea]. *ilo.org*. [Consulta: 2024]. Disponible en: https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=111289&p_lang=en

Concepto de la política exterior de la Federación de Rusia [en línea]. (2023). Министерство иностранных дел Российской Федерации. *kremlin.ru*. [Consulta: 2024].

Costello, J. A. (2018). *China's strategic support force: A force for a new era. Testimony to the U.S.-China Economic and Security Review Commission*. Ministry of National Defense of the People's Republic of China.

Darczewska, J. (2014). *The anatomy of Russian information warfare. The Crimean operation, a case study*. *OSW*.

—. (2015). The devil is in the details. Information warfare in the light of Russia's military doctrine. *OSW*.

Duguin, A. (1999). *Proyecto Eurasia Teoría y Praxis*. Hipérbola Janús.

Evan, M. K. (2022). Moscow's Strategic Culture: Russian Militarism in an Era of Great Power Competition. *Journal of Advanced Military Studies*.13, 1.

Fabian, S. (2019). The Russian hybrid warfare strategy-neither Russian nor strategy. *Defense & Security Analysis*. 35, 3.

Fei, W. B. (1997). Information Warfare. En: Pillsbury, M. *Chinese Views of Future Warfare*. Washington D. C., National Defense University Press.

Galán, C. (2023). El ecosistema de propaganda rusa. *Política exterior*.

Galeotti, M. (2016). Putin's hydra: inside Russia's intelligence services. *European Council on Foreign Relations*.

Gerasimov, V. (2016). Hybrid Warfare Requires High-Tech Weapons and a Scientific Basis. *Military Industrial Courier*.

Gilpin, R. G. (1984). The richness of the tradition of political realism. *International organization*. 38, n.º 2, pp. 287-304

Green, K. R. (2016). People's War in Cyberspace: Using China's Civilian Economy in the Information Domain. *Military Cyber Affairs*.

Guerasimov, V. (2013). The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review*.

Harknett, R. J. (1996). Information warfare and deterrence. *The US Army War College Quarterly*. 26, 3, pp. 93-107.

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

Jincheng, W. (1996). INFORMATION WAR: A NEW FORM OF PEOPLE'S WAR. *Liberation Army Daily*.

Johnson, L. S. (2004). *A Major Intelligence Challenge: Toward a Functional Model of Information Warfare*. CIA: Lessons in Intelligence, p. 392.

Kamiński, M. A. (2020). Operation «Olympic Games». Cyber-sabotage as a tool of American intelligence aimed at counteracting the development of Iran's nuclear programme [en línea]. *Security and Defence Quarterly*. 29. [Consulta: 2024]. DOI: https://doi.org/10.35467/sdq/121974

Keating, K. C. (1981). Maskirovka: The Soviet system of camouflage. *US Army Russian Institute.*

Kucheryn, G. (2023). The outstanding stealth of Operation Triangulation [en línea]. *Securelist*. [Consulta: 2024].

Laswell, H. D. (1948). The structure and function of communication in society. *The Communication of Ideas*.

Liang, Q. A. (1999). *Unrestricted warfare*. Beijing, PLA Literature and Arts Publishing House Arts.

Libicki, M. C. (1995). *What is information warfare?* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University.

—. (2017). The convergence of information warfare. *Strategic Studies Quarterly*. 11, 1.

Lippman, W. (1946). *Public opinion*. Nueva York, Penguin Books.

Liu, M. (2024). The «Gray Zone» Conflicts in China-US Relations: From a Geopolitical Perspective. *International Journal of Education and Humanities*. 12, n.º 1.

Lysenko, V. A. (2018). Russian information troops, disinformation, and democracy. *First Monday*. 23, n.º 5

Maddox, J. D. (2021). Toward a Whole-of-Society Framework for Countering Disinformation. En: *Great Power Cyber Competition*. Londres, Routledge.

Mally, L. (2003). Exporting Soviet culture: The case of Agitprop theater. *Slavic Review*. 62, n.º 2.

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. Nueva York, WW Norton & Company.

—. (2021). The inevitable rivalry: America, China, and the tragedy of great-power politics. *Foreign Affairs*.

MEMBERS OF THE IC [en línea]. (2023). *ODNI*. [Consulta: 2024]. Disponible en: https://www.dni.gov/index.php/what-we-do/members-of-the-ic#:~:text=The%20CIA%20is%20separated%20into,and%20Offices%20of%20the%20Director

Miles, R. (2021). Russia in Latin America. En: *External Powers in Latin America*.

Mittler, B. (2014). *A Continuous Revolution: making sense of Cultural Revolution culture*. Harvard University Asia Center Publications Program.

Neilson, E. (1997). *Sun Tzu and Information Warfare*. National Defense University.

Nye, J. S. (1990). Soft power. *Foreign Policy*. N.º 80.

ODNI. (2023). *National Intelligence Strategy* [en línea]. [Consulta: 2024]. Disponible en: https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf

Ota, F. (2014). Sun Tzu in contemporary Chinese strategy. *Joint Forces Quarterly*. 73, n.º 2.

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *Proceedings of the 7th European Conference on Information Warfare*.

Partido Comunista de China. (2003). The Circular of the CCP Central Committee on Chinese People's Liberation Army Political Work Regulations (中共中央关于颁布《中国人民解放军政治工作条例》的通知). *News of the Communist Party of China*.

Perez, E. V. (2023). El giro Indo-Pacífico de la política exterior de Estados Unidos: una aproximación geopolítica desde el realismo neoclásico. *Revista Del Instituto Español De Estudios Estratégicos*. 20.

Pillsbury, M. (1998). *Chinese views of future warfare*. National Defense University.

Presidente de Rusia. (2014). The President approved new edition of Military Doctrine [en línea]. *Kremlin.ru*. [Consulta: 2024]. Disponible en: http://www.en.kremlin.ru/events/president/news/47334

Pufeng, W. (1995). The Challenge of Information Warfare. *China Military Science*.

Renz, B. (2016). Russia and 'hybrid warfare'. *Contemporary Politics*. 22, n.º 3, pp. 283-300.

Robinson, M. K. (2015). Cyber warfare: Issues and challenges. *Computers & Security*. 49, pp. 70-94.

Robinson, P. (1999). The CNN effect: can the news media drive foreign policy? *Review of International Studies*. 25, n.º 2, pp. 301-309.

Ruiz, M. G. (2018). La viñeta, la nueva Arma durante la I GuerraMundial. *Revista Del Instituto Español De Estudios Estratégicos*. 9.

Rumer, E. (2019). The Primakov (not Gerasimov) doctrine in action. *Carnegie Endowment for International Peace*.

Sampanis, S. E. (2024). Cyberwarfare in the Modern World. Hybrid Threats, Cyberterrorism and Cyberwarfare. *CRC Press*.

Sanger, D. E. (2016). Spy agency consensus grows that Russia hacked DNC. *New York Times*.

Soriano, M. T. (2018). Guerras por Delegación en el Ciberespacio. *Revista Del Instituto Español De Estudios Estratégicos*. 9, pp. 15-36.

Staun, J. A. (2023). Russian influence operations in the wars in Ukraine in 2014 and 2022: active measures and maskirovka. *Política*. 55, n.º 2.

Swiss Institute of Global Affairs. (2023). Chinese Definitions of Information Warfare [en línea]. *globalaffairs.ch*. [Consulta: 2024]. Disponible en: https://www.globalaffairs.ch/2022/06/08/chinese-definitions-of-information-warfare/

The White House. (2022). *National Security Strategy* [en línea]. [Consulta: 2024]. Disponible en: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

USA-JCS. (2022). Joint Publications Operations Series [en línea]. *jcs.mil*. [Consulta: 2024]. Disponible en: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/

Votel, J. L. (2016). Unconventional warfare in the gray zone. *Joint Forces Quarterly*. 80, n.º 1

Waltz, K. (2018). *Man, the state, and war: A theoretical analysis*. Columbia University Press.

Weiguang, S. (1985). *Information warfare*.

Woolley, S. C. (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford, Oxford University Press.

Zhenxing, L. (1997). New military revolution and information warfare. *Zhongguo dianzi bao (china electronic news)*

Военная доктрина Российской Федерации [en línea]. (2010). *Kremlin.ru*. [Consulta: 2024].

рф. (2013). *Концепция внешней политики Российской Федерации* [en línea]. *kremlin.ru* [Consulta: 2024]. Disponible en: http://static.kremlin.ru/media/events/files/41d447a0ce9f5a96bdc3.pdf

рф. (2015-2021). *Национальная стратегия безопасности* [en línea]. *kremlin.ru*. [Consulta: 2024]. Disponible en: http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cERog5tZC.pdf

рф. (2016). *Доктрина информационной безопасности Российской Федерации* [en línea]. *Dirussia.ru* [Consulta: 2024].

РФ, П. (2014). *Военная доктрина российской федерации* [en línea]. *Emsu.ru*. [Consulta: 2024]. Disponible en: http://emsu.ru/extra/pdf5s/lobbyist/2014/6/24.pdf

Панарин, И. (2021). *пропаганда и информационные войны*.

Artículo recibido: 28 de octubre de 2023.
Artículo aceptado: 19 de mayo de 2024.