Facultad de Ciencias Humanas y Sociales
Grado en Relaciones Internacionales

Trabajo Fin de Grado

Ciberguerra desde el Kremlin

Las capacidades cibernéticas rusas como herramienta para mantener su esfera de influencia

Estudiante: **Luis Enrique Blas Barba**

Director: Prof. Alberto Priego

Madrid, junio de 2020

Resumen: El presente trabajo analiza la estrategia militar rusa en el ciberespacio en aras de analizar y entender las motivaciones de Rusia a la hora de implementar ofensivamente sus capacidades cibernéticas. Este estudio presenta la perspectiva mundial de Rusia y las consecuencias directa de esta que son la estrategia defensiva en materia militar y el desarrollo de las capacidades cibernéticas, incluyendo la maquinaria propagandística y la división cibernética del ejército. Se han analizado cuatro ciberataques (Estonia en 2007, Georgia en 2008, Ucrania en 2014 y Lituania de manera intermitente entre 2015 y 2017) para comprender como Rusia aplica su estrategia militar, dictaminada por la Doctrina Gerasimov, y determina el uso de ciertas capacidades o no, discriminando entre guerra híbrida o ciberguerra, dependiendo de la posición internacional del adversario al que se enfrenta.

Palabras clave: Rusia, ciberguerra, ciberataques, desinformación, guerra híbrida, Doctrina Gerasimov.

Abstract: The following paper examines the Russian military strategy in cyberspace in order to analyze the motivations behind Russia's use of offensive cybernetic power. This paper presents the Russian diplomatic perspective, understanding how this leads to a proclaimed defensive military strategy and the development of the Russian cybernetic capacities, including its propagandistic machinery and the army's cyber division. Four main instances of cyberattacks (Estonia in 2007, Georgia in 2008, Ukraine in 2014 and Lithuania intermittently from 2015 to 2017) have been analyzed to understand how Russia applies its strategy, dictated by the Gerasimov Doctrine, and determines the use of different methods, deciding on the use of hybrid warfare or cyberwar, depending on the international position of the adversary it is facing.

Keywords: Russia, cyberwar, cyberattacks, disinformation, hybrid war, Gerasimov Doctrine.

ÍNDICE

ÍNDICE DE SIGLAS

- DDoS – Distributed Denial-of-Service
- FSB – Servicio Federal de Seguridad (*Federal'naya sluzhba bezopasnosti*)
- GRU – Dirección Principal de Inteligencia (*Glavnoe razvedevatel'noe upravlenie*)
- ONU – Organización de las Naciones Unidas
- OTAN – Organización del Tratado del Atlántico Norte
- PSYOP – Operaciones Psicológicas
- RFAF – Fuerzas Armadas de la Federación Rusa (*Russian Federation Armed Forces*)
- RMA – Revolución en Asuntos Militares (*Revolution in Military Affairs*)
- UE – Unión Europea
- URSS – Unión de Repúblicas Socialistas Soviéticas

ÍNDICE DE GRÁFICOS Y TABLAS

1. INTRODUCCIÓN

Históricamente, la guerra ha conocido tres ámbitos: tierra, mar y aire. La introducción de un cuarto ámbito es muy reciente, finales del siglo pasado, donde por primera vez los medios militares tradicionales se subordinaron a un nuevo tipo de guerra, una basada en flujos de información, hardware, software y llevada a cabo en el ciberespacio. Una pregunta recurrente en relaciones internacionales es si este ámbito supone una nueva esfera para el conflicto entre naciones.

El ciberespacio supone un cambio radical en la manera de hacer la guerra, derivando en estrategias donde el impacto sobre la sociedad civil está casi siempre presente. Ciertos estrategas darán más importancia a lo humano, argumentando que todo lo cibernético es simplemente una herramienta a voluntad de los seres humanos. Otros, con afán de ser parte de una película de ciencia ficción, argumentarán que el rápido desarrollo de la tecnología nos está llevando inevitablemente al desarrollo de *Skynet*, o similar. La realidad es que las armas cibernéticas ya son una constante en los conflictos de hoy en día; forman una parte esencial de la estrategia militar de los estados y, dependiendo de como son empleadas, pueden rentabilizarse para inclinar la balanza en un conflicto entre estados a favor de quien mejores capacidades cibernéticas de ataque y/o protección tenga desplegadas firmemente en el campo de batalla.

Tanto es así, que suponen una de las grandes amenazas a la paz mundial, suponiendo un cambio radical sobre la manera actual hacer la guerra. Los ciberataques pueden darse estado contra estado, entre actores privados o incluso actor privado contra estado, en todos los casos con una dificultad inherente para determinar el origen y autor de los ataques; podría ser que no existiera o se reconociera un autor, lo cual supone un riesgo importante. Puede argumentarse el caso más improbable, pero también más taquillero, donde un grupo de adolescentes paralicen el sistema financiero de la potencia número uno mundial desde el desván de su casa.

El ciberespacio en materia de defensa supone enfrentarse a una amenaza invisible, capaz de afectar a las instituciones e infraestructuras públicas y las compañías privadas que sustentan la economía de un estado.

Para la Unión Europea, la cual sigue sin tener una política exterior o de defensa común, la amenaza de un ciberataque es más que real. Las intervenciones de Rusia en elecciones de estados como Reino Unido y Francia o incluso en Estados Unidos hacen peligrar la situación y credibilidad de las democracias de occidente; si el sistema justo que defienden tiene influencia exterior, pierde toda credibilidad. Por ahora, las campañas de desinformación se han dedicado a distribuir y compartir artículos en páginas sensacionalistas que pudieran, de manera

indirecta, afectar los resultados finales y crear una división social, pero esto podría ser solo el comienzo de ataques cada vez más focalizados en la desestabilización social u otros que pudieran afectar al modelo de vida y estructura política de países u organismos multinacionales.

Rusia se ha convertido en el centro de múltiples noticias en materia cibernética y, junto con China, tiende a ser visto como el *villano* de la película. Ha desarrollado técnicas tanto ofensivas como defensivas y probado sus estrategias y métodos en estados colindantes. Rusia es una clara amenaza a la estabilidad de Europa, especialmente del Este, ya que es su vecindario más inmediato y la región donde, históricamente, ha ejercido su influencia y ha considerado su esfera más cercana.

Este artículo tratará estas dos áreas conceptuales, buscando trazar líneas a través de ambas con intención de comprender la conexión entre ellas e intentar responder a las preguntas que se expondrán en la quinta sección. En primer lugar, se tratará el concepto de guerra cibernética (o ciberguerra) y el uso de estas capacidades tecnológicas para mermar, coercer o directamente atacar otros estados y sus infraestructuras. En segundo lugar, se tratará la estrategia militar rusa tanto en materia general como específicamente relacionada al ciberespacio. También, se explorará el concepto de guerra híbrida – la combinación de ataques de manera tanto cibernética como presencial (sea aire, tierra o mar) – y cómo y por qué razones ha empleado la Federación Rusa estas capacidades. Para comprender las motivaciones, objetivos y estrategias rusas, este artículo contemplará cuatro ocasiones donde se han llevado a cabo ciberataques por parte del gobierno ruso: Estonia, Georgia, Ucrania y Lituania.

2. FINALIDAD Y MOTIVOS

Uno de los motivos principales por los cuales este trabajo analizará la situación en materia militar cibernética rusa es la inminente amenaza que esta supone para Occidente, desde un plano tanto social como político. Si bien se avanzado mucho en el tema de ciberguerra y Estados Unidos sigue siendo una potencia mundial en el área, Europa no dispone de una estrategia adecuada ni ha llevado a cabo las inversiones necesarias en programas de defensa en esta materia. De hecho, en todas las ocasiones en que supuestos ataques cibernéticos rusos han impactado en la UE o sus aliados, Europa ha actuado de manera reactiva y nunca proactiva. Entender la estrategia rusa en esta materia es primordial para poder posicionarse adecuadamente ante la amenaza del Kremlin. Además, la ciberguerra[1] se ha convertido rápidamente en uno de los temas de mayor relevancia a nivel internacional. Hay una creciente preocupación por la rápida escalada de armamento cibernético y las consecuencias de esto en el panorama político mundial. El motivo principal, por ende, es pragmático por naturaleza: si es posible entender el planteamiento ruso, la estrategia europea puede ser proactiva y evitar así el posicionamiento de Rusia como líder indiscutible de su región fronteriza.

Otro motivo a destacar de esta investigación es el teórico. Dado que la cuestión de la ciberguerra es relativamente reciente, es imperativo encontrar las metodologías adecuadas para entender la ciberguerra. Llegar a comprender y discernir la importancia de la agencia humana y la tecnológica en materia militar, y, por supuesto, el efecto que tienen las armas cibernéticas sobre aquellos en quien se utilizan, tanto a nivel institucional como social, especialmente en cuanto a desinformación.

Por último, en motivo significativo para esta investigación es entender cómo Rusia utiliza su maquinaria propagandística como herramienta esencial en tiempos de guerra. También entender los resultados que esta tiene sobre poblaciones y gobiernos extranjeros.

[1] Ver estado de la cuestión, sección 3.1, para la definición de ciberguerra.

3. ESTADO DE LA CUESTIÓN

3.1 CONCEPTOS

Como se comentaba, la explotación del ciberespacio por los estados es un tema relativamente reciente en relaciones internacionales. El ciberespacio se presenta como un posible cuarto ámbito donde los estados pueden ejercer fuerza coercitiva e impactar económica, social y/o políticamente a sus rivales. El término ciberguerra origina a finales de la década de los 80 en la revista *Omni* definido como una guerra llevada a cabo con robots y vehículos autónomos (Greenberg A. , 2019), pero esa definición se quedó obsoleta rápidamente, dando paso a otras basadas en lo que ahora se considera ciberespacio – el ámbito artificial creado por medios informáticos. Aunque ha habido una rápida revolución cibernética y un incremento imparable de la literatura sobre el particular, aún no existe una definición de ciberguerra consensuada por los académicos. John Arquilla y David Ronfeldt la van a definir como la ejecución de operaciones militares acorde a principios relacionados con la información; especialmente refiriéndose a la disrupción de sistemas de información y comunicación enemiga (Arquilla & Ronfeldt, 1993). Por otro lado, Jeffrey Carr la define capturando su naturaleza indirecta como "el arte y la ciencia de pelear sin pelear, de derrotar a un enemigo sin derramar su sangre" (Carr, 2011). Este artículo empleará la definición de Scott J. Schakelford:

> "la ciberguerra se refiere, generalmente, al ataque de una nación hostil a los ordenadores o redes de otra nación con el objetivo de causar daños a su infraestructura o una ruptura (o disrupción) de su sociedad o sistemas gubernamentales" (Shackelford, 2013, pág. 94).

Otra cuestión a tener en cuenta es qué se considera un arma en este nuevo tipo de guerra. Rid va a definir las armas cibernéticas como software que se usa, o está designado para usarse, con el objetivo de amenazar o causar daño físico, funcional o mental a estructuras, sistemas o seres vivos (Rid, 2013). Se incluirá también el uso de desinformación como arma social y con el objetivo de plantar dudas sobre el gobierno local u otras entidades.

A pesar de ser un tema relativamente reciente, la ciberguerra ha sido estudiada desde numerosos puntos de vista y ha ganado mucha importancia rápidamente. Think tanks como THIBER, RAND, el German Marshall Fund, Brookings y el Real Instituto Elcano tienen numerosas aportaciones dedicadas al tema. Muchos expertos en la materia provienen de agencias estatales u organizaciones internacionales y contribuyen desde medios de comunicación o las propias publicaciones de sus agencias (ejemplo: Ministerio de Defensa de EEUU). De hecho, Dorothy Denning argumentaba en 1999 que uno de los grandes desafíos

del área de estudio ha sido la dificultad de mantenerse actualizada en cuanto a nuevas tecnologías, métodos de ataque, leyes y nuevos estudios (Denning, 1999). Más de 20 años después, el aluvión de artículos, noticias de prensa y desarrollos es aún mayor.

Un problema de la literatura sobre ciberguerra es que las concepciones epistemológicas no están definidas por los propios autores y no se siguen unos colegios de pensamiento definidos. A pesar de eso, la literatura existente se podría ordenar alrededor de tres escuelas principales: los conservadores, los revolucionarios y los liberal-materialistas (Martin, 2016). Estas tres escuelas intentan contestar a la pregunta: ¿es lo *cibernético* un área sustancialmente diferente como para tener un imperativo cultural que trascienda los dominios del mar, tierra y aire? (Martin, 2016) Para organizar las líneas de argumentación, el teniente-coronel P.E.C. Martin, del ejército canadiense, ubica las tres escuelas en un espectro que comienza en importancia alta de la agencia humana hasta nula humana y alta de la agencia tecnológica,[2] posicionando a los materialistas revolucionarios en el extremo de la agencia tecnológica y los conservadores en el lado opuesto; los materialistas liberales ocuparían el punto intermedio entre ambos (Martin, 2016).

3.1.1 ESCUELA CONSERVADORA

Aquellos que suscriben el pensamiento conservador en ciberguerra son cautelosos con la percepción de los cambios en la sociedad y la aceptación de los avances tecnológicos en la manera en la que se hace la guerra (Martin, 2016). Se basan en pensamientos de académicos militares clásicos como Sun Tzu, Jomeini y Clausewitz y, por ende, tienen un marco de referencia histórico que reduce su análisis a la inducción en cuanto a la evidencia presentada (Martin, 2016). Clausewitz argumentaba que la guerra es un acto basado en la fuerza con el objetivo de imponer la voluntad de uno sobre el enemigo (Tzu, Griffith, & Liddell Hart, 1963). Según esta escuela, la aplicación de la fuerza coercitiva debe seguir tres criterios: uno, el acto es violento; dos, el acto es instrumental; y tres, el acto es político por naturaleza (Rid, 2013). Por ende, un acto puramente cibernético no constituye un acto de guerra para los conservadores. De hecho, consideran que la actividad cibernética se asemeja a la subversión, espionaje y sabotaje, pero nunca a un acto de *guerra per se* (Rid, 2013).

La escuela conservadora romantiza la guerra – un acto violento por naturaleza entre humanos donde la tecnología juega un papel secundario, como mera herramienta. El ciberespacio no es mas que otro instrumento para dañar al rival, pero no constituye un cambio

[2] Ver anexo 1

radical en la manera de hacer la guerra (Martin, 2016). Dado que no hay una amenaza directa a la vida humana, el poder coercitivo en términos emocionales de la fuerza cibernética se ve reducido significativamente (Rid, 2013). Para los conservadores, la guerra, además, no es simplemente el uso de la fuerza en sí, sino también lo es la propia amenaza de ejercerla y la imagen que esta amenaza refleja. Las capacidades cibernéticas de un país no pueden desfilar junto con los tanques y la artillería pesada (Martin, 2016), ni se pueden presentar al lado de un nuevo portaaviones de 13 mil millones de dólares (Cohen, 2018). Para los conservadores, por tanto, la violencia (y la amenaza que conlleva) inducida por *un par de* líneas de código está limitada tanto física como emocional y simbólicamente (Rid, 2013).

Generalmente, los conservadores se muestran reacios a aceptar o contemplar nuevos conceptos que desafíen el dogma de guerra que ellos defienden; entienden los desarrollos tecnológicos como construcciones de manera incremental sobre tecnologías previas (Martin, 2016). Así pues, nunca aceptarían una RMA (Revolución en Asuntos Militares) cibernética y entenderían cualquier cambio en materia de guerra como un simple desarrollo de las tecnologías ya existentes.

3.1.2 ESCUELA MATERIALISTA-REVOLUCIONARIA

Esta escuela representa el lado opuesto a los conservadores, entienden el ciberespacio como un ámbito no solo capaz de ejercer un cambio, sino como naturalmente disruptivo en la manera de hacer guerra. Los revolucionarios contemplan posibles futuros en términos del *peor de los casos* para defenderse de las amenazas del futuro (Martin, 2016). Esta escuela está muy influenciada por visionarios y escritores de ciencia ficción como Isaac Asimov, Arthur C. Clarke, Marshall McLuhan y Gene Roddenberry; además, se enfocan casi exclusivamente en aquellas oportunidades informáticas e impactos de armas de guerra cibernéticas que podrían causar el colapso de la infraestructura crítica de un país y resultar en caos social, un *corralito*, y condiciones socio-económicas que lleven a una parálisis política (Martin, 2016).

El teniente general Rober Elder expresaba parte del pensamiento revolucionario cuando comentaba que, si estás defendiendo en el ciberespacio, ya has llegado demasiado tarde. Si no dominas en el ciberespacio, no puedes vencer en otros dominios. Recibir un ataque cibernético en un país desarrollado supone la paralización del sistema (Clarke & Knake, 2010). Los revolucionarios creen en la posibilidad de un evento de destrucción de la sociedad actual dadas las interdependencias tecnológicas entre industria, finanzas, transporte y comunicaciones

(Martin, 2016). Un evento de este calibre se ha llegado a definir como un Pearl Harbor Electrónico (Schwartz, 2007) o un 11-S Digital (Greenberg K. J., 2012).

Schwartau (1996) presenta la posibilidad de un mundo donde el conocimiento y la información usurpan el poder militar: quien controla la información puede controlar a la gente, la privacidad deja de existir, y, a fin de cuentas, se llega a un mundo donde las bombas y las balas han sido reemplazadas por bits y bytes. Schwartau escribe también que la guerra informacional es sobre el dinero, la adquisición de riqueza y denegación de esta a los rivales; la guerra de información es sobre poder, quien controla la información controla el dinero; la guerra de la información es sobre el miedo, quien controla la información es capaz de instigar el miedo (Schwartau, 1996). Un revolucionario podría llegar a argumentar que la pérdida del control de un individuo sobre su información representa una pérdida potencial del control sobre la noción de su existencia (Martin, 2016).

Esta escuela presenta escenarios casi apocalípticos que podrían ejemplificarse con la idea de *Skynet* en *Terminator*. Hay un claro miedo hacia las crecientes capacidades de los ordenadores y de la inteligencia artificial que guía el debate sobre la aplicación de estás tecnologías con objetivos militares como, por ejemplo, los sistemas autónomos de armas letales (Harris, 2015).

Para los revolucionarios, la ciberguerra supone una nueva era donde el objetivo de la información es encontrar y mantener el dominio de las decisiones (Martin, 2016). Tienen en especial cuenta la maniobrabilidad en el ciberespacio. Arquilla y Ronfeldt, dos de los autores revolucionarios más importantes, explican que la ciberguerra supone una necesidad de repensar la estrategia y doctrina militar actual que será inadecuada en un ambiente de conflicto no linear donde el aspecto que predomina es el uso de *ciberarmas* (Arquilla & Ronfeldt, 2001). Argumentan también que la falta de claridad en la ciberguerra supone una complicación para ejercer la soberanía y autoridad del estado nación (Arquilla & Ronfeldt, 2001).

En resumen, la escuela revolucionaria advoca por una estrategia militar donde prima la maniobrabilidad y enfatiza las ventajas de adoptar enfoques irregulares para atacar las vulnerabilidades del enemigo. Para los revolucionarios, el ciberespacio es la nueva superioridad estratégica desde donde ejercer poder (Martin, 2016).

3.1.3 ESCUELA MATERIALISTA-LIBERAL

La escuela liberal comparte el pensamiento materialista de los revolucionarios en cuanto al énfasis de como el contexto tecnológico actual proporciona nuevas oportunidades al igual que nuevos peligros para individuos, organizaciones y estados (Martin, 2016). Su enfoque, muchos menos sensacionalista, es evolutivo (en vez de revolucionario) donde todavía hay espacio para la actuación del estado. Para los liberales, los desarrollos no son lo nuevo, sino el cambio reflexivo que causan en la interacción entre avances tecnológicos y asuntos humanos (Martin, 2016). Para los liberales hay problemas técnicos inherentes a la propia naturaleza de las tecnologías y a aquellos que la distribuyen; la naturaleza mutable y multifuncional de internet lo convierte en algo innatamente creativo en manos de quien lo usa.

Deibert y Rohozinski explican que al contrario que los otros dominios militares, el ciberespacio es dependiente de la intervención humana para mantenerlo en funcionamiento y, por ende, las acciones de la agencia humana afectan su propia constitución (Deibert, Rohozinski, & Crete-Nishihata, 2012). Los liberales entienden que existe una creciente distribución de poder en el ciberespacio gracias a la privatización de la gobernanza de internet que llega como respuesta estructural a las limitaciones gubernamentales (Martin, 2016). Los liberales presentan una dicotomía ante la ciberguerra: es naturaleza anti-intervención contradicha por la necesidad de políticas y capacidades gubernamentales para proteger a los ciudadanos y fuerzas militares de su dependencia en tecnologías informáticas (Knight, 2013). Para los liberales prima la defensa de las libertades individuales y la propiedad privada ante la amenaza cibernética, ya que entienden, como los revolucionarios, la amenaza que supone estar desprotegido en la red. Knight explica que es imperativo defenderse ante los *ciberadversarios* que posean la financiación, poder humano y acceso comercial para romper con las defensas perimetrales comerciales – refiriéndose a aquellas mediante contratación de software de empresas de ciberseguridad (Knight, 2013).

El estudio de la literatura liberal conlleva tres conclusiones principales. En primer lugar, los liberales aceptan que la tecnología está cambiando el funcionamiento de la sociedad, pero ven estos cambios como una evolución en vez de una revolución; en segundo lugar, existe un debate en el núcleo del pensamiento entre la libertad del individuo y el control estatal; y, en último lugar, se entiende que la escuela liberal es más pragmática y razonable que las dos anteriores siendo que los revolucionarios proponen situaciones casi apocalípticas y los conservadores no acaban de comprender la amenaza cibernética (Martin, 2016).

3.2 EL ROL DEL ESTADO

Desde finales de los 90, cuando la idea de una guerra en el ciberespacio empezaba a verse como una posibilidad muy real, la literatura sobre el estado en el ciberespacio creció rápidamente a base de publicaciones de personal del ejército y funcionarios, especialmente de ministerios de defensa. Desde entonces, la concepción del funcionamiento del control estatal se ha dividido en dos ramas principales: socioeconómica y militar.

Nigel Cory habla de "proteccionismo digital" y "comercio libre digital" como las dos estrategias diferentes al afrontar las posibilidades económicas que brinda el ciberespacio (Cory, 2019). La mayoría de la literatura ubica los dos pensamientos como opuestos, fielmente defendidos por China y Estados Unidos respectivamente. El comercio digital – la transferencia de información y productos/servicios a través de fronteras en la red – no es bienvenido en China, donde la aplicación del Gran Cortafuegos domina el uso de internet y vigila a sus ciudadanos, mientras tanto Estados Unidos potencia el uso libre del ciberespacio y comenta la necesitad de su liberalización (Cory, 2019). Dado que los flujos de información se mueven libremente en la red y los productos digitales no se enfrentan a barreras (Cory, 2019) surgen dos respuestas: la *ciberpaternalista* – que propone mayor regulación – y la *ciberlibertaria* – que aboga por la libertad de expresión (Shackelford, 2013).

Como explica Nicolás de Pedro, experto en campañas de desinformación – la difusión de información falsa de manera deliberada –, el flujo libre de informaciones puede ser una entrada completamente desprotegida y vulnerable para un ciberataque; también comenta que esta es una de las mayores amenazas para las democracias actuales (de Pedro, 2017). Miembros de ministerios de defensa y parte de los ejércitos abogan por el desarrollo de capacidades y estrategias cibernéticas para poder enfrentarse a la posibilidad de ciberataques tanto privados como estatales. Dado que recibir ciberataques es una realidad cada vez más posible y común en muchos estados, hay un entendimiento de que el estado debe tener un rol, aunque sea mínimo, en el ciberespacio, especialmente en materias de protección civil y defensa. (Lohaus, 2017). Entendiendo que es obvia la necesidad de *ciberdefensa*, la complicación de definir el rol del estado proviene del ámbito militar-ofensivo.

3.3 LEGALIDAD

Uno de los problemas de la ciberguerra es la falta de regulación legal internacional – esta es una de las cuestiones propias de relaciones internacionales: la ausencia de autoridad internacional desemboca inevitablemente en anarquía. Se tiende a usar el *ius ad bellum* – los criterios que han de ser consultados para entrar en guerra de manera permisiva – como principal instrumento legal (Martin, 2016). El problema del *ius ad bellum*, y por consecuente el *ius in bello*, en ciberguerra es la dificultad de definir concretamente el autor del ataque que puede derivar en una zona gris legal y estratégicamente (Gady & Austin, 2010).

En términos de guerra híbrida, donde el caso es uno de conflicto armado, la legalidad se ajusta y se aplica el derecho internacional atendiendo, además del *ius ad bellum*, a la Carta de Naciones Unidas, resoluciones de la asamblea general, y el derecho de legítima defensa entre otros (Galán, 2018). En este aspecto, instituciones como el Consejo de Europa, la ONU y la propia OTAN han contribuido a definir las características legales que conllevan las amenazas híbridas, así como la retaliación hacia estas. Carlos Galán extrae las siguientes conclusiones de la literatura existente: en primer lugar, "los adversarios híbridos explotan las lagunas en la ley y la complejidad legal, operan [en] espacios no regulados … y están preparados para cometer violaciones sustanciales de la ley al amparo de la ambigüedad legal y fáctica;" segundo, "niegan sus operaciones hibridas para crear una zona gris legal dentro de la cual pueden operar libremente;" los problemas en cuanto a derechos humanos pueden abordarse con medidas similares al derecho utilizado en materia de terrorismo; "las respuestas de los Estados a las amenazas hibridas deben estar sustentadas en la ley y ser proporcionales;" podrían "imponer[se] algunas restricciones" en cuanto a libertad de expresión "para controlar el contenido de las noticias (especialmente para combatir el discurso de odio), pero no deben ser discriminatorias ni llevar a una censura general; y, por último, "las campañas de desinformación pueden implicar un conflicto entre ciertos derechos humanos y libertades fundamentales" (Galán, 2018).

3.4 ESTRATEGIA MILITAR RUSA

Por último, este estado de la cuestión expondrá la extensión de la literatura en cuanto a la estrategia militar rusa, sus capacidades y las instancias donde atacado a otros estados usando el ciberespacio como medio.

La estrategia rusa ha sido foco de estudio desde la caída de la unión soviética. Guillem Colom en "¿guerra híbrida a la rusa?" presenta como principal estrategia rusa la unión entre medios militares y no militares (Colom, 2018). Uno de los principales focos de atención es la Doctrina Gerasimov y las aportaciones del general en cuanto a materia estratégica y métodos efectivos en conflictos durante el tercer milenio. Nicolás de Pedro también explora la estrategia rusa en materia cibernética, con especial foco en las campañas de desinformación y como los rusos emplean sus capacidades cibernéticas para mermar a sus adversarios desde dentro (de Pedro, 2017). Numerosos expertos como James N. Miller y Sergey Sukhankin han hecho aportaciones en cuanto a la estrategia rusa en materia cibernética y su posicionamiento sobre gobernanza en la red. Además, la literatura informativa en este aspecto es muy extensa, aunque a veces especulativa, con publicaciones en medios de información como el FT, la BBC y el New York Times, entre otros muchos, donde se exploran tanto las instancias donde Rusia ha atacado tanto a rivales menos poderosos (Estonia, Georgia o Ucrania) como los ataques a estados como Alemania y Estados Unidos. Como se explorará en la novena sección, la percepción del funcionamiento de las relaciones internacionales que tiene Rusia influencia directamente su manera de organización y su estrategia tanto defensiva como ofensiva.

En cuanto a las capacidades rusas para ejercer poder coercitivo en la red, nos encontramos con tres complicaciones que expone Marcus Willett: en primer lugar, las capacidades ofensivas en materia digital no suelen ser declaradas, ya que están normalmente diseñadas para crear confusión sin ser detectadas; en segundo lugar, algunos estados, e indudablemente Rusia, subcontratan sus operaciones cibernéticas a actores no estatales (o *proxies*); y, en tercer lugar, las capacidades en términos de *hardware* y *software* de un estado suelen estar compartidas entre gobierno, sector privado y los propios ciudadanos (Willett, 2019). Por ende, para la comprensión de sus capacidades este artículo se basará en la utilización de sus medios (sin conocerlos en detalle) y los efectos de estos sobre sus adversarios.

4. OBJETIVOS

Objetivo principal:

- Entender las razones (el porqué) de la estrategia militar rusa en materia de ciberespacio para posicionar a Rusia como potencia en los estados miembros de la antigua Unión Soviética.

Objetivos secundarios:

- Comprender el nivel de las capacidades cibernéticas rusas y hasta que punto son capaces de infringir daños sustanciales a una nación
- Encontrar la motivación o el origen de la necesidad rusa de tener una presencia masiva en el ciberespacio tanto defensiva como ofensivamente
- Visualizar hacia donde puede evolucionar un conflicto cibernético (y la posibilidad de una carrera armamentística en materia cibernética)
- Entender los efectos que puede tener un conflicto cibernético sobre un país

5. PREGUNTAS

Preguntas clave:

- ¿Cuál es la motivación principal de Rusia en materia de ciberespacio?
- ¿Hasta que punto difiere su estrategia cibernética de una militar tradicional? ¿es una simple herramienta más del ejército o una división independiente con una línea de actuación?
- ¿Cuáles son las razones de Rusia para atacar a Ucrania, Estonia, Georgia y Lituania?
- ¿Cómo y qué efectos ha tenido un ataque de Rusia?

6. HIPÓTESIS

Este artículo argumentará que, ante un mundo sin la Unión Soviética como uno de los pilares políticos globales, Rusia, desde una perspectiva declaradamente defensiva, necesita asegurar su zona de influencia mediante ataques cibernéticos y campañas de desinformación que acompañarán una invasión física (guerra híbrida – la combinación de elementos virtuales y físicos en un conflicto armado) en estados no miembros de la OTAN y utilizando solo la vía cibernética cuando se trata de estados miembros de la OTAN. La variable independiente de esta investigación es la participación de un estado en la OTAN como miembro o no; y la variable dependiente el tipo de ataque por parte de Rusia (ciberataque o guerra híbrida).

7. MARCO TEÓRICO

Esta investigación se orientará bajo el marco de la teoría liberal materialista en términos de ciberguerra. Esta teoría entiende la importancia tanto de la agencia humana como de la agencia tecnológica y evita caer en hipérboles en cualquiera de ellas. Desde el punto de vista de los revolucionarios, la tecnología supone tal cambio en la manera de hacer guerra que el ser humano se convierte en un ente irrelevante en el conflicto. Esto, evidentemente, presupone el final de la guerra como se entiende a día de hoy y, además, conlleva que no hay efecto humano sobre como se conducen los conflictos. Para poder analizar la actuación de Rusia en materia de ciberguerra, se ha de tener en cuenta la perspectiva humana y la percepción global que se tiene desde el Kremlin. La teoría conservadora propone una opción más atractiva: la tecnología se subordina a la actuación humana y es siempre una herramienta de las personas. A pesar de esto, la escuela conservadora comete el error, acorde a la opinión del autor, de subestimar la amenaza cibernética y no considerar el ciberespacio como un cuarto ámbito para la guerra.

Para ello, es necesario atender a la tercera teoría, la más pragmática y la que entiende la tecnología como un elemento evolucionario en la sociedad. Para comprender la actuación de Rusia es necesario entender el ciberespacio como un nuevo ámbito para la guerra y poder estudiar tanto las motivaciones humanas como el desarrollo de un nuevo tipo de guerra, completamente diferente a modos anteriores.

Por otro lado, esta investigación se enfocará en un marco temporal de 10 años entre 2007 y 2017 para englobar los ciberataques a Estonia (2007), Georgia (2008), Ucrania (2014) y Lituania (2015-17) además del desarrollo de la Doctrina Gerasimov (sección 9.2.2). El marco geográfico atenderá también a estos casos de estudio y será, por ende, Europa del Este. Se quiere esclarecer también que este artículo está escrito desde una perspectiva europeísta, viendo, por ende, la situación rusa como una posible amenaza a la seguridad de la región.

8. METODOLOGÍA

Esta investigación requiere el estudio de varios casos mediante el método comparado con cuatro casos donde se estudiará el origen del conflicto, la aplicación de las capacidades cibernéticas rusas y sus métodos de ataque, y los motivos y objetivos que perseguía Rusia en cada uno. Se estudiarán los casos de Estonia, Georgia, Ucrania y Lituania; así, se podrá analizar la estrategia rusa en la antigua región de la URSS y como esta estrategia se ve afectada (o no) cuando un país pertenece a la OTAN.

Este trabajo recurrirá a análisis de expertos, documentos de organizaciones como el Parlamento Europeo y reportes de *Think Tanks* como RAND, y declaraciones del propio gobierno ruso y el ministerio de exteriores para poder comprender la perspectiva global de Rusia. Además, estudiar la estrategia militar rusa requiere el análisis de expertos en la materia como Sukhankin, la comprensión del pensamiento militar a manos de generales del ejército como Gerasimov y el análisis de documentos militares rusos traducidos. Finalmente, para entender los cuatro casos en cuestión, este artículo se basará, además de las aportaciones ya comentadas, en publicaciones de medios de comunicación que reportaron de las incidencias y en posteriores análisis de organizaciones como la OTAN.

En 2007, Estonia recibió ataques cibernéticos donde no se pudo reconocer oficialmente el autor. Aún así, varias direcciones IP desde donde originaron los ataques venían de Moscú. Rusia se negó a colaborar y también negó la participación en los actos. La comunidad internacional, apoyando a Estonia, culparon a Rusia de los ataques que supusieron enormes costes para el gobierno estonio y conllevó la transformación digital del país.

Un año después, Rusia invadiría Georgia bajo el pretexto de estar protegiendo los derechos humanos de las poblaciones de dos regiones clave. Además de la propia invasión física, Rusia llevó a cabo una extensiva campaña de desinformación para debilitar la opinión pública y dividir a la sociedad.

El caso de Ucrania es quizás el más conocido. En 2014, Rusia invadió la península de Crimea, causando una reacción muy negativa de la comunidad internacional, pero sin ninguna consecuencia más allá de sanciones económicas. Antes y durante la invasión, los rusos llevaron a cabo medidas de control reflexivo, como en Georgia, mediante campañas de desinformación además de llevar a cabo ataques cibernéticos hacia infraestructuras.

Por último, el estudio considerará el caso de Lituania donde se han visto afectados durante varios años por ataques cibernéticos similares a las campañas de desinformación y ataques DDoS (Distributed Denial-of-Service) de los casos anteriores.

9. ANÁLISIS Y DISCUSIÓN

Durante la sección de análisis, este artículo tratará la percepción rusa del mundo actual en términos de seguridad y relaciones internaciones y como, a raíz de esta, se ha forjado su estrategia militar durante las primeras dos décadas del siglo XXI. Teniendo en cuenta la estrategia y las capacidades cibernéticas rusas, se explorarán los cuatro casos de ciberataques para así responder a las preguntas establecidas anteriormente.

9.1 PERCEPCIÓN DEL MUNDO 'A LA RUSA'

La percepción rusa del mundo post-Unión Soviética es una donde occidente se ha aprovechado de la disolución de esta para expandir el poder de occidente sobre los estados fronterizos con Rusia (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). El Kremlin entiende que, dada la aparición de un sistema multipolar de relaciones internacionales, las cuales son cada vez más complejas, el mundo actual está cambiando su funcionamiento (The Ministry of Foreign Affairs of the Russian Federation, 2016). Con la inclusión de Hungría, Polonia y la República Checa en la OTAN en 1999 y los países bálticos (Estonia, Letonia y Lituania) en 2004, Moscú percibe una "gran deslealtad" de occidente hacia la estabilidad mundial; desde el Kremlin se cree que la estrategia al incluir los países del este de Europa en la alianza no es más que una maniobra de expansión camuflada como altruismo democrático con el objetivo fragmentar el poder de Rusia (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017), que Sergey Karaganov luego definió como *Versalles con guantes de terciopelo* (Karaganov, 2014). Para Nicolás de Pedro "el gobierno ruso cree que simplemente reacciona y hace probar a [Occidente] su propia medicina" y que tanto Europa como Estados Unidos "forma[n] parte de un gran plan euroatlántico … urdido con el único fin de usurpar el poder en Rusia" (de Pedro, 2017) . Rusia entiende que sus actuaciones son defensivas por naturaleza y mantiene el pensamiento de que un ataque por parte de la OTAN a día de hoy es posible (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017); consideran que el entorno actual está caracterizado por la transformación, competición, complejidad, riesgos y valores confrontados y occidente es el factor desestabilizante (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Para Moscú, la OTAN es causante de una brecha que no solo surge a raíz de diferentes intereses sino también en cuanto a los principios fundamentales que han de mantener el nuevo sistema internacional (The Ministry of Foreign Affairs of the Russian Federation, 2016).

Hasta cierto punto, Rusia quiere que se le considere, llegando casi a demandarlo, una de las grandes potencias mundiales, capaz de establecer las reglas del juego e influenciar la política internacional; quiere, hasta cierto punto, un reconocimiento, sea este implícito o

explícito, de su esfera de influencia (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Para mantener ese *status*, Rusia ha de tener seguridad, estabilidad e influencia (Zakem, Saunders, & Antoun, 2015). En la antigua región URSS, que denominan el *extranjero cercano* (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017), la seguridad se basa en gobiernos afines al Kremlin (Zakem, Saunders, & Antoun, 2015). Además, estos estados tienen un componente clave: su demografía y la presencia de minorías rusas[3]. Para Rusia, la defensa de los 'compatriotas' que viven en el extranjero es una prioridad evidente, incluso llegando a declarar la caída de la Unión Soviética como un desastre geopolítico (Putin, 2014) dados los millones de personas (co-ciudadanos y compatriotas) que se quedaron *atrapados* fuera de su madre patria, Rusia (Zakem, Saunders, & Antoun, 2015).

Acorde a la propia Unión Europea, parece ser que hay un convencimiento general desde el Kremlin, que la propia UE considera preocupante, de que Rusia se está enfrentando a una amenaza existencial (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017), lo cual conlleva que la percepción rusa del mundo sea de uno hostil donde la defensa es esencial para su subsistencia – defensa que se extiende a los estados que son parte de su *esfera de influencia* (Zakem, Saunders, & Antoun, 2015). Esta percepción de la UE y OTAN como organismos hostiles hace imposible la colaboración entre ambos lados; Rusia ha llegado a rechazar la fórmula de 'vecindario compartido' propuesto por la Unión Europea – que buscaba extender las relaciones entre Rusia y la UE hacia los estados colindantes entre ambos como Ucrania, Bielorrusia, y los países Bálticos entre otros (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Esta situación de crisis puede suponer una ventaja para los rusos ya que desde Moscú "se sienten cómodos en contextos de crisis y tienden a interpretarlos en clave de oportunidad" (de Pedro, 2015)

[3] Ver anexo 2

9.2 ESTRATEGIA MILITAR

Rusia ha adoptado una política exterior conservadora y estratégicamente defensiva (Zakem, Saunders, & Antoun, 2015), ejemplo evidente es la militarización gradual de Kaliningrado a medida que crecía la preocupación desde Moscú hacia el nuevo orden mundial (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). La percepción del mundo post-URSS, "la idea central [del gobierno ruso] [de] que las guerras ya no se declaran" y el hecho de que "los elementos virtuales son tan relevantes como los físicos" son factores determinantes de la estrategia militar rusa (de Pedro, 2017). "Los estrategas rusos [han] conceptualizado la llamada *guerra no lineal*" o guerra híbrida – la combinación de elementos virtuales y físicos (de Pedro, 2017) – y, por ende, Rusia utiliza una combinación de tres elementos en sus campañas: acciones directas, acciones indirectas y métodos de control reflexivo[4] (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017).

Para poder mantener la antigua esfera de influencia, proteger los derechos de los rusos en el exterior, y no perder *terreno* ante la OTAN y UE, las RFAF han cambiado su modelo hacia un nuevo concepto operacional que se basa en romper con el modo tradicional de hacer la guerra (Selhorst, 2016). Vasily Kopytko define cinco periodos en estrategia operacional rusa (soviética antes de su disolución): primero de 1920 a 1940, un *modus* operandi centrado en operaciones militares a gran escala y de manera frontal; el segundo periodo hasta 1953 enfatizaba el uso de batalla en tierra, apoyada por una potencia de fuego abrumadora; el tercer periodo, de 1954 a 1985, está definido por las armas nucleares; el cuarto, hasta el año 2000, se enfoca en armas de alta precisión y largas distancias (misiles dirigidos y artillería de precisión); y, el quinto periodo, donde se ubica actualmente la estrategia rusa, marca el cambio hacia dominios no tradicionales y la combinación de medios tanto militares como no militares – guerra híbrida (Selhorst, 2016). Para comprender la estrategia rusa, esta subsección explorará tres áreas clave en materia militar rusa: la creación y funciones de la división cibernética del ejército (9.2.1), la Doctrina Gerasimov (9.2.2) y, por último, las campañas de desinformación rusas (9.2.3).

[4] Ver anexo 3

9.2.1 DIVISIÓN CIBERNÉTICA

Si bien hay documentos – como la doctrina sobre seguridad de información del año 2000 – que indican la existencia de un componente ofensivo en materia cibernética desde principios de siglo (Sukhankin, 2016), el discurso oficial que presenta las *cibertropas* rusas se remonta a 2012 cuando Dmitry Rogozin, antiguo encargado de proyectos e investigación avanzada en materia de defensa, lo menciona públicamente por primera vez (Sukhankin, 2017). Si bien el ejército y gobierno ruso caracterizan las actividades del área cibernética como defensivas, Yaakov Kedmi – antiguo dirigente de Nativ, el servicio de inteligencia Israelí – argumenta que las *cibertropas* existen en todo ejército *medianamente serio* y, subordinados al ministerio de defensa, están encargados a una tarea propagandística y una tarea operacional, las cuales define como actividades diseñadas para distraer a los adversarios proveyendo información falsa – campañas de desinformación (Коммерса́нтъ, 2017). Zecurion Analytics situaba a Rusia, en 2017, dentro del top 5 mundial de *cibertropas*, con un personal estimado de 1000 militares y una inversión anual de alrededor de US$300 millones (Kolomyichenko, 2017), sin tener en cuenta las subcontrataciones a *proxies*. Los primeros ataques cibernéticos de Rusia eran llevados a cabo por actores privados apoyados por Moscú; ahora, el estado ruso se ha coordinado y planificado para que el ciberespacio esté eficazmente gestionado y las acciones llevadas a cabo sean dirigidas por instituciones como el FSB (Servicio Federal de Seguridad) y el propio ministerio de defensa (Sukhankin, 2016). A pesar de eso, muchas de las actividades cibernéticas rusas se hacen a través de agentes privados, o *proxies*, como son dos grupos de *hackers* descubiertos en 2016: *Cozy Bear* y *Fancy Bear* coordinados por el FSB y el ministerio de defensa ruso respectivamente (Turovsky, 2016). Estas dos instituciones han hecho una división eficiente de sus responsabilidades que ha permitido a la rama cibernética del FSB llevar a cabo operaciones ofensivas desde 2008 y continuar obteniendo poderes hasta 2013 cuando comenzaron a ser considerados parte de la infraestructura crítica defensiva del estado (Sukhankin, 2016). Posiblemente, sea esta misma rama la responsable de diseñar los famosos ataques DDoS dadas sus conexiones con distribuidores de red y telefonía rusos (Turovsky, 2015).

Sergei Shoigú, ministro de defensa desde 2012 comentó públicamente la necesidad de crear unidades militares especializadas, de manera análoga a aquellas del *Cibercomando* de Estados Unidos (Turovsky, 2016). En 2013, el ministro anunciaba el comienzo de una caza de talentos en programación dado el volumen de desarrolladores de *software* que iba a necesitar el ejército en un plazo de 5 años (Popsulin, 2013). El propio Vladimir Putin resaltaba la importancia de los ataques basados en tecnologías de la información en un discurso en el

Consejo de Seguridad; Shoigú usaría más tarde las palabras del presidente y añadiría que la amenaza de las armas cibernéticas a día de hoy se acercaba poco a poco a la de "armas de destrucción masiva" (Turovsky, 2016). En 2014, aparecía, oficialmente, en documentos del ministerio de defensa la creación de "tropas de operaciones de información" (Tass, 2014) creadas para la disrupción de las redes de adversarios políticos (Saltykov, 2014), incorporando matemáticos, programadores, criptógrafos e ingenieros de las universidades más importantes del país. Entre las declaraciones de varios estudiantes que acudieron a la academia de entrenamiento y posteriormente se incorporaron a la división del ministerio de defensa destacan algunas en las que comentan haber aprendido métodos de ciberataques, algoritmos tanto de ataque como de defensa, explotación de vulnerabilidades en *software* y seguimiento de cibercriminales entre otras cosas (Turovsky, 2016). La estrategia militar rusa en materia cibernética está en plena expansión, siendo un ejemplo evidente la creación de la *Rosgvardia* – la guardia nacional rusa – que ha adquirido una dimensión aún mayor expandiéndose hacia el ciberespacio para controlar ciberseguridad e inteligencia (Sukhankin, 2017).

Cabe destacar también la función de la GRU (*Glavnoe razvedevatel'noe upravlenie*, o Dirección Principal de Inteligencia) como agencia encargada de dirigir la *informatsionnoe protivoborstvo* – confrontación informacional – y las operaciones psicológicas (PSYOP) que son parte de la estrategia militar rusa (Cheravitch, 2020). Cheravitch indica que la mayor fuerza del aparato de guerra informacional de la GRU es la capacidad de combinar operaciones cibernéticas, electrónicas y psicológicas (2020). A diferencia de otras divisiones cibernéticas o militares del estado ruso, el GRU tiene una visión a largo plazo y se mantiene en la vanguardia de los esfuerzos de Moscú para socavar digitalmente a sus adversarios e influenciar en la red.

9.2.2 LA DOCTRINA GERASIMOV

En febrero de 2014, el general Gerasimov exponía un marco de referencia para el ejército donde se utilizan medios militares y no militares – fuerzas especiales, *proxies*, medios de comunicación y otras capacidades cibernéticas) – para influenciar a los actores del conflicto, interrumpir comunicaciones y desestabilizar regiones (Selhorst, 2016). La doctrina es una reacción doble a un mundo sin Unión Soviética: primero, por la élite política rusa a efectos del papel decreciente de Rusia en su esfera de influencia tradicional (contrastado con la creciente importancia de la OTAN en la zona) y, segundo, por las supuestas preocupaciones de la población rusa a sus *compatriotas* y la marginalización de estos (Selhorst, 2016). Este nuevo concepto operacional se compone de seis fases (figura 1): origen encubierto, escalada, actividades conflictivas, crisis, resolución, y restablecimiento de la paz (Selhorst, 2016). Gerasimov entiende que hay diferentes medidas que se deben llevar a cabo en cada una, por ejemplo, alianzas y coaliciones hasta la tercera fase, acciones militares entre el momento de crisis y la resolución, o sanciones y bloqueos económicos en la escalada. Pero cabe destacar la importancia de la guerra de información: relevante desde la primera hasta la última fase.

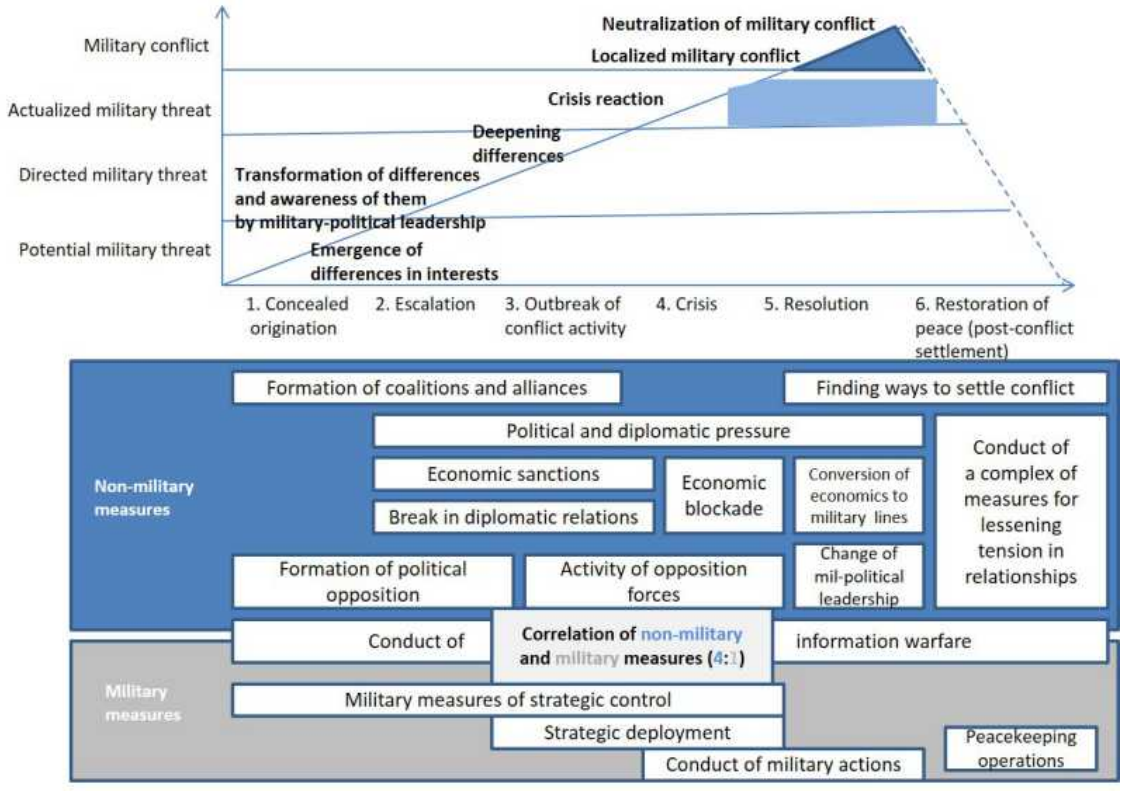


Figura 1. El rol de los métodos no-militares en la resolución de conflictos entre estados (Gerasimov, 2013).

Gerasimov explica que la información, dado que trasciende fronteras, puede servir de base para operaciones encubiertas y remotas, desestabilizando la seguridad interna de un país (Blank, 2020). El sistema central de la doctrina es, por tanto, la guerra de información y, con ella, el 'control reflexivo' – manejo de la percepción – para señalar al liderazgo enemigo y alterar su orientación para beneficio de Rusia (Selhorst, 2016). Los métodos de control reflexivo consideran características psicológicas humanas y se enfocan en influenciar el proceso de toma de decisiones, para generar desde un simple engaño hasta una profunda sugestión[5] (Selhorst, 2016). Gerasimov entiende que la guerra ya no es un conflicto sólo entre estados y se ha convertido en un conflicto con varios participantes y medidas que van desde económicas hasta informacionales (Blank, 2020). El sistema operacional actual, evolución del soviético, añade la aplicación de acciones indirectas y asimétricas por componentes tanto militares como civiles, fuerzas especiales y armas técnicas (Gerasimov, 2013).

La doctrina Gerasimov es una aproximación militar de *sociedad total* – el objetivo pasa a cubrir otros ámbitos de la sociedad, especialmente civil – que supone un cambio en medios usados y dominios donde se lleva a cabo y, a su vez, un desafío a la manera occidental de hacer la guerra dada la falta de familiaridad con sus métodos (Selhorst, 2016). La doctrina busca explotar divisiones sociopolíticas, étnicas o religiosas para proyectar la influencia y poderío ruso donde se desee (Blank, 2020).

Algunos académicos advierten que, en su ensayo, Gerasimov se dedica a detallar, desde un punto de vista puramente militar y no visionario, las acciones que se están llevando a cabo en la actualidad por otros estados, no Rusia (Foy, 2017). Pero la relevancia del estudio del general ruso no es en cuanto a la visión que provee, sea esta original o una mera observación, sino de la aplicación de estos métodos como el modo de hacer la guerra por parte de Rusia.

[5] Ver anexo 3

9.2.3 'DEZINFORMATSIYA'

La desinformación (*desinformatsiya* en ruso) como estrategia militar es una pieza clave del funcionamiento de Rusia, parte integral de su doctrina militar, y lo que las figuras militares más veteranas denominan *un frente de batalla decisivo* (MacFarquhar, 2016). Distribuir información falsa activamente era una de las tácticas centrales soviéticas para influenciar gobiernos extranjeros y a su población, quebrantar las relaciones entre naciones y debilitar a los opositores del comunismo y la URSS (Zakem, 2017). Es una estrategia rápida, barata y con rendimientos muy altos donde actualmente Rusia puede llegar a manejar miles de cuentas falsas y publicar y promocionar artículos falsos diariamente (Zakem, 2017).

Con mucha inversión de fondo, "la maquinaria de propaganda rusa [está] concebida como un arma estratégica, pero con vocación de ser empleada masivamente para socavar, desorientar, agitar, debilitar o paralizar al adversario" (de Pedro, 2017). En la nueva estrategia propagandística, a diferencia de la propaganda tradicional, el diálogo es constante (Gennadievich Evstaf'ev, 2018) y la 'confrontación informacional' les permite usar dicha maquinaria tanto en momentos de paz como de guerra, de manera defensiva u ofensiva, demostrando así la característica permanente de la desinformación como estrategia (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Se utilizan medios convencionales al igual que canales encubiertos para socavar la versión oficial de los hechos y fomentar una parálisis política (MacFarquhar, 2016). Todas las campañas de desinformación tienen una dinámica similar: origen en páginas web rusas (o similares) y propagación de ese documento o artículo cuando se convierte en fuente para una página de noticias de extrema izquierda o extrema derecha (más sensacionalistas que aquellos ubicados en el centro) para acabar extendiéndose a medios tradicionales, de centro, redes sociales, etcétera (MacFarquhar, 2016).

Las campañas de desinformación rusas no tratan de distribuir información falsa o datos erróneos, sino que tratan de construir narrativas, calando en la población con un mensaje clave: "no confíes en nadie" (MacFarquhar, 2016). Dmitry Kiselyev – director de la organización que lleva Sputnik, uno de los medios rusos más importante – comenta que Rusia quiere, a toda costa, ganar toda guerra informacional (MacFarquhar, 2016). Además, comentaba también que el precio tanto de matar como de persuadir a una persona se ha encarecido respecto a situaciones de guerra anteriores (Primera o Segunda Guerra Mundial), pero que, si un gobierno es capaz de persuadir a una persona, no es necesario matarla (Kiselyev, 2016). En otras palabras, el objetivo final de la desinformación es crear narrativas capaces de persuadir tanto a individuos como a grupos para posicionarse en contra de los adversarios políticos de Rusia.

Hay tres consecuencias inevitables de las campañas de desinformación rusa: primero, el hecho de que otros estados o entidades privadas repliquen la manera de actuación rusa en la red; segundo, las inevitables teorías, dudas y difusión de ideas de manera incontrolada en la red (esta es consecuencia directa y, posiblemente, la manera de medir la efectividad de una campaña); y, en tercer lugar, el hecho de que refleja las debilidades de occidente ante la facilidad de crear el caos publicando información falsa, especialmente en referencia a la inhabilidad de la población de hacer frente a esto (Zakem, 2017).

9.3 CIBERATAQUES RUSOS

Considerando la percepción global de Rusia y la estrategia que se sigue desde el Kremlin en materia militar, este artículo pasará a analizar los casos de estudio relevantes para comprender la motivación de Rusia en materia de ciberguerra. Entendiendo la importancia de la región de la antigua Unión Soviética y la amenaza que supone la OTAN para Rusia, la investigación se enfocará en cuatro casos recientes dentro de esa zona geográfica, pero con diferentes relaciones con la OTAN: dos estados miembros y dos en aras de intentar serlo.

9.3.1 ESTONIA 2007

Estonia se independizó después de la caída de la Unión Soviética en 1991 y es miembro de la OTAN desde el 11 de marzo de 2004 (EATA, 2020). Un 25,1% de la población pertenece a minorías de habla rusa de los cuales solo un 7% cree que Rusia supone una amenaza de algún tipo (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Por el contrario, un 80% de los estonios consideran como una amenaza al gobierno ruso (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Hay una clara división social y un sentimiento de desigualdad muy evidente desde el comienzo cuando, poco tiempo después de independizarse, Estonia rechaza el ruso como lenguaje oficial y obliga a los *compatriotas* rusos a renegar su idioma y aprender estonio para poder obtener la nacionalidad (Selhorst, 2016).

El descontento de este cuarto de la población del país va a llevar a una escalada de tensiones entre rusos y el gobierno de Estonia cuando se decide retirar un monumento en memoria de las víctimas rusas de la Segunda Guerra Mundial; el monumento había desarrollado dos simbolismos muy diferentes y se había convertido en un foco de conflicto: para los rusos era una imagen del *liberador* mientras que para los estonios era la imagen del *opresor* (Ottis, 2008). A medida que se acerca el día en el que estaba previsto trasladar la estatua, la minoría rusa comienza a organizar protestas y huelgas (Selhorst, 2016). Viendo el posible daño que puede causar el traslado de la estatua, la propia Rusia denuncia el

comportamiento de Estonia y se dedica a intentar crear una atmósfera de preocupación y hostilidad; comentan las cúpulas dirigentes rusas que se sienten ofendidas por un 'comportamiento inaceptable' del gobierno de Estonia (Socor, 2007).

El 27 de abril, fecha establecida para retirar el monumento, Estonia recibe la primera oleada de ciberataques no-coordinados a las páginas web del presidente, parlamento, policía, partidos políticos y principales medios de comunicación (OTAN, 2018). Los ataques continuaron durante tres semanas afectando a servidores de correo electrónico, proveedores de internet y *routers*, medios de comunicación en línea, empresas locales y páginas gubernamentales entre muchas otras (Ottis, 2008). La segunda oleada de ciberataques comienza el 4 de mayo y cinco días después, el 9 de mayo – celebración de la victoria sobre los nazis en Rusia – el número de ciberataques alcanza su pico (OTAN, 2018). Los ciberataques consiguieron, primero, bloquear los flujos de información atacando a los medios y *webs* similares; segundo, estrangular el sistema financiero y paralizar el acceso y uso de liquidez atacando bancos y otras instituciones financieras: y, en tercer lugar, instigaron el descontento social, ampliando su magnitud, gracias a la comunicación desde cúpulas del estado ruso, incluido Putin, especialmente por el sentimiento social y patriota del 9 de mayo (OTAN, 2018). Como país informatizado y dependiente en tecnología para funcionar, Estonia estuvo a punto del colapso tanto gubernamental como bancario (Melikishvili, 2008).

Cubierta por la dificultad inherente a los ciberataques para identificar a los agresores a través de la red, Rusia no se hizo responsable de estos ataques en ningún momento y tampoco quiso colaborar con Estonia para buscar a los autores de los ataques (Ottis, 2008). Estonia sufrió pérdidas de productividad, enormes costes de oportunidad, elevados costes de remediación y una variada gama de costes informáticos que dejaban la factura de los ataques en varios miles de millones de euros; aún así, la OTAN interpreta que, a pesar de que el ataque ha alterado el orden del país y ha tenido un coste económico elevado, nunca tuvo el objetivo de causar daños a largo plazo, sino que era una demostración de las capacidades de la Federación Rusa, capaz de paralizar un país de manera remota (OTAN, 2018). Era también, inevitablemente, una declaración de intenciones hacia su esfera de influencia.

9.3.2 GEORGIA 2008

A diferencia de Estonia, Georgia cuenta solo con un 1,5% de población étnicamente rusa (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Aún así, es la cercanía geográfica y haber sido parte de la Unión Soviética hasta 1991 que convierten Georgia en un objetivo clave para Rusia. Georgia no es parte de la OTAN, pero está en proceso de formar parte de la alianza. En abril de 2008, tuvo lugar la Cumbre de Bucarest donde se estipuló que Georgia sería miembro de la OTAN en cuanto cumpliera con los requerimientos necesarios (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). El acercamiento de Georgia a la OTAN puede suponer la pérdida de un antiguo estado satélite a occidente que tiene el añadido geográfico de ser un estado intermedio entre Rusia y Oriente Medio.

El conflicto entre Georgia y Rusia surge a raíz de las regiones de Abkhazia y Osetia del Sur que, aunque no tenían una mayoría étnica rusa ni minorías rusas importantes, comparten costumbres y maneras con regiones al norte, las cuales están dentro de Rusia (Selhorst, 2016). La guerra comienza oficialmente el 7 de agosto, cuando el ejército georgiano avanza hacia las regiones y Rusia, gracias al GRU y su máquina propagandística, argumenta la necesidad de intervenir para evitar un genocidio (Selhorst, 2016). El 8 de agosto, mientras los tanques rusos comenzaban a pasar a través del túnel Roki hacia Osetia del Sur, las páginas del gobierno y medios de comunicación georgianos comienzan a fallar y caerse de manera intermitente debido a ataques de DDoS (Melikishvili, 2008). Durante las primeras fases del conflicto, varios *hackers* rusos tumbaron las páginas del presidente de Georgia, el parlamento, el ministerio de defensa y el de asuntos exteriores, el banco nacional y medios de comunicación tanto nacionales como internacionales (Melikishvili, 2008). A diferencia de los anteriores, los ataques en Georgia estuvieron coordinados, utilizando un dominio (www.StopGeorgia.ru) donde se especificaban los objetivos de *hackeo* (Melikishvili, 2008). La máquina de guerra rusa fulminó al ejército georgiano apoyando la avanzada por tierra con medios no tradicionales para poner a los georgianos psicológicamente a la defensiva, desmantelar sus comunicaciones y romper con su posicionamiento estratégico; una vez conseguido esto, hicieron retroceder a los georgianos frenando antes de los oleoductos internacionales para evitar intervención de otros estados (Selhorst, 2016).

Aunque la guerra como enfrentamiento bélico entre ambos estados duró 5 días, el conflicto comienza con las campañas de desinformación en las regiones para asegurarse de que se generaba una percepción positiva de Rusia, obtenía el apoyo de la población local independentista y los *compatriotas* rusos a la vez que se creaba una percepción negativa de Georgia (Selhorst, 2016). A nivel internacional, Rusia dio a entender que las misiones de paz

tenían objetivos similares a las de Kosovo y surgían a raíz de discriminación por parte del gobierno hacia las minorías rusas (Selhorst, 2016). Para convencer a la esfera internacional, Rusia manipuló los resultados de encuestas en medios de comunicación como la CNN, llegando a obtener un 92% de votantes (todos rusos o afines al gobierno ruso) que justificaban la actuación de Rusia en Georgia como una misión de paz (Melikishvili, 2008). La campaña de confrontación informacional por parte del GRU consiguió posicionar una única visión de la información, crear un bloqueo de flujos de datos, desinformar y silenciar eventos inconvenientes para Rusia, escoger deliberadamente a sus testigos y críticos del gobierno georgiano, y crear versiones favorables a Rusia de los ocurrido, denegando daños colaterales entre otras cosas (Selhorst, 2016).

Una vez finalizado el conflicto armado el día 12 de agosto, Rusia reconoció la independencia de ambas regiones y, desde entonces, el conflicto está estancado, con la OTAN defendiendo las regiones como parte del territorio de Georgia y Rusia negando esto (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017).

9.3.3 UCRANIA 2014

Ucrania tiene una minoría rusa importante, más del 15% de la población del país, mucha de la cual se agrupa hacia el este; la defensa de los *compatriotas* y el destino de las comunidades de habla rusa que residen en Ucrania fue uno de los argumentos utilizados por Rusia cuando invadió Crimea en 2014 (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). A pesar de que el conflicto entre ambos estados podría remontarse a la caída de la URSS, realmente comienza en la Revolución naranja de 2003; desde entonces Rusia ha intentado en múltiples ocasiones socavar y menospreciar la soberanía ucraniana (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Históricamente, los rusos perciben a Ucrania como una parte de su región fronteriza, no como a una entidad política y geográficamente independiente, especialmente en referencia a Crimea y Sebastopol – puerto donde Rusia tiene la armada del Mar Negro (Hodgson, Ma, Marcinek, & Schwindt, 2019).

En febrero de 2014, el presidente Yanukovych, presionado por Rusia, abandona unas negociaciones con la Unión Europea, y abandona el cargo para que un nuevo gobierno, afín a occidente, tome riendas del país (Hodgson, Ma, Marcinek, & Schwindt, 2019). Por un lado, Rusia denuncia la entrada de este nuevo directivo, argumentando que no se habían seguido los protocolos establecidos por la ley ucraniana y que se estaba actuando en contra de los *compatriotas* rusos que residen en Ucrania (Selhorst, 2016). Por otro, influenciados por Rusia

y su maquinaria de confrontación informacional, la gente va a salir a las calles en protestas, huelgas y Ucrania va a sufrir una rápida escalada de tensiones que acaba en violencia.

Bajo el pretexto de defensa de los derechos humanos de los *compatriotas*, el ejército ruso invade la península de Crimea; mientras tanto, simpatizantes rusos y fuerzas paramilitares comienzan a tomar el control de instituciones gubernamentales (Hodgson, Ma, Marcinek, & Schwindt, 2019). En paralelo, la operación rusa se dedica a manipular la opinión pública usando métodos no lineares – campañas de desinformación y propaganda. Con un 75% de aprobación de los medios rusos, un 95% de la población de Crimea utilizando medios de comunicación rusos y un 70% de los usuarios de internet de la península usando las dos mayores redes sociales rusas para informarse, el GRU es capaz de posicionarse como líder indiscutible en el área informacional (Selhorst, 2016). Para evitar la intervención de la OTAN y la UE, la confrontación informacional se extiende a occidente con mensajes que demostraban que la OTAN había violado acuerdos con Rusia sobre la expansión hacia el este consiguiendo que, al final, el gobierno ucraniano esté completamente aislado del exterior (Selhorst, 2016).

El ejército ruso (aunque con uniformes sin emblemas ni escudos) y las milicias paramilitares toman control de instalaciones clave y centros de telecomunicaciones y proceden a apagar todas las conexiones móviles e internet (Selhorst, 2016). Valentyn Nalivaichenko – miembro del servicio de seguridad ucraniano – confirmaba que durante varios días los teléfonos de miembros del parlamento estaban siendo atacados y los centros de telecomunicaciones que no estaban bajo control de Rusia recibían ataques DDoS constantes que frenaban su funcionamiento habitual (Daly, 2014). Utilizando la ventaja estratégica que poseían, los rusos aterrizan alrededor de 40.000 tropas en los aeródromos incautados y las movilizan físicamente (Selhorst, 2016).

Durante y después de la invasión de Crimea, el gobierno ruso utilizó varias armas cibernéticas que se extienden desde campañas de desinformación, a ataques DDoS, y *malware* dirigido a sistemas empresariales e institucionales como fueron los troyanos que afectaron infraestructura energética; esta variedad de ataques infligieron mucho daño a Ucrania, paralizando su funcionamiento y arrebatando servicios básicos a la población, como lo es la electricidad durante invierno (Hodgson, Ma, Marcinek, & Schwindt, 2019). La figura 2 a continuación busca mostrar los sectores que utilizó Rusia para ejecutar la invasión de Crimea. Cabe destacar que Galán no comenta que hay indicios de la creación de narrativas favorables al gobierno ruso en Ucrania desde 2008 como la promoción de un referéndum en Crimea (Selhorst, 2016). A pesar de eso, la distribución que muestra Galán podría encajar con las medidas propuestas en la parte inferior del gráfico de la doctrina Gerasimov (figura 1).

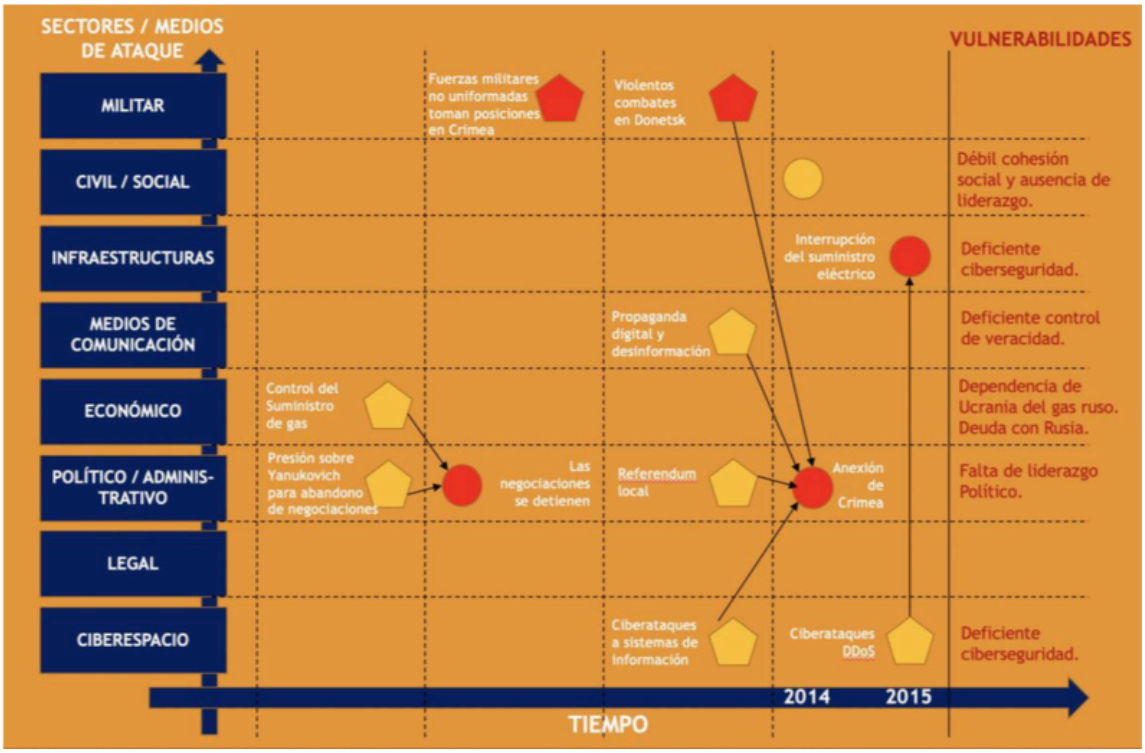


Figura 2. Modelo de ataques híbridos aplicado a Ucrania (Galán, 2018).

La estrategia que se siguió en Ucrania demuestra una intención de establecer una posición de poder empleado una combinación de maniobras militares y no militares para desestabilizar políticamente al adversario y crear rupturas socioeconómicas (Hodgson, Ma, Marcinek, & Schwindt, 2019) y, aunque los rusos no se pronunciaron en cuanto a objetivos ni hicieron demandas al gobierno ucraniano, Galán argumenta que "Rusia toma [estas] medidas para evitar la integración económica y política de Ucrania en la Unión Europea" (2018).

9.3.4 LITUANIA 2015/17

En Lituania un 5.8% de la población es étnicamente rusa, porcentaje significativamente más bajo que Ucrania y Estonia, pero relativamente más alto que Georgia (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Al igual que los casos anteriores se trata de un estado independiente desde 1991, pero en este caso no es colindante con la Rusia continental, aunque sí lo es con el enclave Kaliningrado. De los estados bálticos, Lituania ha sido el más exitoso en la inclusión e integración de la minoría rusa, creando legislación permisiva, otorgando la ciudadanía completa y no ha perseguido una agenda nacionalista (Zakem, Saunders, & Antoun, 2015). Por estas razones, la tensión étnica en Lituania es muy baja y, en general, las minorías se sienten completamente integradas. A pesar de esto, Lituania también ha sido objetivo de

ciberataques por parte de Rusia, especialmente después de la crisis de Crimea (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017) y a razón de la consiguiente crisis económica en la cual esta sumida Rusia (Sukhankin, 2017).

Las operaciones que se han llevado a cabo en Lituania tienen como objetivo general crear una división socioeconómica. En 2015, una campaña de desinformación rusa a través de grupos de Facebook intentaba crear una brecha entre los lituanos y los polacos residentes promocionando la idea de un referéndum en la región de Vilnius de manera similar a las campañas promocionadas en Crimea antes de la invasión (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). Lo más preocupante para el estado báltico quizás sean los movimientos de tropas a Kaliningrado – a fin de cuentas, la frontera este de la UE y la OTAN con Rusia – que llegan acompañados de ataques cibernéticos a departamentos gubernamentales lituanos, descritos por oficiales como ejemplo de una "guerra de información masiva" (Boffey, 2017).

Por otro lado, Rusia ha llevado a cabo varias campañas de desinformación con el objetivo de atraer a ciudadanos a trabajar en el enclave ruso presentando a Lituania, y también Polonia, como estados empobrecidos con peores condiciones que Kaliningrado (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). La desinformación decía que un trabajador del enclave tenía tres veces más poder adquisitivo que el de su contraparte lituana y proveía enlaces y nombres a las páginas de propaganda rusa más notorias como *Sputnik* o *RT* (Sukhankin, 2017). La frecuencia de las campañas desde Kaliningrado ha aumentado considerablemente y la extensión incluye medios de comunicación locales e incluso políticos, como un gobernador lituano de origen ruso que vilificaba a Lituania en repetidas ocasiones y menospreciaba su desarrollo económico (Sukhankin, 2017).

El 20 de febrero de 2017, casualmente coincidiendo con la ratificación del acuerdo de cooperación en defensa con Estados Unidos, Lituania recibió lo que las autoridades consideran el ataque más grave hasta la fecha y llaman 'guerra informacional' por parte de Rusia (de Pedro, Manoli, Sukhankin, & Tsakiris, 2017). En un ataque similar a uno llevado a cabo en Alemania un mes antes, se propagó información sobre una niña que había sido abusada sexualmente pasando por la región donde estaban ubicadas las tropas de la OTAN; además, antes del debate y la firma del tratado, varios legisladores lituanos recibieron correos electrónicos advirtiendo que si ratificaban el acuerdo, perderían su posición en el parlamento (Bankauskaitė, 2017). El incremento de ciberataques podría darse también por la cercanía del *Zapad* – un ejercicio ofensivo ruso donde los militares simulan una invasión báltica (Bankauskaitė, 2017).

9.4 APLICACIÓN DE LA ESTRATEGIA RUSA

Los estudios de caso presentados demuestran el desarrollo y aplicación de una estrategia basada en la combinación de métodos convencionales con los nuevos no-lineares. La figura 3 detalla la estrategia rusa desarrollada durante los ataques a Estonia y Georgia y su aplicación después en Ucrania y Lituania (Selhorst, 2016). La importancia del ámbito cibernético y las campañas de desinformación es evidente, siendo una de las tres piezas clave. Rusia va a comenzar la operación pronto, antes de la escalada de tensión, para situarse como el actor dominante en el ciberespacio y conseguir el dominio absoluto de información.

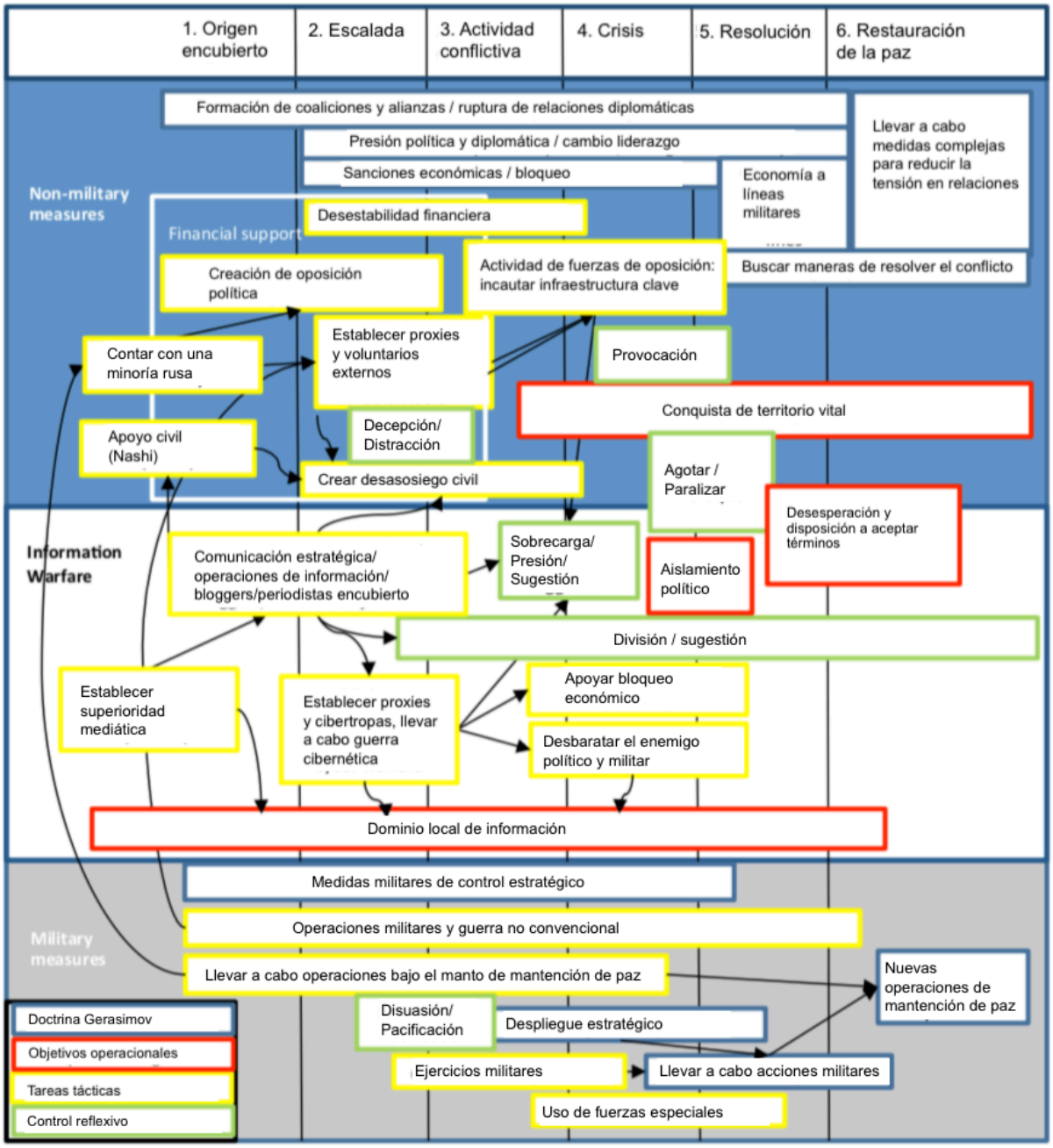


Figura 3. Marco de actuación operacional ruso Fuente: Selhorst, 2016. Traducido por Luis Enrique Blas.

Si bien se hace de diferentes maneras, la aplicación de la doctrina Gerasimov es evidente en los cuatro casos presentados. En los ciberataques rusos hacia los estados de la antigua Unión Soviética, el elemento primordial era el presentado en la franja blanca: la confrontación informacional. Aquí Rusia busca crear división, mantener siempre el dominio absoluto de la información y ejercer presión tanto a sociedad como gobierno para conseguir sus objetivos, desencadenando una resolución donde se acepten términos favorables a Rusia (detener la expansión de occidente y mantener la hegemonía sobre su esfera de influencia). En el caso de Estonia y Lituania, se utiliza un segundo modo de operaciones, presentado en la franja azul: medidas no militares como pueden ser la influencia de las minorías – los *compatriotas* rusos – y desestabilización financiera. Por otro lado, los casos de Georgia y Ucrania presentan una combinación de los tres elementos y, por ende, una guerra híbrida absoluta con elementos tanto tradicionales como no-lineares y cibernéticos

10. CONCLUSIÓN Y RECOMENDACIONES

10.1 CONCLUSIONES DEL ANÁLISIS

La motivación principal de Rusia en materia de ciberespacio es generar un entorno que permita aventajarse respecto a sus adversarios. En muchas ocasiones, esto va a suponer generar una percepción positiva de Rusia mediante campañas de desinformación, otras será generar la discordia y el desasosiego en un estado adversario, y otras, directamente, la destrucción de infraestructura o paralización de la actividad. Pero siempre sirviendo a los objetivos principales de la estrategia militar rusa. Estos objetivos, en cuanto a lo que respecta a este artículo, son dos: en primer lugar, la mantención de Rusia como potencia mundial, para lo cual necesita mantener su esfera de influencia; y, en segundo lugar, frenar la expansión hacia el este de la OTAN y UE. Ambos van de la mano. La consecución de un objetivo es, inevitablemente, un avance del otro. Así pues, la motivación principal del estado ruso en el ciberespacio no difiere de la estrategia general de Rusia, al contrario, es la herramienta esencial para llevarlas a cabo.

Durante el análisis de los casos de estudio, se han podido observar ciertas similitudes y diferencias entre ellos. La similitud más relevante para reforzar el punto anterior es la naturaleza central que tiene la confrontación informacional. Desde la perspectiva rusa, los cuatro casos suponen una defensa de su esfera de influencia y los ataques son reacciones directas, o eso quiere hacer parecer Rusia, a acciones tomadas por Occidente. Rusia va a argumentar que su política militar es completamente defensiva: en Estonia intervino por ofensas a sus *compatriotas*, en Georgia por la expansión premeditada de Occidente dada la cumbre de Bucarest, en Ucrania por el acercamiento a la UE y la defensa de su armada en el Mar Negro, y en Lituania por su aumento de relaciones con Estados Unidos. Rusia defiende sus actuaciones como legítima defensa de sus intereses y su población – considerando especialmente a los *compatriotas* desplazados. A pesar de eso, aunque Rusia habla mucho de defender los intereses de sus compatriotas, realmente se dedica a generar diferencias nocivas y odio entre vecinos, aprovechar la brecha que se abre entre ellos y generar la discordia y desasosiego social con el único objetivo de desestabilizar un régimen afín a occidente, independientemente de si este es beneficioso para los rusos étnicos viviendo allí.

Por otro lado, los casos de estudio también ofrecen una diferencia clave en el modo de actuación del ejército ruso. En estados miembros de la OTAN como son Estonia y Lituania, Rusia empleó métodos puramente cibernéticos, atacando en remoto y sembrando el caos a distancia. En estados en aras de ser miembros de la OTAN, los cuales todavía se pueden considerar parte de la esfera de influencia rusa, pero quieren *escapar*, Rusia no ha empleado

únicamente métodos cibernéticos, sino que ha llevado a cabo guerra híbrida empleando invasiones físicas tanto en Georgia como en Ucrania. La razón más evidente para la utilización de métodos cibernéticos ante miembros de la OTAN es la dificultad de probar realmente quien es el autor de los actos, dificultando la represalia de los aliados. En el caso de miembros fuera de la Alianza, la intervención militar completa no supone una represalia directa y, por ende, no es ningún riesgo añadido. Se podría concluir, por tanto, que Rusia, desde una perspectiva declaradamente defensiva, querrá asegurar su zona de influencia y distinguirá al atacar entre estados miembros de la OTAN, donde llevará a cabo ataques cibernéticos y campañas de desinformación, y estados no miembros de la OTAN donde empleará guerra híbrida.

10.2 VENTAJAS Y LIMITACIONES

Una potencial ventajas de este estudio es que presenta la posibilidad de anticipar futuras acciones de Rusia en materia de defensa nacional. Si, como se argumenta en el artículo, Rusia define su actuación dependiendo del nivel de participación de un estado en la OTAN y, además, utiliza el modelo operacional comentado por Selhorst como desarrollo de la doctrina Gerasimov, sería posible por tanto realizar una estrategia cibernética que permite prever los movimientos del ejército ruso, cuales son los *proxies* bajo su control – en aras de bloquear su intervención – y promover campañas informativas que anulen la actividad de desinformación rusa. Conociendo la percepción rusa del mundo a su alrededor y su concepción del estado inminente de peligro y constante hostilidad, es posible adaptar la diplomacia occidental en el vecindario compartido. Se plantean dos opciones de gestión política por parte de Occidente: 1) el acercamiento a Rusia, debido a sus reticencias que le han abocado a una visión defensiva, con objeto de establecer el vecindario compartido que quería la UE, o 2) un avance diplomático con los países de Europa del Este por parte de la UE, si los objetivos de Rusia fueran coercitivos para los antiguos estados soviéticos en base a la excusa de hostilidad de Occidente.

Otra de las ventajas de este estudio es la reflexión sobre una estratega cibernética efectiva que puede ser empleada no solo por occidente sino por aliados y adversarios por igual. Otros estados, excluyendo posiblemente a China que continua a la vanguardia de la ciberguerra, podrían emular las actitudes de Rusia en materia de ciberespacio para influenciar a sus adversarios. Estar al tanto de esta posibilidad y conocer el funcionamiento de la estrategia puede dar una gran ventaja competitiva a Europa.

Una última ventaja de este estudio sería la posibilidad de utilizar las lecciones aprendidas como fuente para la creación de un escudo protector de la UE. Habiendo recibido

ataques de desinformación durante elecciones presidenciales en países como Francia y Reino Unido, este estudio considera de suma importancia desarrollar una defensa común adecuada, que conste de las medidas necesarias como para cubrir dos áreas esenciales: en primer lugar, un método de defensa proactivo que permita a Europa funcionar sin un miedo constante a un ataque cibernético; y, en segundo lugar, el desarrollo de una política exterior común y de *ciberdefensa* común que permita reaccionar de manera coherente y cohesionada a todos los miembros de la Unión.

Por otro lado, se han de considerar las limitaciones que presenta este estudio. En primer lugar, como se comentaba en el estado de la cuestión, la literatura en materia de ciberguerra está en constante evolución, con la inclusión de nuevos estudios, desarrollos y acontecimientos de manera casi diaria. Por esta razón, este estudio se ha atenido a la mayor cantidad de información posible que existe actualmente, pero existe una posibilidad razonable para que lo expuesto durante este artículo quede obsoleto en poco tiempo y nuevos estudios aclaren o evolucionen aspectos no recogidos en este estudio.

Hay que añadir como segundo aspecto, además del avance de la propia literatura, el propio avance de la tecnología en la materia: como por ejemplo métodos de ciberguerra basados en nuevos desarrollos de *software*, y *hardware*, nuevas redes sociales, medios de comunicación, tecnología 5G, y un largo etcétera que es imposible de concebir a día de hoy. El desarrollo de nuevas tecnologías supone una evidente evolución del funcionamiento de la sociedad y, por ende, un cambio relevante también en materia de ciberguerra que cambiaría el paradigma actual.

Finalmente debemos considerar la propia limitación de información procedente de los organismos gubernamentales rusos y de su ejército. Esta consideración no solo se refiere a las fuentes de origen ruso como el Kommersant u otros medios sino también a la inevitable necesidad de confiar en esa información por parte de otros académicos para desarrollar sus reportes y artículos. Dada la falta de transparencia por parte de Rusia, las consideraciones de este estudio en materia de capacidades y percepción podrían no estar bien fundamentadas.

10.3 VÍAS DE INVESTIGACIÓN Y POLÍTICAS PARA EL FUTURO

Posiblemente, una de las vías de investigación mas relevantes en esta materia sea la instalación de tecnología 5G alrededor de Europa y como esto puede suponer un nuevo objetivo para Rusia y la necesidad de una defensa fuerte por parte de Europa. Otro aspecto a considerar como vía de investigación, no revisada en este estudio, es la RuNet 2020 – la idea de Rusia de desarrollar un internet propio, que podría extenderse a los estados colindantes.

Una de las vías principales a futuro debería ser el desarrollo de políticas en materia de defensa del ciberespacio. Si bien es necesario para la gran mayoría de estados en la actualidad desarrollar una política para defenderse en el ciberespacio, lo es más aún para un país desarrollado donde la tecnología es parte central de su funcionamiento. La amenaza cibernética supone enfrentarse a un enemigo invisible, capaz de afectar a las instituciones e infraestructuras públicas como y las compañías privadas que sustentan la economía de un estado. Para la Unión Europea, la amenaza de un ciberataque es más que real debido a la cercanía con Rusia y la posición de esta. Ataques como intervenciones rusas en elecciones y campañas de desinformación que podrían hacer peligrar la credibilidad y estabilidad de las democracias europeas, y por tanto afectan a la propia estabilidad del orden mundial.

11. BIBLIOGRAFÍA

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar Is Coming! En J. Arquilla, & D. Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age.*

Arquilla, J., & Ronfeldt, D. (2001). The Advent of Netwar (Revisited). En J. Arquilla, & D. Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy.* Santa Monica: RAND Corporation.

Bankauskaitė, D. (20 de February de 2017). *A CURIOUS FAKE: LITHUANIA ENCOUNTERS AN ECHO FROM THE "LISA CASE"*. Obtenido de CEPA: http://infowar.cepa.org/Briefs/Lt_20_Feb17

Blank, S. (2020). *A Russian Global Expeditionary Force?* Washington D.C.: Center for Strategic and International Studies.

Boffey, D. (24 de August de 2017). *'We know how to live next to Russia': Lithuania builds border fence with Kaliningrad*. Obtenido de The Guardian: https://www.theguardian.com/world/2017/aug/24/russia-lithuania-border-fence-kaliningrad-estonia-eston-kohver

Carr, J. (2011). *Inside Cyber Warfare: Mapping the Cyber Underworld.* O'Reilly Media, Inc.

Cheravitch, J. (2020). *From Leaflets to "Likes": The Digitalization and Rising Prominence of Psychological Operations in Russia's Military.* Washington D.C.: Center for Strategic and International Studies.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What To Do About It.* New York: Ecco.

Cohen, Z. (15 de May de 2018). *US Navy's most expensive warship got even pricier*. Obtenido de CNN: https://edition.cnn.com/2018/05/15/politics/uss-gerald-ford-aircraft-carrier-cost-increase/index.html

Colom, G. (2018). *¿Guerra híbrida a la rusa?* Madrid: THIBER.

Cory, N. (2019). *China and the United States: Digital Protectionism vs. Digital Free Trade.* Washington D.C.: Center for Strategic and International Studies.

Daly, J. C. (20 de March de 2014). *Ukrainian-Russian Dispute Moves Into Cyberspace*. Obtenido de The Jamestown Foundation: https://jamestown.org/program/ukrainian-russian-dispute-moves-into-cyberspace/

de Pedro, N. (Septiembre de 2015). *RUSIA EN SIRIA: ¿la vista puesta en Ucrania y Europa?* Barcelona: CIBOD.

de Pedro, N. (19 de Noviembre de 2017). *Rusia se apunta a la guerra híbrida*. Obtenido de El País: https://elpais.com/elpais/2017/11/18/opinion/1511025644_093966.html

de Pedro, N., Manoli, P., Sukhankin, S., & Tsakiris, T. (2017). *Facing Russia's strategic challenge: Security developments from the Baltic to the Black Sea.* Brussels: European Parliament.

Deibert, R. J., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war.

Denning, D. E. (1999). *Information Warfare and Security.* Reading: Addison-Wesley.

EATA. (2020). *Estonia in NATO*. Obtenido de Estonian Atlantic Treaty Association: https://www.eata.ee/en/nato-2/estonia-in-nato/

Foy, H. (15 de September de 2017). *Valery Gerasimov, the general with a doctrine for Russia*. Obtenido de Financial Times: https://www.ft.com/content/7e14a438-989b-11e7-a652-cde3f882dd7b

Gady, F.-S., & Austin, G. (2010). *Russia, The United States, and Cyber Diplomacy.* EastWest Institute.

Galán, C. (2018). *Amenazas híbridas: nuevas herramientas para viejas aspiraciones.* Madrid: Real Instituto elCano.

Gennadievich Evstaf'ev, D. (23 de August de 2018). Transformatsiya informatsionnykh voyn: ot klassicheskoy propagandy k informatsionno-sotsial'noy dekonstruktsii na baze integrirovannykh kommunikatsiy. *Konferentsiya 'psikhologicheskaya oborona'*.

Gerasimov, V. (26 de February de 2013). *Ценность науки в предвидении*. Obtenido de VPK News: https://www.vpk-news.ru/articles/14632

Greenberg, A. (22 de August de 2019). *The WIRED Guide to Cyberwar*. Obtenido de WIRED: https://www.wired.com/story/cyberwar-guide/

Greenberg, K. J. (21 de October de 2012). *Tomgram: Karen Greenberg, Preparing for a Digital 9/11*. Obtenido de TomDispatch: http://www.tomdispatch.com/blog/175607/

Harris, K. (9 de April de 2015). *'KillerRobots' Pose Risks and Advantages for Military Use*. Obtenido de CBC: http://www.cbc.ca/news/politics/killer-robots-pose-risks-and-advantages-for-military-use-1.3026963

Hodgson, Q. E., Ma, L., Marcinek, K., & Schwindt, K. (2019). *Fighting Shadows in the Dark.* Santa Monica: RAND Corporation.

Isserson, G. S. (2005). *The evolution of operational Art.* Fort Leavenworth: SAMS Theoretical .

Коммерса́нтъ. (22 de 2 de 2017). *В России созданы войска информационных операций*. Obtenido de Коммерса́нтъ: https://www.kommersant.ru/doc/3226925

Karaganov, S. (April/June de 2014). *EUROPE AND RUSSIA: PREVENTING A NEW COLD WAR*. Obtenido de Russia in Global Affairs: https://eng.globalaffairs.ru/articles/europe-and-russia-preventing-a-new-cold-war/

Kiselyev, D. (7 de June de 2016). Киселев: я не пользуюсь словом "пропаганда". (P. 24, Entrevistador)

Knight, S. (2013). War by Computer: Canadian Cyber Forces in 2025. En J. Granatstein, *The Canadian Forces in 2025 Prospects and Problems.* FriesenPress.

Kolomyichenko, M. (1 de 10 de 2017). *В интернет ввели кибервойска*. Obtenido de Коммерса́нтъ: https://www.kommersant.ru/doc/3187320

Lohaus, P. (11 de August de 2017). *From cybersecurity to information warfare*. Obtenido de AEI: https://www.aei.org/articles/from-cybersecurity-to-information-warfare/

MacFarquhar, N. (28 de August de 2016). *A Powerful Russian Weapon: The Spread of False Stories*. Obtenido de The New York Times: https://www.nytimes.com/2016/08/29/world/europe/russia-sweden-disinformation.html

Martin, L.-C. P. (2016). Cyber Warfare Schools of Thought: Bridging the Epistemological/Ontological Divide, Part 1. *Royal Canadian Air Force Journal, 5*(3).

Martin, L.-C. P. (2016). Cyber Warfare Schools of Through: Bridging the Epistemological/Ontological Divide, Part 2. *Royal Canadian Airforce Journal*.

Melikishvili, A. (12 de September de 2008). *THE CYBER DIMENSION OF RUSSIA'S ATTACK ON GEORGIA*. Obtenido de The Jamestown Foundation: https://jamestown.org/program/the-cyber-dimension-of-russias-attack-on-georgia/

OTAN. (2018). *2007 cyber attacks on Estonia.* Riga: NATO Strategic Communications Centre of Excellence.

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallin: Cooperative Cyber Defence Centre of Excellence.

Popsulin, S. (7 de April de 2013). *Сергей Шойгу объявил о «большой охоте» на молодых программистов*. Obtenido de C News: https://www.cnews.ru/news/top/sergej_shojgu_obyavil_o_bolshoj_ohote

Putin, V. (18 de March de 2014). *Address by the President of the Russian Federation*. Obtenido de http://en.kremlin.ru/events/president/news/20603

Rid, T. (2013). *Cyber War Will Not Take Place.* New York: Oxford University Press.

Saltykov, E. (12 de March de 2014). *В России созданы кибервойска*. Obtenido de Vesti: https://www.vesti.ru/doc.html?id=1573024

Schwartau, W. (1996). *Information Warfare.* New York: Thunder's Mouth Press.

Schwartz, J. (24 de June de 2007). *Preparing for a Digital Pearl Harbor*. Obtenido de New York Times: https://www.nytimes.com/2007/06/24/business/worldbusiness/24iht-cyber.1.6299676.html

Selhorst, L.-C. (2016). Russia's Perception Warfare: The Development of the Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine. *Militaire Spectator*, 148-164.

Shackelford, S. J. (2013). Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance. *American University Law Review, 62*(5), 1273-1364.

Socor, V. (2 de May de 2007). *RUSSIA BEGINS CYBER ATTACKS AGAINST ESTONIAN GOVERNMENT*. Obtenido de The JamesTown Foundation: https://jamestown.org/program/russia-begins-cyber-attacks-against-estonian-government/

Sukhankin, S. (30 de November de 2016). *Russia Beefs up Its Offensive Cyber Capabilities*. Obtenido de The Jamestown Foundation: https://jamestown.org/program/russia-beefs-offensive-cyber-capabilities/

Sukhankin, S. (27 de January de 2017). *Lithuania: The Old-New Target of Russian 'Hybrid Warfare?'*. Obtenido de The Jamestown Foundation: https://jamestown.org/lithuania-old-new-target-russian-hybrid-warfare/

Sukhankin, S. (11 de May de 2017). *Russian 'Cyber Troops': A Weapon of Aggression*. Obtenido de The Jamestown Foundation: https://jamestown.org/program/russian-cyber-troops-weapon-aggression/

Sukhankin, S. (21 de March de 2017). *Russian National Guard: A New Oprichnina, 'Cyber Police' or Something Else?* Obtenido de The Jamestown Foundation: https://jamestown.org/program/russian-national-guard-new-oprichnina-cyber-police-something-else-2/

Tass. (12 de March de 2014). *Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций*. Obtenido de Tass: https://tass.ru/politika/1179830

The Ministry of Foreign Affairs of the Russian Federation. (30 de November de 2016). *Foreign Policy Concept of the Russian Federation (approved by President of the Russian Federation Vladimir Putin on November 30, 2016).* Obtenido de Министерство иностранных дел Российской Федерации:

https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248

Turovsky, D. (3 de September de 2015). *Грузить по полной программе Зачем госкорпорации понадобилась система для организации DDoS-атак. Репортаж Даниила Туровского*. Obtenido de Meduza: https://meduza.io/feature/2015/09/03/gruzit-po-polnoy-programme

Turovsky, D. (7 de November de 2016). *Российские вооруженные киберсилы Как государство создает военные отряды хакеров. Репортаж Даниила Туровского*. Obtenido de Meduza: https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily

Tzu, S., Griffith, S. B., & Liddell Hart, B. H. (1963). *The Art of War.* New York: Oxford University Press.

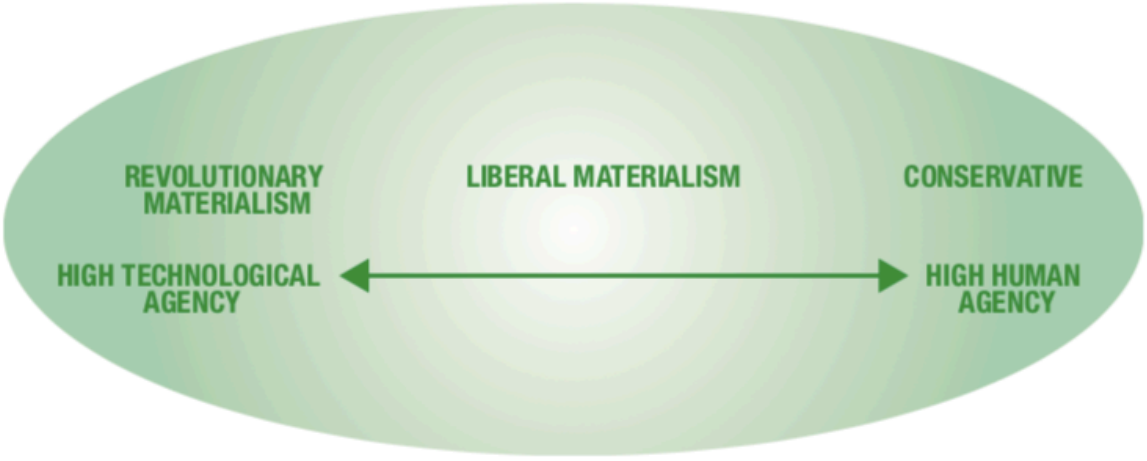
Willett, M. (12 de March de 2019). *Cyber instruments and international security*. Obtenido de International Institute for Strategic Studies: https://www.iiss.org/blogs/analysis/2019/03/cyber-instruments-and-international-security

Zakem, V. (6 de January de 2017). *How Russia's Disinformation Campaign Could Extend Its Tentacles*. Obtenido de npr: https://www.npr.org/2017/01/06/508032496/how-russias-disinformation-campaign-could-extend-its-tentacles?t=1590166067869

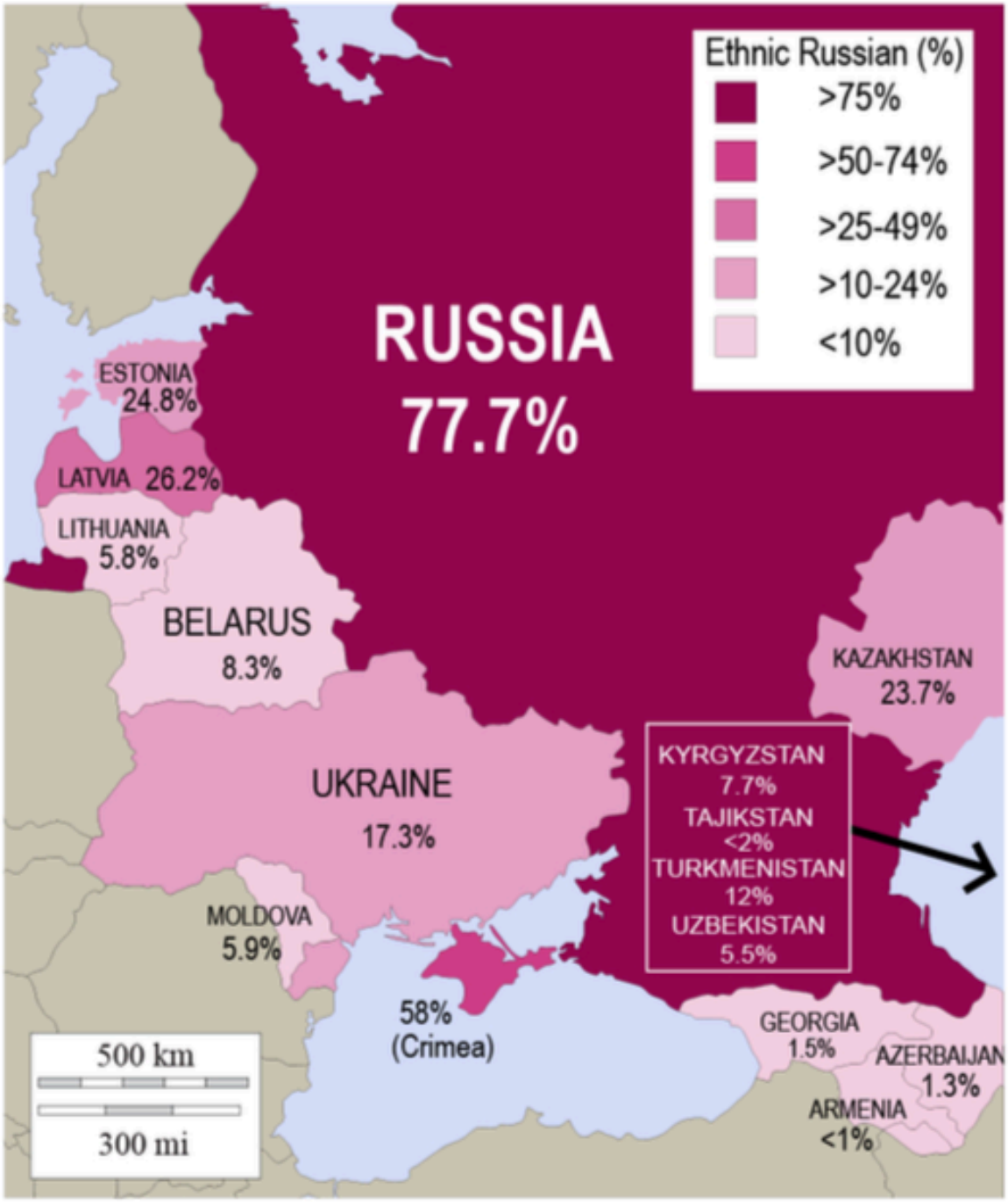
Zakem, V., Saunders, P., & Antoun, D. (2015). *Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union.* Arlington: CNA.

12. ANEXOS

Anexo 1: espectro escuelas ciberguerra (Fuente: Martin, 2016)



Anexo 2: porcentaje de minorías étnicas rusas en los países vecinos de Rusia (Fuente: CNA)



Anexo 3: mecanismos de control reflexivo (Fuente: Selhorst, 2016)

Deception	*forcing the enemy to reallocate forces to a threatened region during the preparatory stages of combat operations*
Deterrence	*creating the perception of insurmountable superiority*
Distraction	*creating a real or imaginary threat to one of the enemy's most vital locations during the preparatory stages of combat operations, thereby forcing him to reconsider the wisdom of his decisions to operate along this or that axis*
Division	*convincing the enemy that he must operate in opposition to coalition interests*
Exhaustion	*compelling the enemy to carry out useless operations, thereby entering combat with reduced resources*
Overload	*frequently sending the enemy a large amount of conflicting information*
Pacification	*leading the enemy to believe that pre-planned operational training is occurring rather than offensive preparations, thus reducing his vigilance*
Paralysis	*creating the perception of a specific threat to a vital interest or weak spot*
Pressure	*offering information that discredits the government in the eyes of its population*
Provocation	*force him into taking action advantageous to your side*
Suggestion	*offering information that affects the enemy legally, morally, ideologically, or in other areas*