

CAPÍTULO 3

LA NIEBLA DE LA GUERRA DE INFORMACIÓN RUSA

Lionel M. Beehner, Coronel Liam S. Collins y Robert T. Person

“Esta es una carrera armamentista”, dijo Mark Zuckerberg, Director Ejecutivo de Facebook a una nueva comisión del Congreso, en referencia al uso de las redes sociales por parte de la Federación Rusa para llevar a cabo la guerra de información. “Ellos van a seguir mejorando”.¹ Las herramientas y tácticas de la guerra de información rusa pueden haber cambiado a lo largo de las décadas, pero como muchos analistas han señalado, los fines permanecen en gran medida sin cambios desde los tiempos soviéticos: complicar, contener y restringir la proyección del poder estratégico de EEUU y de sus aliados, predominantemente en Eurasia pero también en el Medio Oriente. Es una forma completamente racional de dar forma al entorno estratégico para obtener ventaja, dadas las asimetrías cuantitativas y cualitativas entre Rusia y Occidente en capacidades convencionales.

Con el Ejército de EEUU cambiando su enfoque doctrinario desde contra-insurgencia hacia operaciones de combate a gran escala, competidores pares y casi pares tales como China, Irán y Rusia adquieren una importancia renovada.² Pero eso no implica necesariamente un cambio doctrinario completo hacia operaciones convencionales a gran escala, dados todos los tipos de guerra que estos estados prefieren llevar a cabo. Después de todo, la así llamada “guerra sin contacto”, como la definen los rusos, está destinada a negar su desventaja militar evitando cualquier contacto directo con las fuerzas occidentales, ya sea demostrando disciplina de fuego o desplegando “pequeños hombres verdes” en lugares como Crimea.³ Rusia ha mostrado una capacidad notable y voluntad, con medios bastante directos, para interrumpir instituciones democráticas, socavar la cohesión social y sembrar confusión, duda y desconfianza entre los aliados occidentales y sus públicos. Las redes sociales solo han acelerado el ritmo del avance de la guerra de información (IW).

Deberíamos tener claro qué se entiende por guerra de información rusa, o *informatsionnaya voyna*. La guerra de información no es simplemente una he-

rramienta para lograr algún tipo de objetivo táctico limitado o ventaja durante tiempo de guerra, típicamente en la fase inicial de hostilidades. Más bien, la guerra de información debería ser considerada más ampliamente. Calculada y sistemática, consiste en operaciones destinadas a degradar la capacidad del enemigo para controlar el espacio de información, negarle la capacidad técnica para tomar represalias a través de medios del ciberespacio y defiende una narrativa de nacionalismo ruso, para glorificar su papel en el escenario mundial –una forma manipuladora del “poder blando” ruso–. La guerra de información rusa comprende una gran cantidad de innovaciones tácticas, desde operaciones psicológicas tradicionales (psy-ops) y comunicaciones estratégicas dirigidas a controlar la narrativa, hasta el despliegue de sofisticados trolls [N. del T.:^c] y bots descentralizados en las redes sociales y otras plataformas en línea.⁴

La guerra de información rusa –*informatsionnaya voyna*– consiste en tres pilares. Primero y lo más benigno, apunta a dar el mejor giro posible a noticias ordinarias. Lo hace a través de medios controlados por el estado como RT (ex “Rusia Today”), radio en idioma ruso (“Sputnik”), así como a través de canales de televisión que dan servicio a la población ruso-parlante de los ex estados soviéticos. Este giro generalmente pinta a Rusia como una alternativa viable y preferida y contraria a la avaricia y agresión de EEUU.⁵ Segundo, utiliza desinformación para crear suficiente ambigüedad para confundir a las personas, tanto en el país como en el extranjero, sobre sus operaciones actuales, ya sea en Ucrania, Siria, o en otra parte, todo con el objetivo de proporcionar un señuelo y contribuir a la proverbial “niebla de guerra”. Tercero, miente rotundamente cuando se le da información verdadera y afirma que es falsa. Esta última estrategia tiene varios objetivos: degradar la confianza en las instituciones de todo el mundo; presionar a poblaciones actualmente en conflicto para simplemente aceptar el statu quo del conflicto y no presionar por resolución; y finalmente, evitar que países en su deseada esfera de “interés privilegiado” ingresen a alianzas occidentales como la OTAN, al mantener estas áreas en perpetuo conflicto.

Curiosamente, mientras que las empresas tecnológicas occidentales apuntan a una carrera armamentista con competidores pares como la Federación

^c [Nota del T]: *Troll: En la jerga de Internet, persona que se dedica a provocar con comentarios, busca crear controversia o desviar la atención de una temática.*

Rusa y la República Popular China, el gobierno de EEUU no se considera en guerra. Nosotros argumentamos que esta ingenuidad es un error estratégico. En este capítulo, examinamos cómo opera la guerra de información rusa y cómo debería ser conceptualizada en el nivel estratégico. ¿Cómo encajan las operaciones de información (IO) en los objetivos estratégicos mayores de Rusia? ¿Cuáles son sus métodos primarios? Y finalmente, y quizás lo más importante, ¿cómo pueden los militares estadounidenses combatir eficazmente la guerra de información rusa, mientras se mantienen fieles a sus valores y simultáneamente evitar la escalada del conflicto? En este capítulo, presentamos tres argumentos centrales:

- Primero, el liderazgo de Rusia no aplica guerra de información únicamente para apoyar sus objetivos militares, —como una manera de ablandar al enemigo o preparar el campo de batalla, por así decirlo— sino más bien a la inversa. Sus operaciones militares en lugares como Ucrania o Siria a menudo son subordinadas al objetivo estratégico más inmediato de Rusia: desafiar los intereses de EEUU siempre que sea posible y socavar la capacidad de Estados Unidos para avanzar sin obstáculos con sus propios objetivos estratégicos. Como tal, puede considerarse una forma de balanceo estratégico posterior a la Guerra Fría por parte de Moscú, que involucra medios políticos, económicos, de ciberespacio y, —más formidablemente—, de información, para contener y restringir las actividades de EEUU globalmente. En este sentido, la IW no debe verse simplemente como una herramienta dentro el juego de herramientas *militares* de Rusia. Aunque la IW rusa ciertamente ha sido usada como parte de operaciones militares, a menudo se aplica para la obtención de objetivos políticos rusos donde los objetivos militares pueden estar ausentes. Por lo tanto, cuando los observadores perciben evidencia de IW rusa, no deberían saltar inmediatamente a la conclusión de que son parte de una estrategia militar para formalmente apoderarse de más territorio en el este de Ucrania o enviar una columna de tanques a los Países Bálticos. En relación con los esfuerzos de IW de Rusia, los fines son desafiar los intereses estadounidenses y socavar los cimientos de las instituciones democráticas occidentales; al sembrar incertidumbre, discordia y división en los Estados Unidos y sus aliados, las tácticas de IW son un medio particularmente barato, ambiguo y efectivo para obtener esos fines estratégicos. En la medida en que la guerra de información va de la mano de las operaciones militares convencionales rusas, la experiencia

reciente demuestra que estas últimas son, en cierto sentido, acontecimientos secundarios para la primera, no a la inversa.

• Segundo, aunque la guerra de información se aplica con frecuencia para fines políticos no militares, Rusia sin embargo, se considera en guerra con Occidente y aporta esa mentalidad a sus operaciones. Moscú conduce así la guerra de información principalmente de forma preventiva para debilitar a su enemigo –Estados Unidos y Europa–. La guerra de información fue incorporada formalmente en la doctrina militar rusa en 2010 y se remonta a los momentos más críticos de la Guerra Fría, pero se ha expandido exponencialmente desde entonces. Hasta la fecha, Rusia se ha visto a sí misma como capaz de lograr el “dominio de la información”, –es decir, la capacidad de penetrar el entorno de información estadounidense, desde plantar historias en los medios hasta piratear los correos electrónicos de políticos y sus operarios, e influir en los resultados políticos.⁶

• Tercero, cuando se trata de agresión rusa en el ámbito de la información, estamos en guerra. Aunque puede ser “guerra política”, para pedir prestada la expresión de George Kennan en un memorando de Personal de Planeamiento de Política de 1948, esto es guerra de todas formas.⁷ Para contrarrestar la actividad maliciosa rusa, uno debe “combatir el fuego con fuego.” La disuasión convencional de EEUU en la región ha consistido principalmente en emplazar varios batallones en socios de la OTAN como Polonia y los Paises Bálticos. Incluso, un informe reciente de RAND descubrió que Rusia sobrepasaría las fuerzas de la OTAN en cuestión de horas.⁸ El desequilibrio es aún más severo en el ámbito de información: no existe una disuasión suficiente para evitar ataques de IW rusa, ni un mecanismo punitivo para poner en práctica medidas de represalia más allá de emitir declaraciones condenando tales actos. Reconocemos que la atribución es un problema en este espacio, como lo es el riesgo de escalada de conflicto. Sin embargo, la posición defensiva actual de los Estados Unidos no está funcionando. Para citar un congresista, “[P]or qué no ir a la ofensiva y divulgar información que expone la corrupción en el Kremlin?”⁹ Sin reglas de empeñamiento más libres y una estrategia más ofensiva, podemos esperar que Rusia y sus agentes continúen sin cesar sus operaciones de información planificadas, porque Estados Unidos continúa cediendo la iniciativa estratégica en el entorno de información.

Este capítulo continúa de la siguiente manera: primero proporcionamos algunos antecedentes de IW rusa, definimos varios conceptos clave e identificamos los principales métodos que Rusia utiliza y los desafíos que plantean. A continuación, exponemos los objetivos estratégicos de mayor envergadura de la IW rusa, tanto contra Occidente como contra Ucrania y otros ex estados soviéticos. Luego, detallamos sus métodos de IW examinando el estudio de caso de Ucrania. Concluimos describiendo una lista de recomendaciones para los militares de EEUU para combatir eficazmente los esfuerzos de IW de Rusia.

Operaciones de Información 101

Clausewitz notó correctamente que la naturaleza de la guerra nunca cambia, solo su carácter. El habría reconocido el carácter de la guerra de información como una forma distinta y efectiva de guerra para lograr los fines políticos propios, dado que el centro de gravedad de un enemigo está cambiando. La mayor fortaleza de Estados Unidos es, paradójicamente, también su mayor debilidad: o sea, nuestra libertad de expresión y prensa. Aquí los rusos están practicando un libro de tácticas salidas directamente de Clausewitz: ataca al enemigo donde sea *más* vulnerable. Los militares de EEUU definen las operaciones de información como: “el empleo integrado, durante operaciones militares, de capacidades relacionadas con información en concierto con otras líneas de operación para influenciar, perturbar, corromper o usurpar la toma de decisiones de adversarios y potenciales adversarios, mientras protegemos la muestra”.¹⁰ Además, define guerra de información como “actividades de uso de información orquestadas por una amenaza (como operaciones del ciberespacio, guerra electrónica y operaciones sicológicas) para obtener una ventaja en el entorno de información”. En otras palabras, IO se refiere a acciones de propia tropa en el entorno de información, mientras que IW se usa para describir actividades basadas en amenazas.

De acuerdo con nuestro argumento sobre la IW rusa como una forma de guerra política, es importante tener en cuenta que la definición anterior es excesivamente restrictiva, al definir la guerra de información como residiendo estrictamente dentro de los límites de operaciones militares. Por lo tanto, nos resulta útil emplear un “concepto holístico [de guerra de información] que incluye operaciones de red de computadoras, guerra electrónica, operacio-

nes sicológicas y operaciones de información".¹¹ La guerra de información –a veces llamada “operaciones de influencia”– se refiere ampliamente a la práctica de recopilar información sobre un enemigo, así como la difusión de desinformación y propaganda para buscar una ventaja sobre el adversario, ya sea en tiempos de paz o de guerra.

La guerra de información rusa se lleva a cabo a través de cinco métodos principales, que van desde lo sicológico a lo técnico: la manipulación de información (noticias falsas), espionaje (inteligencia), interferencia política, engaño militar (negación creíble) y capacidades basadas en el ciberespacio (redes sociales). Este último es el único elemento que es realmente nuevo e innovador, ya que permite incremento en velocidad y a una mayor distancia. A continuación resumimos estos métodos.

Primero, Rusia ha dominado el uso de noticias falsas y otra desinformación para confundir o persuadir a los consumidores de medios, tanto en Rusia como en Occidente. El propósito de este esfuerzo es erosionar el apoyo público y la confianza en las instituciones democráticas occidentales, para crear y amplificar discordia pública y política, para crear confusión con el fin de demorar a los tomadores de decisiones occidentales en los más altos niveles, e intensificar la competencia en seguridad en áreas de importancia estratégica tanto para Occidente como para Rusia. Esto es especialmente cierto en Europa del Este y el sur del Cáucaso a lo largo de la línea divisoria entre la OTAN y los países que alguna vez orbitaron dentro de la esfera de influencia de la Unión Soviética: los Países Bálticos, Georgia y Ucrania. Intensificar la competencia sirve para agitar a los adversarios de Rusia, provocarlos e influir en sus públicos adversos al riesgo, para desaprobar la toma de cualquier clase de medidas de represalia. Otro subproducto de este uso de IW es apoyar directa e indirectamente a grupos antisistema, partidos y políticos en Occidente –muchos de ellos de derecha o ultranacionalistas–, como una manera de proporcionarles una apariencia de legitimidad e interrumpir el proceso democrático. “La nueva propaganda de Rusia no es ahora tratar de vender una particular cosmovisión”, como argumenta Alexei Levinson. “Es acerca de tratar de distorsionar los flujos de información y exacerbar el nerviosismo entre las audiencias europeas”.¹²

Segundo, la IW rusa incluye el trabajo del tradicional espionaje estilo Guerra Fría, como robar materiales comprometedores e información sobre

el enemigo de uno, conocido en ruso como *kompromat*.¹³ Durante la era soviética, este tipo de guerra de información era referida como “control reflexivo”, una teoría con raíces profundas en la investigación en psicología y cibernética del Ministerio de Defensa Soviético, que mapeó cómo los enemigos formaban las decisiones y encuadraban problemas.¹⁴ “En el contexto de la guerra”, como señala Maria Snegovaya, “el actor que es más capaz de predecir e imitar el razonamiento y las acciones de su oponente, tiene la mayor probabilidad de éxito”.¹⁵

Durante la Guerra Fría, los principales soldados de a pie en este frente fueron oficiales de inteligencia de la KGB, incluido un joven oficial de la KGB en Dresden con el nombre de Vladimir Putin. Hoy Rusia depende de “tropas de información”, que actúan como armas de alquiler en el ámbito de la propaganda: contratistas, ex criminales y otros actores e intermediarios de la guerra cibernética.¹⁶ Son mantenidos a un brazo de distancia de Moscú, para proporcionar al Kremlin una negación creíble si son atrapados. El objetivo de estos mercenarios es diverso: perturbar las telecomunicaciones del enemigo o sistemas de almacenamiento de datos; interferir y socavar las elecciones democráticas en Occidente, ya sea mediante la liberación de información sensible, provocación por Internet (trolls), publicación de noticias falsas u otras tácticas que consideren socavarán a la democracia.

Entrometerse en elecciones extranjeras no es una táctica nueva. Tampoco es una técnica exclusiva de Rusia o su predecesora, la Unión Soviética. Según Dov Levin, “Entre 1946 y 2000, Estados Unidos y la URSS/Rusia intervinieron [para manipular elecciones extranjeras] 117 veces, o, dicho de otra manera, en aproximadamente *una de cada nueve* elecciones ejecutivas competitivas a nivel nacional durante este periodo.”¹⁷ Sin embargo, lo que ha cambiado es la sofisticación tecnológica, el uso de subsidiarios que operan en nombre de los estados nación, y la habilidad para aprovechar la velocidad de las redes sociales. En febrero de 2017, por ejemplo, el fiscal especial Robert Mueller acusó a trece rusos y tres compañías rusas por interferir en la elección presidencial de EEUU de 2016. Entre las compañías acusadas estaba la Agencia de Investigación de Internet, una “granja de trolls rusos”, con el “objetivo estratégico de sembrar discordia en el sistema político de EEUU”.¹⁸ En su libro, *Guerra en 140 Carácteres*, David Patrikarakos describió edificios de oficinas enteros

en Siberia dedicados a crear historias de noticias falsas para influir en el comportamiento de los votantes en las elecciones occidentales.¹⁹

El cuarto componente de la IW de Rusia es sumar a la niebla de la guerra y negar la presencia de las fuerzas militares rusas –específicamente su uso de fuerzas *Spetsnaz* en lugares como Ucrania. Esto es para distraer y oscurecer la existencia de una campaña militar extensiva, –que los soviéticos solían llamar *maskirovka*–, que podría desencadenar una respuesta de Occidente más robusta o empeorar una reacción violenta en casa, si los hechos completos de las operaciones, incluyendo el total de muertos, sean hechos públicos.²⁰ El gobierno ruso siempre niega cualquier uso de este tipo de guerra y en su lugar atribuye estos ataques a “patriotas” rusos operando en su propio nombre, sin directrices de Moscú. Este tipo de campaña de desinformación es difícilmente el trabajo de una red descentralizada de activistas de base pro-Rusia improvisando por cuenta propia, sino más bien es un esfuerzo de nivel nacional fuertemente estructurado, para facilitar el logro de los objetivos estratégicos de Rusia. De acuerdo al desertor ex KGB, Ion Mihai, este tipo de campaña tiene tres puntas: negar involucramiento, minimizar el daño y, si se revela la verdad, echarle la culpa a los enemigos de uno.²¹

Finalmente, además de brigadas de información, intromisión electoral y engaño, Rusia emplea tecnologías digitales para influir en las redes sociales y agregar mayor velocidad y sofisticación a sus campañas de IW. Esto incluye, como señala Keir Giles, “una compleja mezcla de piratería, divulgación pública de correos electrónicos privados y uso de bots, trolls y publicidad dirigida en las redes sociales, diseñada para interferir en los procesos políticos y aumentar tensiones sociales”.²² Actores maliciosos pueden cosechar los datos personales de usuarios confiados de las redes sociales, tal como el historial de navegación y datos de gastos de consumo, lo que les permite dirigirse a grupos e individuos por sus puntos de vista políticos, su nivel de ingresos y su ubicación. Entonces pueden plantar mensajes contradictorios en las noticias que hayan expuesto desavenencias ideológicas. Un ejemplo concreto fueron los bots y trolls vinculados a Rusia promoviendo historias divisionistas y hashtags [N. del T.:^D] en las redes sociales que exacerbaron la controversia del

^D [N. del T.]: **Hashtag:** Palabra(s) o serie de caracteres alfanuméricos precedidos por el símbolo “#” que sirve como etiqueta para ciertas plataformas de redes sociales.

himno nacional en la Liga Nacional de Fútbol. Los piratas informáticos rusos también plantan informes falsos en los principales medios de comunicación. En mayo de 2017, los medios estatales de Qatar publicaron comentarios falsos hechos por el emir de Qatar elogiando a Irán, creando un alboroto entre sus vecinos del Golfo.²³

Objetivos rusos

Esta sección examina los objetivos rusos y cómo la IW encaja en las metas estratégicas mayores de Moscú. A menudo se dice que Rusia está determinada a socavar la democracia como un fin y reescribir las reglas del orden internacional. En este punto, Rusia es en realidad bastante agnóstica respecto al valor normativo otorgado a la democracia o al liberalismo. Si Estados Unidos fuera una dictadura totalitaria desfilando sus fuerzas por todo el mundo, Rusia podría conjeturar que jugar del lado liberal del pueblo puede beneficiar su capacidad para resistir la dominación estadounidense. Rusia, en este papel, está jugando de contrapunto de Estados Unidos. A este respecto, la gran estrategia de Rusia no es ideológica en su motivación: su objetivo no son las instituciones democráticas per se, sino que el objetivo son las instituciones políticas de un estado adversario. Que esas instituciones resulten ser democráticas es –desde un punto de vista ideológico–, irrelevante. Pero desde un punto de vista práctico, la apertura de las instituciones democráticas liberales las hace más vulnerables a ataques.

Lo que muchas audiencias occidentales fallan en apreciar es el hecho de que Rusia cree de sí misma estar enfrentando fuego de IO con fuego de IW. La narrativa de Moscú de la Revolución de las Rosas de 2003 en Georgia, la Revolución Naranja de 2005 y la Revolución de Maidan de 2014 en Ucrania y las protestas masivas de 2011-2012 en Rusia, es la de un intento de Occidente por interferir en las propias elecciones de los países donde Moscú tiene fuertes intereses. Por lo tanto, la visión del Kremlin es que sus propios esquemas son simplemente ojo por ojo, un juego de gato y ratón jugado contra la superpotencia dominante del mundo. Al tratar de desafiar, restringir y contener los intereses estadounidenses, Rusia busca un mundo más multipolar donde se le otorgue un asiento entre las grandes potencias, más allá de lo que ya disfruta con un puesto permanente en el Consejo de Seguridad con poder de voto.

En la visión de Moscú de un mundo multipolar, las grandes potencias como Rusia deberían tener un derecho a esferas de interés privilegiado y mano libre para dedicarse a sus intereses dentro de su esfera, sin impedimentos. La única forma de lograr tal mundo es hacer retroceder la influencia estadounidense. Debería además decirse que Rusia es también un poder económico en declive que juega una mano débil –política, económica y militarmente–. Para contrarrestar los intereses estadounidenses, se basa en la IW como un medio de guerra rentable y menos riesgoso.

Pero esta lógica requiere desempacar. Primero, la guerra de información rusa a menudo se trata como solo una parte de su estrategia militar más amplia, que incluye una serie de otros usos de la fuerza. Sin embargo, esto disminuye la importancia de la IW, y la trata como uno de los varios medios no cinéticos, –una canasta de opciones a veces referida como “guerra de nueva generación”–, que Rusia emplea en conjunción con medios cinéticos en la búsqueda de objetivos militares.²⁴ Pero como se argumentó anteriormente, los objetivos de Rusia son a menudo políticos en naturaleza, en lugar de militares. De hecho, la IW en busca de fines políticos es atractiva por su bajo costo, bajo riesgo y su relativa simplicidad. Rusia se figura a sí misma como el “gran perturbador”, perturbar no requiere un objetivo final adicional más que el mero proceso de desestabilización de la democracia occidental –incluyendo su normas, procedimientos, instituciones–. Sembrar las semillas del caos es, muchas veces, el objetivo principal. Para estar seguro, uno podría argumentar que esto es parte de un gran diseño para inclinar las reglas del juego a su favor al descartar cualquier libro de reglas. Como escriben Edward Lucas y Ben Nimmo, “El enfoque de Rusia, a diferencia del étnico e ideológico de la Alemania Nazi, es profundamente nihilista”²⁵ Sin embargo, debería enfatizarse que el nihilismo no es el fin sino el medio. El fin es contener y restringir la influencia estadounidense en todo el mundo. Cuando se trata de límites de comportamiento aceptable para lograr este fin, Rusia no seguirá ninguna regla. Como es mencionado en el *Manual 2.0 de Tallin* sobre guerra cibernética, “Los rusos son maestros en jugar en el ‘área gris’ de la ley, ya que saben que esto hará que sea difícil afirmar que están violando el derecho internacional y justificando respuestas tales como contramedidas”²⁶

Conceptualmente hablando, la campaña de IW de Rusia es vista por muchos occidentales como defensiva y en línea con lo que Rusia hizo durante la

Guerra Fría. Pero las actividades de guerra de información de Rusia, deberían ser vistas como ofensivas, dado que una gran parte de la efectividad de la IW como un medio, es su elemento sorpresa. Para reiterar, Rusia se considera a sí misma estando “en guerra” (o más precisamente “en guerra política”) con Occidente, pero Occidente no se considera a sí mismo “en guerra” con Rusia. Una teoría popular entre los neorrealistas conocida como la “teoría de defensa ofensiva” ofrece información sobre el desafío en cuestión. La teoría plantea que en casos donde las medidas ofensivas mejoran la seguridad de un estado de manera más eficiente que las medidas defensivas, y donde las intenciones de un estado, –ya sean ofensivas o defensivas– son indistinguibles, entonces la amenaza de guerra e inestabilidad es mayor.²⁷ La lógica es que este tipo de configuración favorece una ventaja al que mueve primero y permite ataques preventivos. Este principio también se aplica al uso de la guerra de información. Hay un elemento de sorpresa incorporado, así como uno de asimetría. Estas operaciones son ofensivas –incluso si no son cinéticas– por diseño. Según Maria Snegovaya, “En el nivel táctico, la guerra de información permite a Rusia lograr sorpresa en el momento o forma de un ataque. Rusia gana así tiempo y eficiencia contra las fuerzas terrestres del enemigo... La cobertura informatacional proporciona más flexibilidad y eficiencia a los militares, así como mejora la velocidad de maniobrabilidad y la velocidad de las respuestas en el campo de batalla”.²⁸

Sin embargo, parte de la confusión (y por lo tanto la utilidad desde la perspectiva rusa) de la IW es que se puede aplicar a fines políticos simultáneamente con fines militares. En tales contextos puede ser difícil determinar a priori cuáles son los objetivos de algunas operaciones de información. Esta es la situación que encontramos en Ucrania, donde los objetivos políticos y militares son, a la vez, parte de la lógica del conflicto. Cabe señalar que la estrategia de Rusia en Ucrania es complicada aunque también aleatoria. El objetivo de las operaciones militares de Rusia en Ucrania *no es* simplemente adquirir territorio –si quisiera, Rusia podría haber fácilmente anexado militarmente al Donbas, la zona de conflicto en el este de Ucrania, por ahora– sino más bien para mantener a Ucrania oprimida, sembrar confusión entre su público y evitar que Ucrania ingrese a instituciones occidentales. Rusia busca socavar los principios fundamentales de cada institución a la que Ucrania quiere unirse.

las plataformas de redes sociales dominantes en idioma ruso –*Vkontakte* y *Odnoklassniki*– las autoridades pudieron bloquear efectivamente cualquier página con una inclinación pro-Maiden. También permitió al gobierno ruso monitorear a los simpatizantes del gobierno ucraniano posterior a Maiden, así como reclutar soldados de a pie para sus pro-separatistas subsidiarios. Segundo [N. del T.^E], el Kremlin dio un giro considerable en su descripción de los acontecimientos en Ucrania, desde la Revolución de Maiden de 2013-2014 a la toma de posesión de Crimea, y hasta la guerra en curso en el este. Retrató a Crimea como tierra que históricamente perteneció a Rusia. Exageró la influencia que ejercieron los nacionalistas ucranianos y neonazis entre los manifestantes de Maiden, y más tarde, aquéllos luchando en la región de Donbas para avivar el miedo entre la población de origen étnico ruso y ucranianos de habla rusa. Demonizar al enemigo fue tácticamente importante para sus subsidiarios, permitiendo el uso de mayor violencia contra sus conciudadanos. Finalmente, los medios de comunicación rusos controlados por el Kremlin ignoraron la presencia de soldados rusos y fuerzas *spetsnaz* en Ucrania, y minimizaron la ilegalidad del arrebato de tierras de Rusia a Crimea. Por el contrario, Rusia exageró enormemente el papel desempeñado por los Estados Unidos en controlar las protestas en Maiden e influenciar en los eventos en el este.

Además, los operativos rusos procuraban configurar el campo de batalla captando y manipulando directamente las mentes de las tropas ucranianas a través de formas subversivas de propaganda y desinformación. En 2017, las autoridades rusas crearon las llamadas “tropas de operaciones de información”, cuyo cometido, según el Ministro de Defensa de Rusia, Sergei Shoygu, era difundir “Propaganda inteligente y eficiente”.³⁰ El objetivo de estas tropas abarca una mezcla de comunicaciones estratégicas, operaciones psicológicas y actividades de influencia. Ellas no deberían ser tratadas como un comando separado basado en el ciberespacio, ya que sus medios van más allá de simplemente llevar a cabo la guerra cibernética para afectar redes, sino que también incluyen manipular los medios e infiltrar contra-propaganda con el fin de controlar y distorsionar la comprensión cognitiva del enemigo, de lo que es real y lo que es falso. Esto involucra infiltrar historias de noticias falsas para avivar la violencia irredentista. Un ejemplo de ello es el flujo constante de desinformación entre las transmisiones de noticias en idioma ruso en el sur

^E[N. del T.]: Se repite “Segundo” en el original.

y el este de Ucrania, amenazando a los lugareños que Kiev anularía su derecho a hablar el idioma ruso. En la plaza Kolika en 2014, el periodista David Patrikarakos documentó cómo a un grupo de hombres enmascarados armados con bates y garrotes, se les dijo que un grupo de nacionalistas ucranianos llamado *Pravy Sektor* (“Sector Derecho”) estaba vieniendo “a incendiar nuestras carpas a las 4:00 a.m.”. Gran parte de la desinformación juega con los valores morales tradicionales de la gente. En 2014, los medios de comunicación rusos también informaron falsamente que los soldados ucranianos habían crucificado a un niño pequeño.³¹ Otro meme [N. del T.^F] popular que circulaba en las redes sociales rusas era el de un activista LGBT (lesbiana, gay, bisexual, transgénero) en Maiden que hostigó a una transeúnte heterosexual hasta el punto de aporrearla hasta la muerte. El objetivo de tales intentos es pintar a los manifestantes con una gran pincelada como activistas LGBT, una forma de sembrar desconfianza entre los segmentos rurales y más conservadores de la sociedad ucraniana.³²

El blanco de estos esfuerzos de IW también fueron los miembros militares de Ucrania combatiendo en primera línea. Poco después de que la lucha comenzara en Ucrania oriental, en 2014, por ejemplo, soldados desplegados a la región de combate comenzaron a recibir “textos falsos”. Los mensajes a menudo tenían intención de amenazar y desmoralizar a las tropas en un conflicto “agotador” con algunos textos que se leían: “Soldados ucranianos, encontrarán sus cuerpos cuando la nieve se derrita”; “Vete y vivirás”; “Nadie necesita que tus hijos se conviertan en huérfanos”; “Soldado ucraniano, es mejor retirarse vivo que quedarse aquí y morir” y “No recuperarás a Donbas. Más derramamiento de sangre no tiene sentido.”³³

Otros mensajes tenían como objetivo socavar la cohesión y la moral de la unidad. Los textos, que a menudo parecían venir de soldados compañeros, habían afirmado que el comandante había desertado o que las fuerzas ucranianas estaban siendo diezmadas y que “Deberíamos huir”. Nancy Snow, una profesora de diplomacia pública en la Universidad de Estudios Extranjeros de Kyoto, describió esto como “propaganda puntual”. En conflictos previos, folletos lanzados por aire o mensajes de radio podían ignorarse fácilmente

^F [N. del T.]: **Meme:** Proceso que transmite información cultural de una mente a otra mente a través de una imagen.

-al negarse a levantar y leer el folleto o al sintonizar otra estación de radio— pero es casi imposible evitar la lectura de mensajes de texto enviados al propio teléfono.³⁴

Rusia combina su IW con operaciones cinéticas, comenzando con un mensaje de texto a un soldado, diciéndole que está “rodeado y abandonado”. Diez minutos después, la familia del soldado recibe (contactos recientes) un mensaje de texto diciendo: “Su hijo está muerto en acción”. Los amigos y la familia probablemente llaman al soldado para ver si la noticia es cierta. Diecisiete minutos después del mensaje de texto inicial, el soldado recibe otro mensaje que le dice “retirarse y vivir” con un ataque de artillería que sigue poco después, sobre la ubicación donde se detecta el gran grupo de teléfonos celulares destinatarios. Así, en una acción coordinada, usan IW para intimidar al soldado y su familia y amigos, y combina esto con guerra electrónica, guerra ciber-electrónica y artillería para producir efectos tanto cinéticos como psicológicos.³⁵ Esta es una técnica que los operativos rusos probablemente emplearán también en operaciones de combate a gran escala, —desdibujando los límites geográficos entre la línea del frente y el frente hogareño en formas nuevas y potencialmente aterradoras—.

Asimismo, los soldados de aliados potenciales no son inmunes a la IW rusa. Las tropas de la OTAN desplegadas en los Países Bálticos y Polonia como parte de la misión de disuasión también han sido atacadas. En lugar de “propaganda puntual”, a los soldados les han pirateado sus cuentas de Facebook, borrado datos o recibieron mensajes que decían “Alguien está intentando acceder a su iPhone” con un mapa apareciendo en el texto con Moscú en el centro del mapa. Un comandante cree que el intento de la IW es intimidar a los soldados y hacerles saber que las fuerzas de inteligencia rusas los están rastreando a ellos y sus datos están en riesgo.³⁶

Rusia también ha fijado como objetivo a los militares de EEUU, empleando IW en un intento para disminuir su alistamiento militar y la de sus aliados de la OTAN. Se sabe que medios de comunicación rusos han contactado a los alcaldes de las ciudades de afuera del área de entrenamiento de Hohenfels en Alemania, preguntándoles si el ruido del entrenamiento militar es perturbador para la población local. Este es un claro intento de sembrar discordia entre

las poblaciones y la base estadounidense, con la intención de influenciar al gobierno alemán para que imponga restricciones al entrenamiento militar.³⁷

Finalmente, la IW rusa en Ucrania ha incluido intentos de interferencia tecnológica en instituciones políticas a través de medios del ciberespacio, con diversos grados de éxito. Ucrania proporcionó un laboratorio de clases para piratas informáticos rusos, quienes luego interferirían más audazmente en las elecciones en los Estados Unidos y en Europa Occidental.³⁸ El concepto de “armamentización de la información” fue perfeccionado en Ucrania para socavar sus instituciones incipientes y erosionar la confianza pública. Además de apuntar a la infraestructura crítica, —grilla eléctrica de Ucrania, sitios web del gobierno y bancos— los operativos rusos eran activos en infiltrar historias de noticias falsas. La efectividad de tales operaciones, sin embargo, es cuestionable. Examinando los efectos de la propaganda rusa con relación a la TV rusa controlada por el estado en Ucrania, los polítólogos Leonid Peisakhin y Arturas Rozenas encontraron que los efectos eran inconsistentes:

Los ucranianos que ya estaban predisuestos a favor de Rusia encontraron su mensaje mediático persuasivo. Ucranianos pro-rusos que vieron la televisión rusa estaban con más probabilidades de votar por candidatos pro-Rusia en las elecciones presidenciales y parlamentarias de 2014, que los ucranianos anti-rusos que vieron la misma programación. Aquellos con puntos de vista anti-rusos fueron disuadidos por el mensaje de los medios rusos y pasaron muy probablemente a votar por políticos pro-occidentales. Parece que individuos sin antecedentes políticos fuertes no han sido influenciados en ninguna dirección.³⁹

Los autores argumentan que la actual erosión de credibilidad, como resultado de la IW rusa, representa no solo una amenaza para las democracias occidentales sino también para Rusia. Si Rusia se encontrara en una guerra prolongada, no muy diferente del actual conflicto subsidiario que encara en el Donbas, puede enfrentar un punto de inflexión donde la eficacia de su propaganda disminuya cada vez más. Esto puede resultar en que sus audiencias objetivo duden incluso de las narrativas falsas presentadas por los bots rusos, piratas informáticos y otros maestros de la interpretación. Sobre la base de investigaciones anteriores, los autores también postulan que la propaganda rusa

no cambia opiniones, sino más bien, empuja a los votantes a adecuar puntos de vista más extremos, e incrementa la polarización política, en sí misma un factor que socava la democracia y normas liberales. Ya sea que esto sea intencional o no, el efecto táctico de la IW rusa en Ucrania no trata de cambiar opiniones sino de empujar a la gente hacia el extremo y excluye el medio. El medio es donde prospera la democracia, los extremos polares son donde se marchita y muere.

Conclusión y Contramedidas

Lo siguiente incluye una lista de contramedidas recomendadas que Estados Unidos y sus aliados deberían implementar para contrarrestar o disuadir a Rusia del uso de la guerra de información.

- *Como lo hizo Durante la Guerra Fría, Estados Unidos debe disputar el Espacio de Batalla de IO.* Estados Unidos estuvo fuertemente comprometido en IO durante la Guerra Fría y la batalla de ideas –la idea que capitalismo y democracia liberal era superior al comunismo como un sistema económico y político– contribuyó significativamente en la victoria. Pero con el fin de la Guerra Fría, Estados Unidos cobró su dividendo de paz y se privó de instituciones de nivel nacional, tal como la Agencia de Información de Estados Unidos, que estaba diseñada para coordinar e integrar de manera efectiva los esfuerzos estratégicos y las respuestas a las amenazas. Como resultado, Estados Unidos ha cedido por omisión en gran medida, la iniciativa estratégica a actores pares y casi pares. Los Estados Unidos deben reinvertir en instituciones estratégicas y armar esas instituciones con el mandato y autoridad necesaria, para permitir que los Estados Unidos recuperen la iniciativa en el entorno de información. Como la superpotencia mundial, otras naciones siguen el ejemplo de los Estados Unidos y si los Estados Unidos elevan la importancia de IO, otras naciones los seguirán.

- *Relajar las Reglas de Empeñamiento para Contrarrestar la IW Rusa con IO.* Los Estados Unidos han hecho realmente poco para tomar represalias contra Rusia. La Ley Magnitsky de 2012 demuestra la efectividad que tales medidas pueden tener para presionar a Moscú y “avergonzar” a los individuos rusos poderosos.⁴⁰ El Congreso ha incorporado fondos de contra-propaganda

en su más reciente Ley de Autorización de Defensa Nacional, además de las reformas propuestas a la Ley de Registro de Agentes Extranjeros y el Comité de Inversión Extranjera en los Estados Unidos. Sin embargo, estos actos legislativos no van lo suficientemente lejos. El Consejo de Seguridad Nacional, en su estrategia de 2017, lo llama “arte de gobernar la información”⁴¹. Pero los Estados Unidos están limitados en su capacidad para empeñarse en este tipo de guerra. Como dijo un miembro superior del CSN, “no vamos a tener una RT. Los rusos lo hacen. Los iraníes lo hacen”⁴². Aun así, se necesitan contramedidas más innovadoras, menos evidentes, para disuadir, prevenir y castigar una agresión rusa futura en este espacio, incluyendo una más sofisticada y orientada versión de Radio Europa Libre/Radio Libertad, y Voz de Norteamérica para la era de Facebook.

- *Establecer una Disuasión Creible Contra IW.* La disuasión se basa en la amenaza de infligir dolor a un adversario para prevenir que tome una acción indeseable. Es importante destacar que el dolor amenazado debe ser suficiente para alterar el análisis de costo-beneficio del estado objetivo, de modo tal que altere sus preferencias: un adversario exitosamente forzado debe preferir evitar el dolor acatando en lugar de ignorar la amenaza y aceptar las consecuencias. Por lo tanto, una exitosa amenaza coercitiva –o disuasoria– depende de las capacidades para infligir dolor, y la voluntad de hacerlo. Queda por ver si Estados Unidos tiene los medios para infligir suficiente dolor sobre Rusia, como represalia por su IW contra nuestro sistema político. Pero no debe haber duda de nuestra voluntad de hacerlo. Si vamos a tener alguna esperanza de disuadir la futura interferencia rusa en nuestros procesos democráticos e instituciones, debemos hacer completo uso de las herramientas políticas y económicas a nuestra disposición, incluidas sanciones y otras formas de guerra financiera, para establecer una amenaza creíble de dolor. Además, debe quedar claro para todos –especialmente Moscú– que las medidas punitivas son castigo por acciones específicas contra las instituciones estadounidenses. Esto requiere que se ilumine con una luz brillante y muy pública sobre esas acciones, cuando hacerlo no amenace revelar fuentes de inteligencia, y declarar muy públicamente las consecuencias de tales acciones. Solo al demostrar regular y visiblemente a Moscú la relación de causa y efecto entre IW y las medidas punitivas, podemos esperar establecer un elemento disuasorio creíble.

• Proporcionar Asistencia de IO a Aliados. Los Estados Unidos proporcionan 50 mil millones de dólares en asistencia extranjera, pero casi nada de esto va a apoyar a esfuerzos de IO.⁴³ A pesar de cuatro años de ser blanco de la IW rusa, Ucrania está a la defensiva y parece no tener respuesta a los esfuerzos de IW rusa. Ucrania debería mejorar sus medidas defensivas para prevenir “propaganda puntual” y contrarrestar mejor las “noticias falsas” de Rusia. Pero no puede hacerlo sin ayuda significativa y experiencia externa. A pesar de que los Estados Unidos deben mejorar sus propias capacidades, los Estados Unidos tienen la capacidad, en términos de experiencia y fondos, para ayudar a Ucrania y otros aliados.

• *Reunir y Analizar Más Datos Sobre IW.* Los Estados Unidos deberían catalogar todos los ataques y adoptar un enfoque basado en evidencia para identificar fuentes y cuantificar su efectividad, como una forma de seguir su propio progreso en disuadir ataques y medir la variación en tiempo y espacio. Por ejemplo, los esfuerzos actuales del ejército ucraniano para transmitir radio en idioma ucraniano (FM Ejército) en el Donbas ni siquiera rastrea el número de oyentes, y mucho menos el efecto que tales mensajes positivos tienen en las actitudes públicas. En los Estados Unidos, hasta donde sabemos, todavía no hay una base de datos que rastree esa clase de cosas.

• *“Proteger Contra Noticias Falsas”.* Emilio Iasiello, un analista cibernético, recomienda “aprovechar la tecnología de punta para ayudar a identificar las mentiras en cuanto estas emergen. Podría usarse inteligencia artificial y análisis de datos para detectar palabras o patrones de palabras que podrían indicar historia fraudulentas”.⁴⁴ Los Estados Unidos deben hacer más que simplemente actualizar el registro. Por naturaleza, las correcciones al registro o las verificaciones de hechos son reactivas, y no son eficaces para contrarrestar los efectos de las noticias falsas proactivas y la propaganda rusa. En la batalla de la percepción, la carrera por dar forma a la narrativa temprana a menudo es la lucha decisiva. Los lectores rara vez se preocupan o leen correcciones, mucho menos desmentidas, especialmente en una era de redes sociales. Para ser efectivo, como recomienda Giles, “las contramedidas no deberían centrarse en la verificación de hechos” sino en el engaño –enfatizando que las personas fueron estafadas– y, como la desinformación original, debería apelar a las emociones de los lectores en lugar de su racionalidad”.⁴⁵ Esto es complicado, dado que los gobiernos occidentales apoyan la libertad de expresión, por lo

que no pueden restringir las noticias de manera general, incluso si son falsas, viniendo de un país o sus ciudadanos.

- *Crear una Fuerza de Tarea Robusta.* En marzo de 2015, la UE creó una Fuerza de Tarea Strat-Com, cuyo propósito es corregir la desinformación proveniente de medios rusos. Este tipo de fuerza de tarea debe ser fortalecida y quizás reforzada con la adición de sanciones económicas. Una fuerza de tarea similar debería crearse en los Estados Unidos, adecuadamente financiada y con poder.

- *Establecer un Marco Normativo más Fuerte para IO, al Igual que el Manual Tallin lo Hizo Para el Ciberespacio.* El problema con la propaganda en la era digital es que no hay reglas o normas acordadas, como las hubo durante el auge de la Unión Soviética. También los actores y perpetradores han sido descentralizados, haciendo más difícil la atribución, pero también más problemática la adherencia a normas o reglas. Aunque Rusia no acatará convenios acordados por otros estados y organismos internacionales, esto puede al menos ayudar a Occidente a determinar las reglas para el camino a una Rusia posterior a Putin, que puede determinar que las IO y el debilitamiento de la influencia estadounidense no son lo mejor para su interés.

- *Fortalecer las tasas de retención entre nuestros aliados.* Ucrania es un país repleto de experiencia en tecnología de información (IT). Sin embargo, el gobierno y sus militares tienen dificultades para retener la experiencia en este ámbito, debido a salarios más altos proporcionados en el sector privado. La asistencia de EEUU debe ser dirigida no solo a entrenar a nuestros socios, sino también a asegurar que retengan a sus combatientes.

- *Fortalecer la sociedad civil.* Muchos de los esfuerzos más innovadores y efectivos realizados para atacar la desinformación y la propaganda rusas están llegando de grupos de la sociedad civil como InformNapalm, que se basa en inteligencia de código abierto y emplea piratas informáticos voluntarios para desacreditar los relatos rusos, o StopFake, que publica contenido de medios para contrarrestar la propaganda rusa. Estos grupos han sido efectivos, dadas las encuestas recientes que muestran que una mayoría de ucranianos ahora dice que la propaganda rusa constituye una amenaza real.

• *Educar a los miembros de las Fuerzas y sus familias sobre la práctica rusa de IW.* Los miembros de las Fuerzas estadounidenses y sus familias deben ser advertidos de las prácticas y esfuerzos de IW rusos, para que no lo descubran por primera vez cuando reciban un mensaje de texto amenazante –esto será muy importante para reducir o eliminar el efecto deseado.

Vale la pena reevaluar la amenaza de la guerra de información rusa, dado el reciente cambio doctrinario hacia operaciones de combate a gran escala contra adversarios pares y casi pares, que incluye un amplio espectro de uso de la fuerza. Aunque puede ser tentador lamentar la amenaza que la IW rusa plantea a los intereses e instituciones estadounidenses en el siglo XXI, sin mencionar los de nuestros amigos y aliados, es importante recordar que hemos estado aquí antes. Como se señaló anteriormente, el legendario diplomático y catedrático George Kennan estaba completamente familiarizado con la amenaza que enfrentamos hoy, aunque las tecnologías han cambiado. Pero lo que es importante reconocer en su memorándum de 1948 sobre guerra política no es la evaluación de tal amenaza planteada por nuestros adversarios. Más bien, es el reconocimiento de que Estados Unidos debe estar dispuesto y capaz de pelear guerras políticas, así como estábamos dispuestos a pelear guerras convencionales, para asegurar nuestros intereses. Kennan escribe:

La guerra política es la aplicación lógica de la doctrina de Clausewitz en tiempo de la paz. En la definición más amplia, la guerra política es el empleo de todos los medios a las órdenes de una nación, excepto la guerra, para lograr sus objetivos nacionales. Tales operaciones son tanto abiertas como encubiertas. Van desde acciones tan abiertas como alianzas políticas, medidas económicas (como ERP [el Plan Marshall]) y propaganda “blanca” hasta operaciones tan encubiertas como apoyo clandestino a elementos extranjeros “amistosos”, guerra psicológica “negra” e incluso el fomento de resistencia clandestina en estados hostiles.⁴⁶

La receta de Kennan permanece tan válida como lo era hace 70 años. Es hora de reconocer la amenaza que la IW rusa representa para el núcleo de intereses de Estados Unidos y responder en consecuencia.

Notas

¹ “Zuckerberg: Facebook está en ‘carrera armamentista’ con Rusia”, *BBC News*, 11 Abril 2018, consultado 02 Mayo 2018, <http://www.bbc.com/news/world-us-canada-43719784>.

² Ver Mike Lundy, Rich Creed, “El Regreso del Manual de Campaña del Ejército de EEUU - FM 3-0, Operaciones”, *Military Review*, Noviembre-Diciembre 2017.

³ Morgan Chalfant, “Ex Director de la CIA: no Llamen ‘Acto de Guerra’ al Hackeo Ruso de las Elecciones”, *The Hill*, 11 Abril 2018, consultado 20 Junio 2018, <https://thehill.com/policy/cybersecurity/328344-former-cia-director-dont-call-russian-election-hacking-act-of-war>

⁴ Keir Giles, “Manual de la Guerra de Información Rusa”, Colegio Defensa de la OTAN, Noviembre 2016.

⁵ Edward Lucas y Ben Nimmo, “Guerra de información: ¿Qué es y cómo ganarla? Centro de Análisis de Políticas Europeas (CEPA) Infowar Paper Nro. 1, Noviembre 2015, 3–4.

⁶ Andrew Blake, “Michael Hayden, ex Jefe de la CIA, de Rusia: ‘Quitamos nuestro ojo del balón’”, *Washington Times*, 01 Mayo 2018.

⁷ George Kennan, “George F. Kennan Sobre la Organizando la Guerra Política” Wilson Center Digital Archive, 30 Abril 1948, consultado 13 Junio 2018, <https://digitalarchive.wilsoncenter.org/document/114320.pdf>.

⁸ Gabriel Samuels, “La OTAN pone a 300.000 tropas terrestres en ‘Alerta Alta’ porque las Tensiones con Rusia Suben”, *The Independent*, 07 Noviembre 2016.

⁹ Greg Keeley, “Combatir la Guerra de Información Rusa –en los Países Bálticos” *The Hill*, 09 Abril 2018.

¹⁰ Consejo de Jefes de Estado Mayor, Publicación Conjunta (JP) 3-13, *Operaciones de Información* (Washington, DC 27 Noviembre 2012), GL-3;

¹¹ Sophia Porotsky, “Guerra Fría 2.0: Guerra de Información Rusa”, *Revista de Seguridad Global*, 08 Febrero 2018, consultado 20 Junio 2018, <https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/>.

¹² Citado por Anne Vandermey, “Ganando Seguidores: Internet y Propaganda Estilo Guerra Fría en las Ex Repúblicas Soviéticas, *Wilson Quarterly*, Otoño 2016, consultado 20 Junio 2018, <https://wilsonquarterly.com/quarterly/>

the-lasting legacy of the cold-war/gaining-followers-the-internet-and-cold-war-style-propaganda-in-the-former-soviet-republic/.

¹³ Bruce McClintock, “La Guerra de Información Rusa: una Realidad que Necesita una Respuesta”, RAND Blog, 21 Julio 2017, consultado 20 Junio 2018, <https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html>.

¹⁴ Peter Mattis, “Contrastando las Operaciones de Influencia de China y Rusia” Guerra en las Rocas, 16 Enero 2018.

¹⁵ Maria Snegovaya, “La Guerra de Información de Putin en Ucrania: Orígenes Soviéticos de la Guerra Híbrida de Rusia”, *Instituto para el Estudio de la Guerra*, Septiembre 2015, 10.

¹⁶ Vladimir Isachenkov, “Rusia anuncia una nueva rama de militares para enfocarse en la guerra de información en medio de acusaciones de piratería”, *The Independent*, 22 Febrero 2017.

¹⁷ Dov H. Levin, “Cuando la Gran Potencia Obtiene un Voto: Los Efectos de Intervenciones Electorales de la Gran Potencia sobre los Resultados Electorales” *Estudios Internacionales Trimestralmente* 60, Nro. 2, 2016, 189-202.

¹⁸ Dustin Volz, “Gran jurado de EEUU acusa a 13 ciudadanos rusos en una investigación de intromisión electoral”, *Reuters*, 16 Febrero 2018.

¹⁹ David Patrikarakos, *Guerra en 140 Carácteres: Cómo las Redes Sociales están Reformando el Conflicto en el Siglo XXI* (Nueva York: Basic Books, 2017), 131-151.

²⁰ JB Vowell, “Maskirovka: de Rusia, con engaño”, *Real-Clear Defense*, 30 Octubre 2016.

²¹ Snegovaya, “La Guerra de Información de Putin en Ucrania”.

²² Keir Giles, “Contraerrestando las Operaciones de Información Rusas en la Era de Redes Sociales”, *Informe del Consejo de Relaciones Exteriores*, 21 Noviembre 2017.

²³ Giles, “Contraerrestando las Operaciones de Información Rusas”.

²⁴ Phillip Karber, Joshua Thibeault, “Rusia Guerra de Nueva Generación” AUSA, 20 Mayo 2016, consultado 14 Junio 2018, <https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare>.

²⁵ Lucas, “Guerra de Información”.

²⁶ McClintock, “Guerra de Información Rusa”.

²⁷ Robert Jervis, “Cooperación bajo el Dilema de la Seguridad”, *World Politics* 30, Nro. 2, 1978, 167–214.

²⁸ Snegovaya, “La Guerra de Información de Putin en Ucrania”.

²⁹ Michael Kofman, y otros, “Lecciones de las Operaciones de Rusia en Crimea y el Este de Ucrania”, *RAND*, 2017.

³⁰ Damien Sharkov, “Rusia Anuncia Tropas de Operaciones de Información con la Misión de ContraPropaganda. *Newsweek*, 22 Febrero 2017.

³¹ Timothy Snyder, *Sobre la tiranía: Veinte Lecciones del Siglo XX* (Nueva York: Duggan Books, 2017), 97.

³² Patrikarakos, *Guerra en 140 caracteres*, 161.

³³ Raphael Satter y Dmytro Vlasov, “Soldados de Ucrania bombardeados por textos de ‘propaganda puntual’ ”, *Associated Press*, 11 Mayo 2017, consultado 14 Junio 2018, <https://apnews.com/9a564a5f64e847d1a50938035ea64b8f> Oleksandar Golovko, Ukrainian Frontline: Cyber + EW + Psyops” PowerPoint brief (Kyiv, Ukraine: General Staff of the Armed Forces, 2018).

³⁴ Satter y Vlasov, “Soldados de Ucrania bombardeados por textos de ‘propaganda puntual’ ”.

³⁵ Golovko, “Primera Línea de Ucrania”.

³⁶ Thomas Grove, Julia E. Barnes y Drew Hinshaw, “Rusia Ataca Teléfonos Inteligentes de Soldados de la OTAN, Dicen Funcionarios Occidentales: “ *The Wall Street Journal* , 04 Octubre 2017, consultado 10 Mayo 2018, consultado 14 Junio 2018, <https://www.wsj.com/articles/russia-targets-soldier-smartphones-western-officials-say-1507109402>.

³⁷ Entrevista con oficiales militares en Hohenfels, Alemania, 08 Mayo 2018.

³⁸ Andy Greenberg, “Cómo una Nación Entera se Convirtió en el Laboratorio de Pruebas de Rusia para Ciberguerra”, *Wired*, junio de 2017. 10/3/2020

³⁹ Leonid Peisakhin, Arturas Rozenas, “¿Cuándo Funciona la Propaganda Rusa –y cuándo es contraproducente? Esto es lo que Encontramos”, *Washington Post*, 03 Abril 2018.

⁴⁰ La Ley Magnitsky de 2012, nombrada en honor a Sergei Magnitsky, un contador fiscal ruso que murió en prisión bajo circunstancias misteriosas, castiga a funcionarios rusos que se cree fueron responsables de su muerte.

⁴¹ Peter Grier y Harry Bruinius, “Con la Estrategia de Seguridad Nacional, Trump marca el comienzo de una nueva era del Arte de Gobernar”, *Christian*

Science Monitor, 18 Diciembre 2017, consultado 20 Junio 2018, <https://www.csmonitor.com/USA/Politics/2017/1218/With-National-Security-Strategy-Trump-ushers-new-era-of-statecraft>

⁴² Nadia Schadlow, “Creando la Estrategia de Seguridad Nacional”, discurso pronunciado al Instituto de la Guerra Moderna en la Academia Militar de los Estados Unidos en West Point, 02 Febrero 2018, consultado 20 Junio 2018, <https://mwi.usma.edu/event/writing-president-trumps-estrategia-de-seguridad-nacional-dr-nadia-schadlow/>.

⁴³ EEUU gastó \$ 49 mil millones en 2015; ver James McBride, “Cómo EEUU Gasta su Ayuda Exterior”, Consejo de Relaciones Exteriores, 11 Abril 2017, consultado 14 Junio 2018, [https://www.cfr.org/backgrounder/how-does-us-spendsuayda-exterior](https://www.cfr.org/backgrounder/how-does-us-spendsuayuda-exterior).

⁴⁴ Emilio J. Iasiello, “Operaciones de Información Mejoradas de Rusia: de Georgia a Crimea”, *Parámetros* 47, Nro. 2, 2017, 62–63.

⁴⁵ Giles, “Manual de la Guerra de Información Rusa”.

⁴⁶ George Kennan, “George F. Kennan Sobre la Organizando la Guerra Política” Wilson Center Digital Archive, 30 Abril 1948, consultado 13 Junio 2018, <https://digitalarchive.wilsoncenter.org/document/114320.pdf>.