Los métodos y las acciones de Rusia contra Estados Unidos y la OTAN

Mayor Collins Devon Cockrell, Ejército de EUA

Rusia ha intentado transformar de forma radical el orden europeo pos Guerra Fría mediante una agresiva campaña de guerra de información en años recientes—tanto es así que en la Declaración de Postura del Comando Europeo de Estados Unidos de 2017 se identificó a Rusia como la amenaza principal y se señaló que «Rusia busca debilitar el sistema internacional y desacreditar a aquellos en Occidente que lo han creado»[1]. En enero de 2017, el general retirado James Mattis, en aquel momento candidato para secretario de Defensa de Estados Unidos, declaró que Rusia era la principal amenaza para Estados Unidos y estaba realizando esfuerzos constantemente para «romper la Alianza Atlántica»[2]. En el discurso que dio en Múnich en 2007, el presidente Vladimir Putin declaró que aplicaría una política exterior que no reconocería un sistema unipolar encabezado por Estados Unidos[3]. Putin declaró públicamente que Occidente, específicamente Estados Unidos, estaba intentando convertir a Rusia en un Estado vasallo débil y estaba impidiendo que Rusia heredara el papel de equilibrador global que una vez desempeñó la Unión Soviética[4]. Esta visión del mundo conflictiva e hiperbólica de la élite gobernante rusa se puede resumir en los comentarios realizados por Andrey Krutskikh, un asesor principal del presidente Putin, en una conferencia en Moscú en febrero de 2017:

> «Ustedes piensan que vivimos en 2016. No, estamos viviendo en 1948. ¿Saben por qué? Porque en 1949, la Unión Soviética realizaba su primera prueba nuclear. Y si hasta ese momento la Unión Soviética había intentado llegar a un acuerdo con [el presidente Harry] Truman para prohibir las armas nucleares, y los estadounidenses no nos tomaban en serio, en 1949 todo cambió y empezaron a dialogar con nosotros en pie de igualdad»[5].

Como reflejo directo de esto, Rusia está interviniendo en los sistemas políticos de toda Europa para desestabilizar los Estados democráticos establecidos y los recién formados. El objetivo de Putin es la restauración de la «Gran Rusia»[6]. En este artículo la doctrina de operaciones de información (IO) de tanto la OTAN como Estados Unidos es resumida y comparada con el análisis actual de los conceptos rusos sobre la guerra de información[7]. Este resumen pretende orientar a los lectores sobre importantes distinciones en la doctrina, la capacidad y el propósito para que los actores occidentales tengan una comprensión clara de la cual puedan tomar decisiones.

La doctrina estadounidense define operaciones de información como «el empleo integrado, durante las operaciones militares, de capacidades relacionadas a la información (IRC) junto con otras líneas de operaciones para influenciar, desestabilizar, degradar o usurpar el proceso de toma de decisiones del adversario, real o potencial, mientras protegemos el nuestro»[8]. Las IRC comprenden las operaciones militares de apoyo a la

información (MISO), las operaciones del ciberespacio, la decepción militar, las operaciones cívico-militares y los asuntos públicos[9]. Como función coordinadora en el campo de la difusión y elaboración de información, las IO son un componente crítico de todas las operaciones ofensivas, defensivas y de estabilidad. En la doctrina estadounidense, las fuerzas de operaciones psicológicas (PSYOP) son las encargadas del esfuerzo principal de influir en el público objetivo extranjero mediante las MISO. Según la doctrina, las fuerzas de PSYOP tiene la tarea de:

> «… elaborar y transmitir mensajes, definir acciones para influir en grupos extranjeros determinados y promover temas que cambiaran las actitudes y comportamientos de esos grupos. Las MISO también pueden degradar el poder de combate del enemigo, reducir la interferencia civil, minimizar los daños colaterales y aumentar el apoyo de la población con respecto a las operaciones»[10].

Los programas y las acciones de IO adoptados por Estados Unidos y Occidente para hacerle frente a las acciones rusas han aumentado desde la anexión de Crimea. Los Estados miembros de la OTAN han reconocido la amenaza cada vez mayor de los esfuerzos rusos para influir en la política interna y exacerbar las divisiones. Sin embargo, estos programas de Occidente son tan efectivos como las actividades rusas porque no tienen la capacidad para influir y corromper de Rusia. Una parte esencial de la estrategia de Estados Unidos y la OTAN es apoyar y desarrollar organizaciones que puedan analizar amenazas en el dominio de la información y hacer recomendaciones a las coaliciones, las Fuerzas Armadas y los Gobiernos occidentales. Por ejemplo, en 2014, la OTAN aprobó la creación del Centro de Excelencia de Comunicaciones Estratégicas de la OTAN (NATO StratCom COE) en Riga, Letonia[11]. Esta organización está encargada de contrarrestar el extremismo violento y la influencia hostil, especialmente en la región de los Estados bálticos. El Centro lleva a cabo un análisis exhaustivo de las actividades rusas en todo el continente. Aunque no forma parte de la estructura de mando de la OTAN, el NATO StratCom COE sirve como un tipo de laboratorio de ideas de la OTAN encargado de «contribuir a los procesos de comunicación de la Alianza proporcionando análisis exhaustivos, asesoramiento oportuno y apoyo práctico»[12]. Su tarea principal es comprender el extremismo y las influencias hostiles, como también apoyar el plan de comunicaciones estratégicas del Comité Militar de la OTAN y la doctrina de la Alianza. Keir Giles, uno de los investigadores más prominentes que ha trabajado para diferentes organizaciones de la OTAN, también ha escrito documentos de análisis oficiales para la OTAN, como el «Handbook of Russian Information Warfare», en 2016[13]. El NATO StratCom COE es una manera eficiente de apoyar a los miembros de la OTAN sobre temas como el extremismo y las acciones rusas contra Europa.

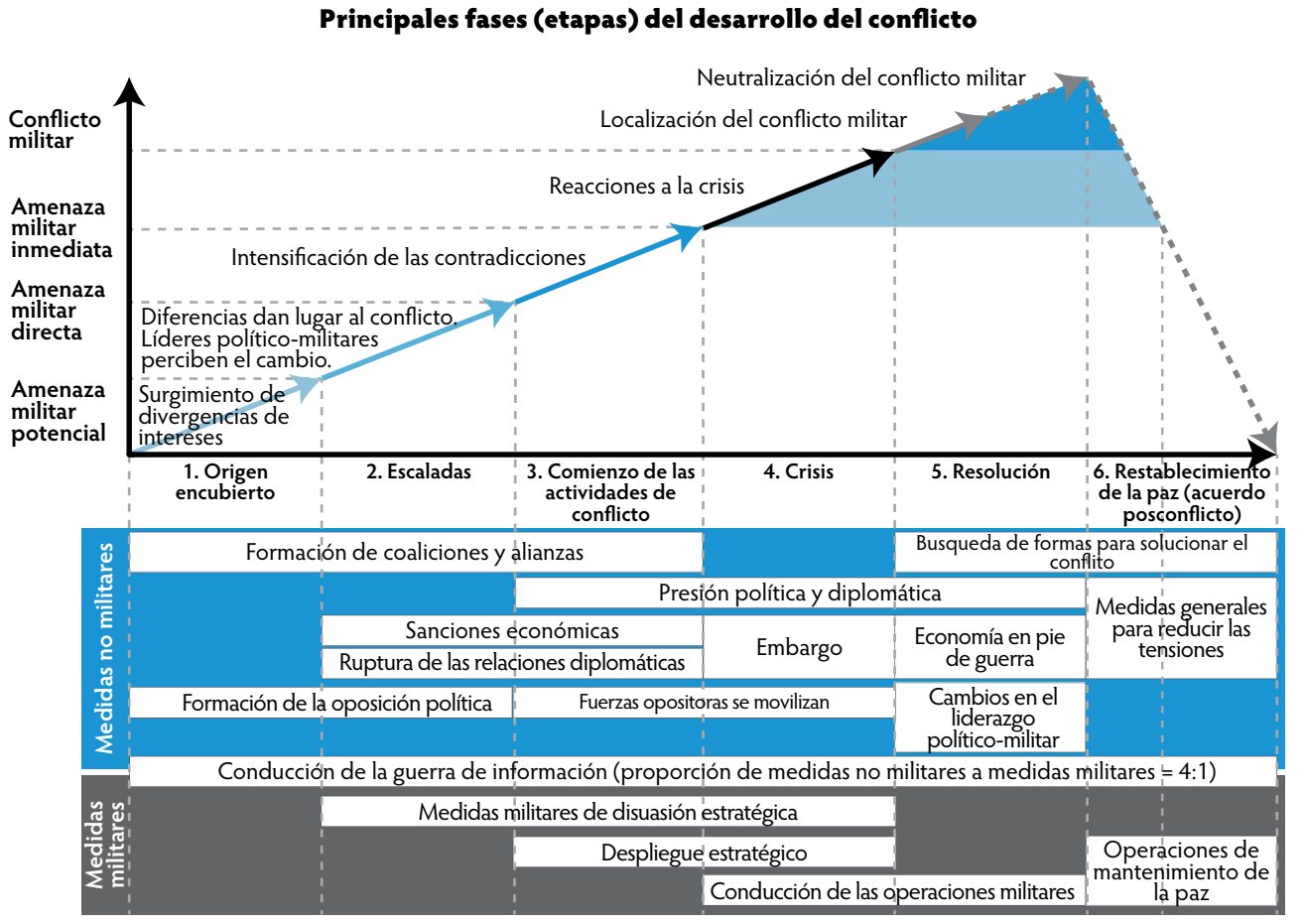
La doctrina sobre las PSYOP de la OTAN está en consonancia con la doctrina estadounidense sobre las MISO. Ambas emplean términos similares para conceptos clave, como análisis del público objetivo, el proceso analítico por el cual la población o grupo más útil se identifica para conseguir un cambio de comportamiento en apoyo de los requerimientos de la misión y los objetivos del comandante[14]. Los límites de la capacidad de la OTAN para responder a las acciones rusas no se deben a la falta de doctrina, sino a cómo veintinueve Estados miembros coordinan una respuesta unificada y oportuna en un ambiente de información que cambia rápidamente. Fuera de la declaración de hostilidades contra miembros de la OTAN, los procesos para la acción de los Estados miembros mediante los comités militares que coordinan las actividades no pueden igualar la acción unificada de la dictadura rusa. Los Estados miembros de la OTAN han reconocido la

El mayor Collins Devon Cockrell, Ejército de EUA, sirve como el S-3 (oficial de operaciones) del 7.º Grupo de Operaciones Psicológicas, en Mountain View, California. Obtuvo una maestría en Ciencias Políticas en la Universidad de Arkansas y una maestría en Ciencias y Artes Militares (MMAS) en la Escuela de Comando y Estado Mayor General (CGSC), en Fort Leavenworth, Kansas. Se ha desempeñado como director e instructor del Curso de Calificación (Q Course) de Oficial de Operaciones Psicológicas en la Escuela y Centro de Guerra Especial *John F. Kennedy* (USAJFKSWCS), en Fort Bragg, Carolina del Norte. Entre sus destinos previos se encuentran períodos de servicio en Corea y misiones en Irak en 2004 como ingeniero y en 2009 como comandante de un destacamento de operaciones psicológicas.

amenaza cada vez mayor de los esfuerzos rusos para influir en su política interna y exacerbar las divisiones. Como declaró Constanze Stelzenmüller, de la Institución Brookings, ante el Comité de Inteligencia del Senado en junio de 2017, Rusia quiere con su guerra de información «desestabilizar el proyecto europeo desde el interior y desmantelar décadas de progreso hacia la construcción de una Europa democrática unida, libre y en paz»[15]. En abril de 2017, nueve Estados miembros de la OTAN y la Unión Europea acordaron crear una organización conjunta en Helsinki para cooperar activamente en «la lucha contra la guerra híbrida»[16]. En Estados Unidos, la Ley de Autorización de Defensa Nacional (NDAA) vigente autoriza el establecimiento de un «Fondo para Combatir la Influencia Rusa», el cual dispone de 80 millones de dólares, para «apoyar las organizaciones de la sociedad civil y otras entidades»[17]. Estos fondos han generado polémica en el Gobierno ya que el Departamento de Estado se negó hasta agosto de 2017 a proporcionar un plan sobre cómo el Centro de Participación Global, un centro encargado de la lucha contra la desinformación, emplearía los fondos[18].

La foto de portada del primer número de *Robotrolling*, una publicación del Centro de Excelencia de Comunicaciones Estratégicas de la OTAN, representa el auge de la automatización en los medios sociales. El Centro de Excelencia de Comunicaciones Estratégicas de la OTAN es una de las muchas instituciones dedicadas a la recolección y el análisis de información para ayudar a los miembros de la OTAN con su complejo proceso de toma de decisiones. (Gráfico de *Robotrolling* 1 [2017], consultado el 8 de septiembre de 2017, http://www.stratcomcoe.org/robotrolling-20171)

De estas y otras maneras, los Estados europeos aliados y de la OTAN están coordinando sus respuestas para el conflicto actual con Rusia en el dominio de la información. Sin embargo, la ejecución de las estrategias de las coaliciones es mucho más



(Gráfico del Departamento de Análisis de Seguridad Nacional, *«Little Green Men»: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*, Assessing Revolutionary and Insurgent Strategies Study (borrador no confidencial, Fort Bragg, Carolina del Norte: Comando de Operaciones Especiales del Ejército de EUA), pág. 18)

Figura 1. El papel de los métodos no militares en la resolución de conflictos entre Estados

complicada que las de un actor autoritario y unificado como Rusia. Además, el elemento esencial de tanto la doctrina de influencia como las PSYOP de Estados Unidos y la OTAN se centra en la difusión de mensajes persuasivos basados en información veraz para influir en el público objetivo. Como se indica en el manual de la OTAN: «Las PSYOP se deben basar en información verdadera. Emplear información falsa es contraproducente para la credibilidad y el éxito de las PSYOP a largo plazo»[19]. Esto es tanto una ventaja como una limitación. Es una ventaja debido a la credibilidad y la fuerza que transmite, pero es una limitación porque Rusia no tiene tales restricciones para sus campañas de influencia.

Rusia considera que este tipo de guerra se puede llevar a cabo antes de que las hostilidades hayan comenzado. En la monografía «Handbook of Russian Information Warfare» para el Colegio de Defensa de la OTAN (NDC), Keir Giles cita:

> «Los rusos al comienzo emplean la información de forma clandestina y después a través de seis fases de guerra hasta alcanzar la victoria. En cada fase se realizan acciones de información contra el objetivo, incluida la fase clandestina, en tiempos de paz y de guerra. Nuestra doctrina no nos permite hacer lo mismo hasta que el combate haya comenzado»[20].

El presidente Putin y sus estrategas han basado sus acciones en lo que en Rusia llaman «guerra de nueva generación» (NGW). En la Doctrina militar de la Federación de Rusia, publicada por primera vez en 2000, los «rusos reconocieron que sus Fuerzas Armadas necesitaban operar en el "espacio de la

información" y las "amenazas de información" que el Ejercito debía enfrentar»[21]. Con respecto a Estados Unidos y la OTAN, guerra híbrida, junto con guerra de información, son los términos que analistas civiles y militares emplean con más frecuencia para describir las actividades rusas. En la doctrina estadounidense se declara que «una *amenaza híbrida* es una combinación dinámica y diversa de fuerzas regulares, fuerzas irregulares y/o elementos criminales unificados para lograr efectos mutuamente beneficiosos»[22]. Esta definición se corresponde con la concepción rusa de guerra de nueva generación. Más importante aún, para los rusos, este tipo de guerra es diferente de la guerra asimétrica ya que esta última es la herramienta de un oponente intrínsecamente débil contra uno más fuerte. Rusia invierte este concepto cuando se trata de los antiguos Estados soviéticos. Estos métodos híbridos son empleados contra Estados más débiles o iguales para lograr objetivos militares o de política exterior. El motivo subyacente de Rusia es obtener resultados políticos decisivos sin recurrir, o hacerlo escasamente, al poder militar, pero está lista para emplearlo de forma abrumadora de ser necesario[23]. Es por ello que una alianza como la OTAN se encuentra en desventaja, no solo porque es una estructura de coalición, sino porque estos métodos asimétricos o híbridos son más difíciles de clasificar como un «ataque» verdadero contra un Estado miembro.

Desde 2012, la estrategia militar rusa se ha centrado en la doctrina Guerásimov, la cual se basa en una serie de discursos y declaraciones del jefe de Estado Mayor General de las Fuerzas Armadas de Rusia, general Valeri Guerásimov. Las ideas del general Guerásimov son una síntesis de un tipo de guerra no convencional o guerra asimétrica. A través de este método se busca crear una «oposición interna» viable en un Estado[24]. Charles K. Bartles ilustra claramente este proceso de fases de guerra irregular rusa que aparece en la Figura 1 en el artículo de 2016 titulado «Getting Gerasimov Right»[25]. El proceso también fue abordado en un documento del Comando de Operaciones Especiales (SOCOM) de 2016 titulado *«Little Green Men»: A Primer on Modern Russian Unconventional Warfare*[26].

Guerásimov declaró:

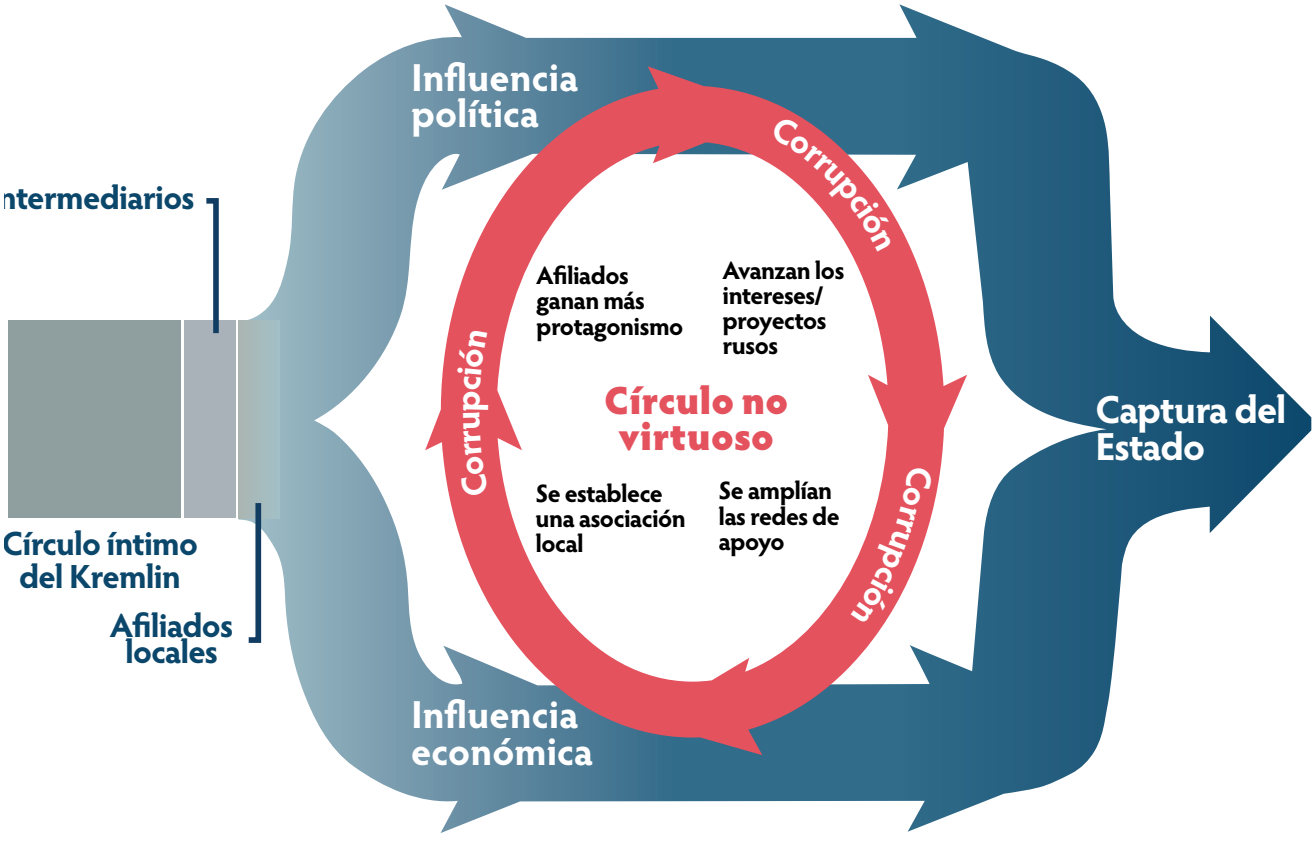
> «Las "reglas de la guerra" han cambiado. El papel de los medios no militares para alcanzar objetivos políticos y estratégicos ha aumentado, y en muchos casos, ha sobrepasado el poder de las armas en efectividad»[27].

Cuando Guerásimov menciona la coordinación de factores económicos, diplomáticos y políticos junto con la fuerza militar, recuerda de cierta manera la «guerra política», un término antiguo que ya definía estas acciones. El término tuvo su origen en la Segunda Guerra Mundial, pero se está empleando nuevamente en la comunidad de operaciones especiales estadounidense[28]. La estrategia militar rusa tiene como objetivo desestabilizar rápidamente países estables mediante acciones no militares[29]. Los métodos rusos se centran en localizar y explotar las debilidades y divisiones internas de un país para socavar su sociedad. Estas acciones pueden incluir «el empleo del potencial de protesta de la población, las fuerzas de operaciones especiales y medidas militares y de guerra de información encubiertas»[30].

En *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* se describe vívidamente cómo la influencia rusa, junto con redes criminales de origen ruso, pueden aumentar la corrupción en una sociedad y actuar como una enfermedad debilitante; como «un virus que ataca a las democracias»[31]. Rusia utiliza su poder económico y sus métodos corruptos para influir en los responsables políticos y las instituciones políticas y económicas de toda Europa. El objetivo de esta influencia encubierta sobre funcionarios electos, hombres de negocio, medios de comunicación, partidos políticos y movimientos políticos es «hacer que las políticas de la región, mediante la coacción y la corrupción, favorezcan a Rusia y no a la unidad europea»[32]. La Figura 2 de *The Kremlin Playbook* ilustra este proceso.

Las actividades que Rusia ha intentado llevar a cabo en los últimos cinco años en Europa no son nuevas. Sin embargo, la aplicación innovadora de medios tecnológicos para difundir sus mensajes ha hecho estas actividades mucho más efectivas que los intentos anteriores. La doctrina y los métodos de influencia rusos ya eran empleados antes de la Segunda Guerra Mundial:

> «La teoría rusa sobre la guerra de información moderna se deriva directamente de la *spetspropaganda*, una asignatura de fuertes lazos con la ideología marxista-leninista que se impartió por primera vez en el Instituto Militar de Lenguas Extranjeras de Moscú en 1942»[33].



(Gráfico de Heather Conley, James Mina, Rusland Stefanov y Martin Vladimov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Centro de Estudios Estratégicos e Internacionales (CSIS), 2016), pág. 3, consultado el 18 de julio de 2017, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf)

Figura 2. Canales de influencia rusa

La guerra de información actual que llevan a cabo los rusos es una actualización bien ejecutada de estos métodos antiguos. Estas tácticas antiguas se centran en dos elementos principales: *medidas activas* y *control reflexivo*. Las medidas activas son esfuerzos para influenciar, socavar, desestabilizar y desacreditar países específicos, sus instituciones y sus organizaciones no gubernamentales[34]. El control reflexivo es similar a lo que el Departamento de Defensa estadounidense describe como decepción militar y operaciones psicológicas. Sin embargo, esta actividad no requiere información veraz. En el artículo que escribió en 2013 para *Russian Military Strategy*, el analista de asuntos rusos Timothy Thomas señala que el objetivo del control reflexivo es manipular y confundir al responsable político de una organización específica para paralizar «la actividad de inteligencia del adversario»[35]. En el «Handbook of Russian Information Warfare», el control reflexivo se define como la intención de manipular el proceso de toma de decisiones de una organización específica «alterando factores clave sobre la percepción del mundo del adversario [...] y haciendo que escoja acciones que son más ventajosas para los objetivos rusos»[36]. El Estado Mayor General ruso interpreta la doctrina de la siguiente manera:

> «Las guerras se solucionarán mediante una combinación eficaz de medidas militares, no militares y no violentas especiales que se implementarán a través de una variedad de formas y métodos y una mezcla de medidas políticas, económicas, de información, tecnológicas y medioambientales que resultan de la superioridad de información»[37].

Jolanta Darczewksa, un escritor polaco, también sostiene que la guerra de información rusa es un reflejo de las prácticas soviéticas:

> «Las suposiciones doctrinales sobre la guerra de información no demuestran tanto un cambio muy marcado en la teoría de su conducción (los cambios están relacionados

> principalmente con la forma de su descripción y no el contenido), sino un aferramiento a los métodos antiguos (sabotaje, tácticas de diversión, desinformación, terrorismo de Estado, manipulación, propaganda agresiva y explotación del potencial de protesta de la población local)»[38].

Los métodos rusos actuales son mucho más avanzados que los que se emplearon contra Georgia en 2008, en particular el empleo de los medios sociales con objetivos específicos. En el documento *Social Media as a Tool of Hybrid Warfare*, el Centro de Comunicaciones Estratégicas de la OTAN señala que existen «troles híbridos» que operan «en el contexto de una determinada agenda militar o política»[39]. El Gobierno ruso emplea sitios web falsos que aparentan ser fuentes de información independientes. Estos sitios falsos (*sockpuppets*) que actúan como agregadores de noticias han sido especialmente efectivos para influenciar el público fuera de Rusia en operaciones como las que se llevaron a cabo en Crimea. Darczewska señala que en 2014, el profesor Igor Panarin, influyente teórico de la guerra de información y el nacionalismo extremo ruso, y en aquel entonces miembro de la Academia Diplomática del Ministerio de Relaciones Exteriores de la Federación de Rusia, describió las acciones contra Ucrania durante la anexión de Crimea como «guerra de información defensiva» ejecutada como una campaña coordinada y planifica que fue autorizada y dirigida por el propio Putin[40].

Como parte importante del movimiento nacionalista ruso y un recurso útil de influencia rusa, los rusos que viven fuera de Rusia han sido identificados y reclutados con para que actúen como agentes de influencia, como compatriotas «que viven en el extranjero». Puesto que Rusia considera que los que se identifican como rusos tienen un vínculo legal con la patria, el estatus de compatriota les atribuye derechos más allá de la ciudadanía[41]. Rusia emplea esta red de personas de origen ruso y sus simpatizantes para ejercer presión e influir en Estados específicos. Tanto los compatriotas no criminales como los criminales con frecuencia son empleados como «grupos asociados» a favor de los intereses rusos. En ocasiones, el propósito de estos individuos es dar la impresión de que las acciones rusas tienen el apoyo local. Pueden servir como testigos directos de acontecimientos y apoyar la narrativa de una amenaza existencial contra las personas de origen ruso en los Estados bálticos, Ucrania y Georgia. Entre estos grupos asociados figuran redes criminales, organizaciones fraternales de la lengua rusa, asociaciones de la Iglesia ortodoxa rusa y grupos paramilitares como el club de moteros *Lobos de la Noche*[42].

En octubre de 2016, Rusia organizó un violento golpe de Estado en Montenegro para impedir que se llevara a cabo una votación en la que se determinaría si el país solicitaría pertenecer a la OTAN[43]. En los Estados bálticos, las fuerzas rusas cuidadosamente emplearon la intimidación y organizaron actos de violencia contra la población rusa mientras retrataban a los efectivos de la OTAN en los medios de comunicación como violadores y amotinadores. Por otro lado, los soldados de la OTAN que se encuentran cumpliendo misión han recibido amenazas contra sus familiares a través de medios sociales por parte de agentes rusos[44].

No hace mucho, Rusia atacó a soldados ucranianos individualmente con mensajes de texto durante los combates que tuvieron lugar en la insurgencia respaldada por los rusos en las provincias orientales de Ucrania[45]. En las elecciones presidenciales francesas en mayo de 2017, Rusia hizo un esfuerzo masivo para que la candidata de la extrema derecha, Marine Le Pen, ganara, incluso con apoyo financiero directo en forma de préstamos multimillonarios a su Frente Nacional[46]. El esfuerzo en los medios sociales incluía el empleo de «Twitter bots» o «amplificadores activos» rusos, los cuales eran extremadamente dinámicos y difundían mensajes contra Macron y a favor de Le Pen. Sin embargo, estos bots ahora se han centrado en las elecciones de septiembre de 2017 para atacar a la canciller Angela Merkel y para apoyar a los candidatos de la extrema derecha alemana, como se documenta en la investigación en línea realizada por el Laboratorio de Investigación Forense Digital (DFRLab) del Consejo del Atlántico[47]. Stelzenmüller también señala que el equivalente alemán del FBI ha declarado que «los servicios de inteligencia rusos también han "intentado influir en la opinión pública y las autoridades decisorias en Alemania"»[48]. Los métodos rusos incluyen el respaldo a partidos políticos de derecha, el empleo de rusos étnicos en Alemania como agentes y el apoyo de amplificadores de mensajes automáticos en varias plataformas de medios de comunicación. Como se puede ver con estos y otros sucesos, las técnicas de guerra de información rusa son sofisticadas y multifacéticas[49].

Este artículo es solo una breve discusión de los métodos y las doctrinas de información de Rusia y Occidente. Mediante el mismo se intenta introducir al lector a un rápido y creciente acervo de documentos de investigación de fuente abierta que aborda la amenaza significativa de las acciones rusas contra los aliados estadounidenses y las partes que han firmado convenios con Estados Unidos. Queda claro que las acciones y la agresión rusa contra Estados Unidos y sus aliados no van a disminuir. Las acciones rusas en la actualidad tienen como objetivo las próximas elecciones alemanas y los miembros de la OTAN de Europa central. Rusia continuará llevando a cabo acciones sincronizadas por toda Europa. Instituciones más fuertes, campañas de respuestas más agresivas y una acción unificada más eficiente en representación de los intereses de Estados Unidos serán esenciales para contrarrestar esta agresión rusa. ■

Notas

1. «U.S. European Command Posture 2017: Posture Statement of General Curtis M. Scaparroti, Commander, U.S. European Command February 25, 2017», sitio web del Comando Europeo de Estados Unidos (EUCOM), 23 de marzo de 2017, consultado el 18 de agosto de 2017, http://www.eucom.mil/mission/eucom-2017-posture-statement.

2. Missy Ryan y Dan Lamothe, «Placing Russia First among Threats, Defense Nominee Warns of Kremlin Attempts to "Break" NATO», *Washington Post* en línea, 12 de enero de 2017, consultado el 14 de julio de 2017, https://www.washingtonpost.com/world/national-security/senate-set-to-question-trumps-pentagon-pick-veteran-marine-gen-james-mattis/2017/01/11/b3c6946a-d816-11e6-9a36-1d296534b31e_story.html?utm_term=.824924803d00.

3. Maria Snegovaya, *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare* (Washington, DC: Instituto para el Estudio de la Guerra (ISW), septiembre de 2015), pág. 9.

4. Katri Pynnöniemi, «The Metanarratives of Russian Strategic Deception», en *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*, FIIA [Instituto Finlandés de Asuntos Internacionales] Report 45, eds. Katri Pynnöniemi y András Rácz (Helsinki: FIIA, 2016), pág. 97.

5. David Ignatius, «Russia's Radical New Strategy for Information Warfare», *Washington Post* en línea, 18 de enero de 2017, consultado el 13 septiembre de 2017, https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/?utm_term=.492f34e18be9.

6. Centro de Excelencia de Comunicaciones Estratégicas de la OTAN (NATO StratCom COE), *Analysis of Russia's Information Campaign against Ukraine: Examining Non-Military Aspects of the Crisis in Ukraine from a Strategic Communications Perspectives* (Riga, Letonia: NATO StratCom COE, 2015), pág. 15, consultado el 20 de julio de 2017, http://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine.

7. Este artículo es una adaptación de una sección de la tesis que el autor completó para obtener una maestría en Ciencias y Artes Militares (MMAS) en la Escuela de Comando y Estado Mayor General (CGSC). Collins D. Cockrell, «Gray Zone Warfare: German and Russian Political Warfare 1935-1939 and 2014» (tesis, Fort Leavenworth, Kansas: CGSC, 2017).

8. Publicación Conjunta (JP) 3-13, *Operaciones de información* (Washington, DC: Oficina de Publicaciones del Gobierno (GPO), 2014), pág. ix.

9. *Ibíd.*, pág. II-4. Las capacidades relacionadas con la información (IRC) «son herramientas, técnicas o actividades que afectan cualquiera de las tres dimensiones del ambiente de información. Afectan la habilidad del público objetivo para recolectar, procesar o difundir información antes y después de tomar decisiones. El público objetivo es el individuo o grupo sobre el que se quiere influir.

10. JP 3-13.2, *Operaciones militares de apoyo a la información* (Washington, DC: U.S. GPO, 21 de noviembre de 2014), pág. vii. La JP 3-13.2 está bajo revisión.

11. Para más información sobre el Centro de Excelencia de Comunicaciones Estratégicas de la OTAN, visite: http://www.stratcomcoe.org/about-us.

12. *Ibíd.*

13. Keir Giles, «Handbook of Russian Information Warfare», (NATO Defense College Fellowship Monograph Series 9, Roma, Italia: Colegio de Defensa de la OTAN, noviembre de 2016).

14. Doctrina Conjunta Aliada (AJP) 3.10.1, *Doctrina conjunta aliada para las operaciones psicológicas* (Bruselas: Oficina OTAN de Normalización (NSO), septiembre de 2014), pág 1-3.

15. Constanze Stelzenmüller, «The Impact of Russian Interference on Germany's 2017 Elections», 28 de junio de 2017, consultado el 5 de septiembre de 2017, https://www.brookings.edu/testimonies/the-impact-of-russian-interference-on-germanys-2017-elections/.

16. «NATO Welcomes Opening of European Centre for Countering Hybrid Threats», sitio web de la OTAN, 11 de abril de 2017, consultado el 14 de julio de 2017, http://www.nato.int/cps/en/natohq/news_143143.htm?utm_source=twitter&utm_medium=press&utm_campaign=20170411-hybrid.

17 «In Massive Spending Bill, U.S. Lawmakers Back Several Measures Targeting Russia», Radio Europa Libre/Radio Libertad, 4 de mayo de 2017, consultado el 16 de agosto de 2017, https://www.rferl.org/a/us-spending-bill-government-running-senate-trump/28468643.html.

18. Nahal Toosi, «Tillerson Moves toward Accepting Funding for Fighting Russian Propaganda», *Politico* en línea, 31 de agosto de 2017, consultado el 5 de septiembre de 2017, http://www.politico.com/story/2017/08/31/rex-tillerson-funding-russian-propaganda-242224.

19. Doctrina Conjunta Aliada (AJP) 3.10.1, *Doctrina conjunta aliada para las operaciones psicológicas*, pág. 1-6.

20. Giles, «Handbook of Russian Information Warfare», pág. 11.

21. Jolanta Darczewska, «Russia's Armed Forces on the Information War Front: Strategic Documents», Estudios del Centro de Estudios Orientales (OSW) nro. 57 (Varsovia, Polonia: OSW, junio de 2016), pág. 8. Para una traducción al inglés de la doctrina rusa actual, véase «The Military Doctrine of the Russian Federation Approved by Russian Federation Presidential Edict on 5 February 2010», sitio web de The School of Russian and Asian Studies (SRAS), 20 de febrero de 2010, consultado el 17 de julio de 2017, http://www.sras.org/military_doctrine_russian_federation_2010.

22. Circular de Entrenamiento (TC) 7-100, *Amenaza híbrida* (Washington, DC: U.S. GPO, noviembre de 2010), pág. V.

23. Diego A. Ruiz Palmer, «Back to the Future? Russia's Hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons», (trabajo de investigación nro. 120, Roma, Italia: Colegio de Defensa de la OTAN, octubre de 2015), pág. 2.

24. Departamento de Análisis de Seguridad Nacional, *«Little Green Men»: A Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014, Assessing Revolutionary and Insurgent Strategies Study* (borrador no confidencial, Fort Bragg, Carolina del Norte: Comando de Operaciones Especiales del Ejército de EUA (SOCOM)), pág. 27. Véase también «SOF Support to Political Warfare White Paper», (Fort Bragg, Carolina del Norte: SOCOM, 10 de marzo de 2015), pág. 201, consultado el 18 de julio de 2017, http://www.soc.mil/swcs/ProjectGray/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20(10MAR2015)%20%20%20.pdf.

25. Charles K. Bartles, «Getting Gerasimov Right», *Military Review* 96, nro. 1 (enero-febrero 2016), pág. 35.

26. Departamento de Análisis de Seguridad Nacional, «Little Green Men», pág. 27.

27. Valeri Guerásimov, «The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations», *Military Review* 96, nro. 1 (enero-febrero 2016): pág. 24. El artículo de Guerásimov fue publicado originalmente en *Voyenno-Promyshlennyi Kurier*, 27 de febrero de 2013.

28. «SOF Support to Political Warfare White Paper».

29. Jolanta Darczewska, «The Devil is in The Details: Information Warfare in the Light of Russia's Military Doctrine», OSW Point of View nro. 50 (Varsovia, Polonia: OSW, mayo de 2015), pág. 12.

30. Timothy L. Thomas, *Russian Military Strategy: Impacting 21st Century Reform and Geopolitics* (Fort Leavenworth, Kansas: Oficina de Estudios Militares Extranjeros (FMSO), 2015), págs. 238–39.

31. Heather Conley, James Mina, Rusland Stefanov, y Martin Vladimov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, DC: Centro de Estudios Estratégicos e Internacionales (CSIS), 2016), pág. 26.

32. Alina Polyakova, Marlene Laruelle, Stefan Meister y Neil Barnett, *The Kremlin's Trojan Horses*, 3.ª ed. (Washington, DC: Centro de Estudios Euroasiáticos *Dinu Patriciu*, Consejo del Atlántico, noviembre de 2016), pág. 4, consultado el 17 de julio de 2017, http://www.atlanticcouncil.org/images/publications/The_Kremlins_Trojan_Horses_web_0228_third_edition.pdf.

33. Edward Lucas y Peter Pomeranzev, *Winning the Information War: Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe* (Washington, DC: Centro de Análisis de Políticas Europeas (CEPA), agosto de 2016), pág. 6.

34. Katri Pynnöniemi, «The Conceptual and Historical Roots of Deception», en *Fog of Falsehood*, pág. 38.

35. Alexey A. Prokhozhev y Nikolay I. Turko, «The Basics of Information Warfare» (informe, Systems Analysis on the Threshold of the 21st Century: Theory and Practice Conference, Moscú, 27–29 de febrero de 1996), citado en Thomas, *Russian Military Strategy*, pág. 118.

36. Giles, «Handbook of Russian Information Warfare», pág. 19.

37. Sergey Checkinov y Sergei Bogdanov, «Forecasting the Nature and Content of Wars of the Future: Problems and Assessments», *Voennaya Mysl'*, nro. 10 (2015): págs. 44–45, citado en Giles, «Handbook of Russian Information Warfare», pág. 6.

38. Darczewska, «The Devil is in the Details», pág. 12.

39. Centro de Excelencia de Comunicaciones Estratégicas de la OTAN, *Social Media as a Tool of Hybrid Warfare* (Riga, Letonia: NATO StratCom COE, mayo de 2016), pág. 27, consultado el 20 de julio 2017, http://www.stratcomcoe.org/social-media-tool-hybrid-warfare.

40. Jolanta Darczewska, «The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study», OSW Point of View nro. 42 (Varsovia, Polonia: OSW, mayo de 2014), pág. 24.

41. Vera Zakem, Paul Sanders y Daniel Antoun, *Mobilizing Compatriots: Russia's Strategy, Tactics, and Influence in the Former Soviet Union*, CNA [Center for Naval Analyses] Occasional Paper (Arlington, Virginia: CNA, noviembre de 2015), pág. 14.

42. Orysia Lutsevych, «Agents of the Russian World: Proxy Groups in the Contested Neighbourhood», (trabajo de investigación, Londres: Chatham House, Instituto Real de Asuntos Internacionales, abril de 2016), pág. 19.

43. Milena Veselinovic y Darran Simon, «Montenegro: Russia Involved in Attempted Coup», CNN, 21 de febrero de 2017, consultado el 17 de julio de 2017, http://www.cnn.com/2017/02/21/europe/montenegro-attempted-coup-accusation/index.html.

44. Tom Porter, «British Soldiers' Latvia Brawl "Was Set Up As Part Of Russian Propaganda Sting"» *International Business Times*, 2 de noviembre de 2016, consultado el 14 de julio de 2017, https://sg.news.yahoo.com/british-soldiers-latvia-brawl-set-104233445.html.

45. Raphael Satter y Dmytro Vlasov, «Ukraine Soldiers Bombarded By "Pinpoint Propaganda" Texts», ABC News, 11 de mayo de 2017, consultado el 14 julio de 2017, http://abcnews.go.com/Technology/wireStory/sinister-text-messages-reveal-high-tech-front-ukraine-47341695.

46. Gabriel Gatehouse, «Marine Le Pen: Who's Funding France's Far Right?», BBC News, 3 de abril de 2017, consultado el 14 de julio de 2017, http://www.bbc.com/news/world-europe-39478066.

47. @DFRLab, «The Kremlin's Audience in France: Breaking Down the Amplifiers of Sputnik and RT in French», Laboratorio de Investigación Forense Digital del Consejo del Atlántico, medium.com, 14 de abril de 2017, consultado el 14 de julio de 2017, https://medium.com/dfrlab/the-kremlins-audience-in-france-884a80515f8b.

48. Steltenmuller, «The Impact of Russian Influence on Germany's 2017 Elections».

49. Snegovaya, *Putin's Information Warfare in Ukraine*, pág. 20.