El capitán Taiwan Veney (*centro*), oficial de operaciones de guerra cibernética, observa los datos de la interfaz web Kibana mientras miembros del 175º Grupo de Operaciones del Ciberespacio —(*izquierda a derecha*) capitán Adelia McClain, sargento segundo Wendell Myler, aerotécnico superior Paul Pearson y sargento segundo Thacious Freeman— analizan los archivos de registro y actualizan el número de amenazas cibernéticas el 3 de junio de 2017 en Warfield Air National Guard Base, Maryland. (Foto: J. M. Eddins Jr., Fuerza Aérea de EUA)

La ciberseguridad social

Un ámbito emergente de la seguridad nacional

Teniente coronel David M. Beskow, Ejército de Estados Unidos
Dra. Kathleen M. Carley

La ciberseguridad social es un subdominio emergente de la seguridad nacional que afectará todos los niveles de la guerra convencional y no convencional con consecuencias estratégicas. Se podría definir como «un área científica en desarrollo que utiliza la ciencia para caracterizar, entender y prever cambios impulsados por los medios cibernéticos en el comportamiento humano, la sociedad, la cultura y la política, y para construir la infraestructura cibernética necesaria que permita a la sociedad retener su carácter esencial en medio de un entorno de información cibernético que se encuentra bajo cambios y enfrenta amenazas cibernéticas sociales actuales o inminentes»[1]. La tecnología hoy en día permite a actores estatales y no estatales manipular las creencias e ideas a escala mundial y a la velocidad de algoritmos, lo cual está transformando el campo de batalla en todos los niveles de la guerra.

Aunque recientemente ha sido analizada bajo el prisma de la guerra «híbrida», la guerra de información se está convirtiendo en un fin en sí mismo. Dmitry Kiselev, coordinador de la agencia estatal rusa para noticias internacionales, declara que las «guerras de información se han convertido [...] en la principal manera de librar la guerra»[2]. La información se está empleando para fortalecer la narrativa propia y al mismo tiempo atacar, desestabilizar, distorsionar y dividir a la sociedad, la cultura y los valores de otras organizaciones o Estados rivales. Al debilitar la confianza de la comunidad internacional en las instituciones nacionales, la opinión general sobre los valores nacionales y el compromiso a ellos, un actor puede ganar la guerra antes de que esta haya empezado. De hecho, reflexionando sobre la transición de conflictos cíclicos a competencia continua, los líderes más antiguos del estado mayor ruso han declarado: «Hay guerras que no han sido declaradas y, sin embargo, ya han empezado»[3].

La información está adquiriendo cada vez más importancia como elemento de poder nacional. La estrategia a menudo es analizada mediante los elementos de poder nacional diplomático, informativo, militar y económico. La tecnología ahora permite que actores estatales y no estatales consoliden su poder en el dominio de la *información* a una escala y complejidad que por mucho tiempo fueron consideradas imposibles. Si no se controla, esta «guerra relámpago de información» en curso tendrá consecuencias estratégicas similares a las de la guerra relámpago de principios de la Segunda Guerra Mundial.

La ciberseguridad social, aunque técnica por naturaleza, difiere de la ciberseguridad tradicional. En la ciberseguridad tradicional, los humanos usan la tecnología para «hackear» la tecnología. El objetivo son los sistemas de información. En la ciberseguridad social, los humanos usan la tecnología para «hackear» a otros humanos. El objetivo son los humanos y la sociedad que los une. Esta distinción en el paradigma cibernético tradicional a veces es llamada «hackeo cognitivo». Operando en el medio cibernético para poder llegar a las masas, este tipo de guerra de información emergente aprovecha la mercadotecnia dirigida, la psicología, la persuasión, las malas políticas de tanto instituciones privadas como gubernamentales y las ciencias sociales para ejecutar operaciones de información coordinadas con fines estratégicos.

La ciberseguridad social es básicamente una ciencia social computacional multidisciplinaria. «Las teorías emergentes combinan las ciencias políticas, la sociología, las ciencias de la comunicación, las ciencias de la organización, la mercadotecnia, la lingüística, la

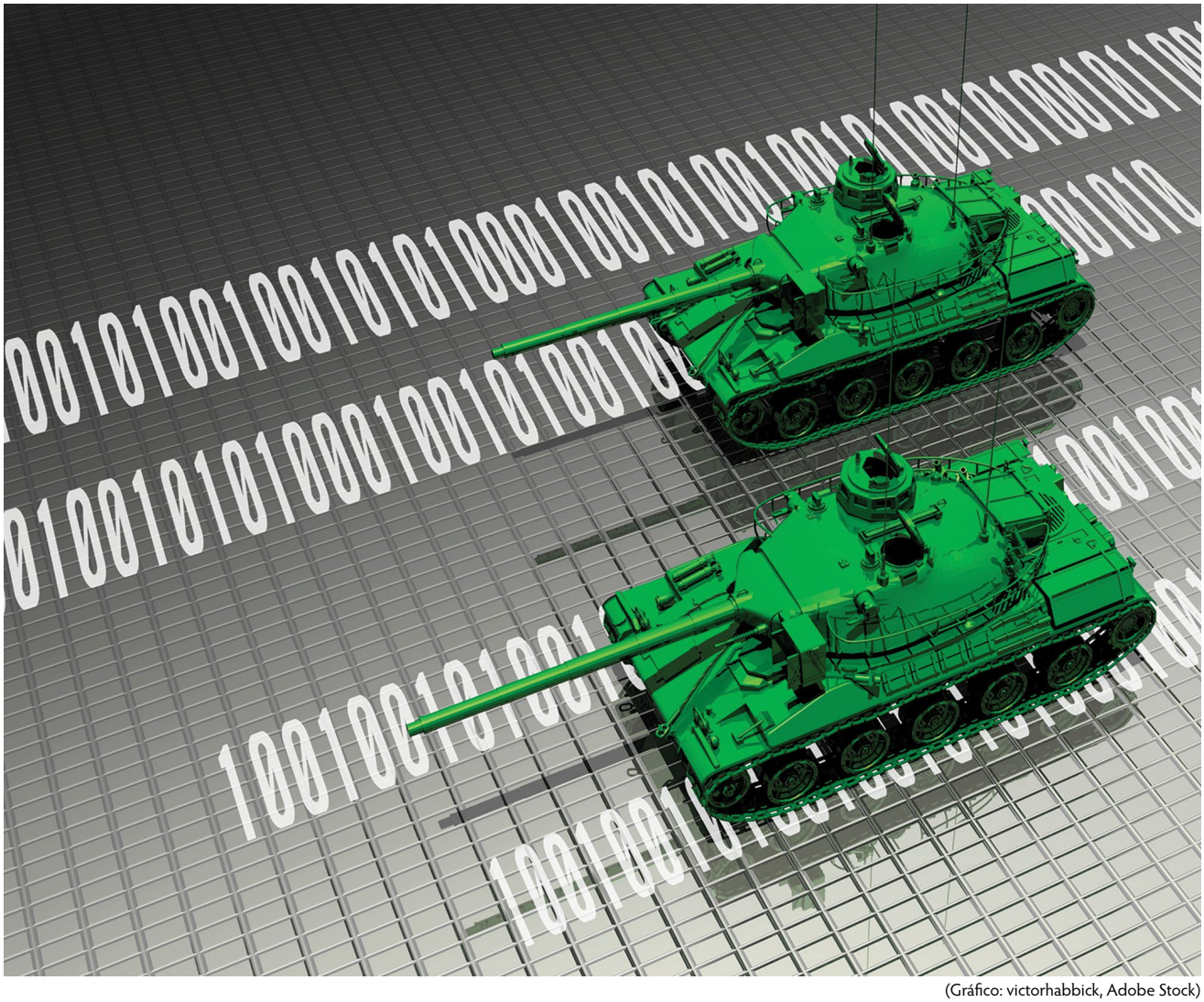
El teniente coronel David Beskow, Ejército de EUA, está cursando un programa de doctorado en la Escuela de Ciencias de la Computación de la Universidad Carnegie Mellon. Obtuvo una licenciatura en Ingeniería Civil por la Academia Militar de Estados Unidos y una maestría en Investigación Operativa por la Escuela Naval de Posgrado. Beskow ha desempeñado varias funciones durante su carrera, entre las que figuran: líder de infantería en la 82ª División Aerotransportada y la 4ª División de Infantería, profesor adjunto en West Point y analista de sistemas e investigación de operaciones en el Comando de Seguridad e Inteligencia del Ejército de Estados Unidos. Su investigación actual se centra en el desarrollo de algoritmos de aprendizaje automático que puedan detectar y caracterizar bots en línea y las campañas de desinformación con las que interactúan.

La doctora Kathleen M. Carley es profesora de Computación Social en la Escuela de Ciencias de la Computación de la Universidad Carnegie Mellon, miembro honoraria del IEEE, directora del Centro para el Análisis Computacional de los Sistemas Organizativos y Sociales (CASOS) y directora general de Netanomics. En 2011 ganó el Premio Simmel de la Red Internacional para el Análisis de Redes Sociales (INSNA) y en 2018 fue condecorada por la Fundación de Inteligencia Geoespacial de Estados Unidos (USGIF) por su trayectoria académica.

antropología, las ciencias forenses, las ciencias de la decisión y la psicología social»[4]. Muchos investigadores en este campo están aprovechando herramientas de la ciencia social computacional como el análisis de redes, el análisis espacial, el análisis semántico y el aprendizaje automático para aplicarlas en múltiples niveles, desde el individual hasta el comunitario.

Para que el Departamento de Defensa (DoD) pueda «defender la seguridad de nuestro país y mantener su influencia en el exterior», nuestros líderes militares deben entender la ciberseguridad social y cómo esta repercute en nuestras fuerzas, en nuestra nación y en nuestros valores[5]. Este artículo introducirá y definirá esta disciplina emergente, discutirá brevemente su historia y los cambios sociotecnológicos que la habilitaron y, por último, abordará las diferentes «formas de maniobra» de la ciberseguridad social actuales y en desarrollo. También elaboraremos sobre las similitudes y las diferencias entre las operaciones cibernéticas tradicionales y las de ciberseguridad social.

> Esta «guerra relámpago de información» en curso tendrá consecuencias estratégicas similares a las de la guerra relámpago de principios de la Segunda Guerra Mundial.



(Gráfico: victorhabbick, Adobe Stock)

Telón de fondo: la guerra relámpago de información

Rusia está librando la guerra relámpago de información más impresionante que hemos visto en la historia de las guerras de información.

—General Philip Breedlove,
Cumbre de la OTAN en Gales de 2014[6]

El aparato propagandístico ruso, que desde hace mucho dirigía sus actividades hacia su propia sociedad como también los Estados satélite de la antigua Unión Soviética, ahora tiene objetivos en el extranjero. En un famoso artículo de 2013 titulado «El valor de la ciencia para predecir», el general Valeri Guerásimov declaró que la guerra de información jugará un papel importante en la manera en la que Rusia librará la guerra en el futuro[7]. Aunque en Occidente este artículo ha sido analizado erróneamente bajo el prisma del conflicto ucraniano, además de ser malinterpretado como una declaración inicial de guerra híbrida, en realidad, Guerásimov con él se estaba refiriendo a los acontecimientos de la Primavera Árabe como también a las operaciones que Estados Unidos condujo en Yugoslavia, Iraq y Afganistán[8]. Para Guerásimov, la Primavera Árabe y las coaliciones que Estados Unidos encabezó en Oriente Próximo demuestran que las fuerzas militares convencionales no son necesarias para influir en los acontecimientos y los objetivos se pueden conseguir por otros medios no convencionales, en particular, a través de las operaciones de información. Las fuerzas militares fueron introducidas en el último minuto como *coup de grâce*.

Después de estudiar estos conflictos, Guerásimov buscó una manera de acelerar las iniciativas de guerra de información en curso y declaró: «La guerra de información abre muchas posibilidades asimétricas para disminuir la posibilidad de luchar directamente contra el enemigo»[9]. Estas iniciativas se alineaban con las operaciones tradicionales del KGB (Comité para la Seguridad del Estado) conocidas como «medidas activas». Estas medidas, según el mayor general del KGB Oleg Kalugin, buscaban «debilitar Occidente, crear divisiones entre las alianzas, en particular la OTAN, sembrar la discordia entre aliados y dañar la imagen de Estados Unidos ante la opinión pública de Europa, Asia, África y América Latina para así preparar el terreno en caso de una guerra verdadera»[10]. Las palabras de Kalugin demuestran uno de los papeles fundamentales de la guerra de información rusa, que es crear divisiones donde sea que fuera posible para debilitar una nación o coalición. Por ejemplo, divisiones entre partidos políticos, razas, religiones, entre una nación y sus fuerzas armadas o sus aliados. Una nación dividida es menos resistente a un ataque.

Los ejemplos recientes de operaciones de información son una continuación de las operaciones propagandísticas de la época de la Unión Soviética. En 1951, el profesor Harold Lasswell, de la Facultad de Derecho de la Universidad de Yale, resumió la máquina propagandística soviética (a la cual el actual aparato de seguridad ruso le debe mucho) de la siguiente manera:

> La estrategia principal [de la propaganda soviética] es economizar el costo material de proteger y extender el poder de la élite rusa domésticamente y en el exterior. Esta propaganda es un desafío para la mente del hombre, desde el punto de vista soviético, en el sentido de que es difícil controlar los medios materiales por los que se cree que se pueden moldear las mentes de las masas. Por lo tanto, el propósito de la propaganda rusa no es persuadir pacíficamente a la mayoría de las personas de un país como preludio a la toma de poder. Más bien, en esta tarea, una minoría debe permanecer una minoría ideológica hasta que logre acumular los medios materiales para obtener el consenso. […] Los propagandistas soviéticos y sus agentes pueden mentir y distorsionar sin ninguna restricción interna porque son generalmente inmunes a los reclamos de dignidad humana en todos los sentidos excepto en la dignidad de […] contribuir al poder presente y futuro de la élite del Kremlin[11].

Este enfoque general, de construir un pequeño núcleo mientras se fomentan divisiones en las organizaciones e instituciones rivales y aprovechar la desinformación en todo momento, continúa en la actualidad. La tecnología, sin embargo, hoy en día permite esto a una escala y distancia inimaginable en 1951.

El Estado ruso toma estas actividades seriamente. Desde principios de 2003, la Academia de Ciencias de Rusia ha conducido investigaciones para desarrollar modelos matemáticos aplicados avanzados de

Alexander Malkevich, 3 de marzo de 2012. (Foto: A. Khmeleva, Wikimedia Commons)

guerra de información y sus efectos en la sociedad. Los investigadores están combinando las ciencias sociales y la modelación matemática para producir investigaciones con títulos como la «Modelación matemática de rumores y propagación de la información en la sociedad». Aunque estas investigaciones se están llevando a cabo supuestamente para hacer frente a los ataques de información, es probable que también se estén empleando en operaciones ofensivas.

Estas operaciones ofensivas son sincronizadas por equipos cada vez más grandes de tecnólogos políticos. Ellos son líderes, tanto dentro como fuera del Gobierno, que entienden la naturaleza interrelacionada de los dominios humano, político, militar y tecnológico. Mediante este entendimiento «multidominio», ellos desarrollan y coordinan operaciones de influencia que aprovechan los dominios cibernético y tecnológico para influir en los dominios social, político y militar. Ejemplo de ello es Alexander Malkevich, un tecnólogo radicado en Moscú que creó la página web www.USAreally.com en anticipación de las elecciones de medio término de 2018 en Estados Unidos[12]. Su misión era difundir una narrativa tergiversada como también crear agitación para fomentar la discordia entre el pueblo estadounidense y que los principales medios de noticias, o por lo menos los principales lectores de noticias, cubrieran estos sucesos. La *descripción* personal que aparece en su cuenta de Twitter dice: «Periodista. Hombre de los medios de comunicación. Una persona que está interesada en la vida. Y no tiene miedo de trabajar en las regiones de Rusia. Y en nombre de Rusia»[13]. Esto es un tecnólogo político.

Cambio en el centro de gravedad estratégico

El siglo XX se inició con las guerras más simétricas y cinéticas de la historia, mientras que el siglo XXI, después de varias décadas de competencia de Guerra Fría, empezó con numerosos conflictos asimétricos y no cinéticos. Durante la Primera Guerra Mundial, las naciones sacrificaron cientos de miles de vidas para capturar unos pocos metros de terreno físico. En la actualidad, muchos actores desarrollan diseños complejos para lentamente ganar «metros» en el dominio humano con ramificaciones en el dominio físico.

La geografía todavía es relevante. Los océanos Atlántico y Pacífico siguen siendo los dos mayores objetivos de seguridad de Estados Unidos[14]. Rusia anexó Crimea principalmente debido a la importancia estratégica de su puerto en el mar Negro (como también por sus implicaciones energéticas)[15]. La inestabilidad en Afganistán continuará debido, en parte, a su geografía[16]. La geografía importa y siempre lo hará. Sin embargo, se podría argumentar que numerosos factores, incluyendo la tecnología, han inclinado la balanza hacia la dimensión humana.

Este énfasis en el dominio humano fue fuertemente debatido entre las fuerzas militares estadounidenses durante la guerra contra el terrorismo. Después de años de debate, la mayoría parecía estar de acuerdo con la cita de un artículo de 2009 de la revista *Small Wars Journal* que señalaba: «Uno de los cambios más profundos que las Fuerzas Armadas de Estados Unidos tienen que hacer para contrarrestar eficazmente una insurgencia es cambiar los centros de gravedad estratégicos del aspecto físico al aspecto humano de la guerra»[17]. Aunque esta declaración es aceptada en los ambientes de contrainsurgencia, queda por ver cómo este énfasis en el dominio humano afectará las operaciones de combate a gran escala.

Esta perspectiva de la población como el centro de gravedad adquirió un nuevo significado después de la Primavera Árabe, cuando movimientos poblacionales descentralizados, a través de la tecnología, se organizaron y derrocaron múltiples regímenes autocráticos establecidos. Estas acciones sorprendieron al mundo y han sido estudiadas por líderes en tanto Occidente como Oriente, puesto que destacan el poder de la dimensión humana como también el poder de los medios sociales para movilizar a las masas. Varios artículos en revistas militares han documentado estos movimientos, centrándose específicamente en los medios sociales que lo habilitaron. Incluso el artículo de 2013 de Guerásimov para la revista rusa *Correo Militar-Industrial*, considerado en Occidente como la génesis de la guerra *híbrida* o guerra *gris*, es más una reflexión personal de la Primavera Árabe (y también de los conflictos en Iraq, Afganistán y Yugoslavia) que un intento de crear un nuevo tipo de guerra[18].

Varios actores estatales y no estatales notaron estos cambios y empezaron a explotar la idea de manipular estos movimientos a través del ciberespacio. Muchos de ellos ya han manipulado a su propia población u organización mediante operaciones de información y ahora buscan lo mismo en otras poblaciones y sociedades[19]. Influir directamente en el tejido social, el verdadero centro de gravedad de una nación, tiene consecuencias significativas desde el nivel táctico hasta el nivel estratégico de la guerra y es la génesis de este dominio emergente de ciberseguridad social.

Habilitando los cambios

Dos cambios en los flujos de información social y de comunicación han dado lugar a la ciberamenaza social. Primero, la tecnología ha eliminado el requisito de proximidad física para influir en una sociedad y la descentralización de los flujos de información ha reducido el costo de entrada. Fabio Rugge, del Instituto Italiano para los Estudios de Política Internacional, resume esto de la siguiente manera: «El ciberespacio es un poderoso multiplicador de los efectos desestabilizadores de la información manipulada porque ofrece una alta conectividad, un bajo costo de entrada, varios puntos de distribución sin intermediarios y completa indiferencia a la distancia física o a las fronteras nacionales. Más importante aún, el anonimato y la inhabilidad de poder atribuir un ataque a alguien con seguridad hacen el ciberespacio el dominio de la ambigüedad»[20].

Descentralización. En los últimos treinta años, hemos visto cómo los flujos de información se han descentralizado rápidamente. Históricamente, los Gobiernos, las grandes organizaciones y algunos canales de noticias controlan la cobertura informativa en los medios impresos, de radio y televisión. Estas organizaciones controlan el flujo de información y generalmente la distribuyen de manera uniforme entre la sociedad. Con el aumento de los blogs, los microblogs y las redes sociales, la mayor parte del mundo obtiene información de forma no uniforme a través de los medios sociales[21]. Ahora hay un bajo costo de entrada, incentivos financieros para crear contenido viral y el anonimato es relativamente fácil de alcanzar. Esta descentralización ha facilitado la entrada de actores externos con mínima atribución.

El control de calidad actual del flujo de información está descentralizado. La verificación de datos ahora se conduce a nivel de usuario en vez de a nivel periodístico. Los usuarios, muchos de los cuales crecieron en una época en la que se confiaba en las noticias, no están preparados para digerir noticias que pueden ser tanto verdaderas como falsas, especialmente si las distorsiones de la verdad validan sus propios sesgos.

El modelo de periodismo tradicional requiere la verdad. Los periodistas pierden sus empleos y las organizaciones de noticias pierden oportunidades de negocio si constantemente cometen errores. El modelo de negocio de los medios sociales, enfocado principalmente en el tráfico y la publicidad, no depende tanto de la verificación de datos. Sin embargo, esto está cambiando poco a poco y ejemplo de ello es la caída de las acciones de tanto Twitter como Facebook en agosto de 2018. Estas

compañías pasaron por un período de crecimiento lento porque empezaron a eliminar cuentas de sus plataformas que propagaban noticias falsas.

Aunque con las leyes aprobadas recientemente a nivel global se busca centralizar el control, esto conllevará censurar y limitar la libertad de expresión. En algunos casos, esto podría acabar en un caos absoluto, especialmente si las compañías de medios sociales son obligadas a proporcionar una función en su plataforma que permita detectar información malintencionada o falsa. Si este tipo de función es expuesta a los usuarios a través de una interfaz de programación de aplicaciones (API) o una interfaz web/móvil, entonces los mismos bots que publican noticias falsas podrían clasificar cualquier contenido que sea verdadero como falso a la velocidad de un algoritmo y causar mucho más daño.

La presencia física no es obligatoria. Durante gran parte de la historia, la influencia requería una presencia física o por lo menos proximidad. Para influir en las conversaciones del foro romano, pulso de aquella sociedad, un actor o representante tenía que estar presente físicamente en el foro, o por lo menos en Roma, y ser además claramente identificable y activo en las conversaciones. Las operaciones

Tabla. El modelo BEND para describir las formas de maniobra de ciberseguridad social

	Maniobra de información		Maniobra de red	
	Manipulación de la red del conocimiento		Manipulación de la red social	
	Lo que puedes lograr si manipulas lo que se está discutiendo		Lo que puedes lograr si manipulas la interacción entre el emisor y el receptor del mensaje	
Positivo	**Difundir**	Discusión que presenta temas relacionados, pero también pertinentes	**Respaldar**	Acciones que aumentan la importancia del líder de opinión
	Explicar	Discusión que ofrece detalles o profundiza en el tema	**Construir**	Acciones que crean un grupo o la apariencia de un grupo
	Animar	Discusión que trae alegría, felicidad, entusiasmo al grupo	**Crear puentes**	Acciones que establecen un vínculo entre dos o más grupos
	Mejorar	Discusión que incita al grupo a continuar con el tema	**Impulsar**	Acciones que aumentan el tamaño del grupo o dan la apariencia de ello
Negativo	**Descartar**	Discusión sobre por qué el tema no es importante	**Neutralizar**	Acciones que limitan la eficacia del líder de opinión reduciendo, por ejemplo, el número de personas que pueden seguirlo, responder o participar
	Distorsionar	Discusión que altera el mensaje principal del tema	**Desmantelar**	Acciones que resultan en la desmantelación del grupo
	Desanimar	Discusión sobre un tema que traerá preocupación, tristeza, enfado al grupo	**Reducir**	Acciones que resultarán en que el grupo se aísle de otros
	Distraer	Discusión sobre un tema completamente diferente e irrelevante	**Descuidar**	Acciones que reducen el tamaño del grupo o dan la apariencia de ello

(Tabla de los autores)

«clandestinas» ocurrían, pero incluso esas operaciones requerían una presencia física. La proximidad fue necesaria durante toda la primera parte del siglo XX, período en el que las operaciones con radios y panfletos emergieron. Si bien estas operaciones no requerían una presencia física directa, sí requerían cierto nivel de proximidad. Incluso las robustas operaciones de propaganda de la Unión Soviética se limitaban principalmente a Europa oriental y a Asia debido a la geografía. Internet ha eliminado este requisito, con la mayoría de las sociedades en ambientes en línea abiertos y libres que permiten a los actores participar desde todos los rincones del globo con pocas fronteras nacionales en el dominio cibernético.

Las naciones que valoran la libertad de expresión y el intercambio de opiniones e ideas son más vulnerables a esas amenazas[22]. Es por ello que Corea del Norte, una de las naciones más aisladas del planeta, por no decir la más aislada, apenas se ve afectada por la manipulación social a través de Internet. Para influenciar directamente a la sociedad norcoreana es necesario tener una presencia física o proximidad.

La vulnerabilidad de las sociedades abiertas ante la manipulación social mediante la tecnología es exacerbada por el hecho de que la mayoría de estos esfuerzos estratégicos de información son realizados en plataformas de medios sociales globales que son privadas y fuera de la supervisión directa de los Gobiernos (aunque sí son sujetas a las leyes). Si bien todas las compañías de medios sociales censuran contenido en sus plataformas, la razón por la cual lo hacen es para mejorar la experiencia del usuario con el producto, no por preocupaciones de seguridad nacional. Tomar partido sobre cualquier tema generalmente es malo para los negocios porque corren el riesgo de enajenar un segmento de su base de clientes. Se supone que la censura del Gobierno es partidista y viola la libertad de expresión defendida por estos Gobiernos. Los esfuerzos de terceros para censurar contenido ya se han empezado a llevar a cabo, pero hasta la fecha, estos han tenido un enfoque limitado y pueden ser fácilmente eludidos. Ejemplo de esto es la iniciativa «Social Science One», una colaboración entre investigadores académicos, el sector privado y fondos del estamento político para llevar a cabo investigaciones sobre los datos de medios sociales sin violar la privacidad individual. Esfuerzos como estos todavía se encuentran en fases iniciales.

Formas de maniobra cibersocial

Como en el dominio físico y el dominio cibernético tradicional, el dominio cibersocial ofrece múltiples «formas de maniobra». En este dominio, el adversario puede manipular tanto la *información* como la *red*. Estas redes pueden ser sociales (Sarah y Peter son *amigos*), de conversación (Sarah le *responde* a Peter) o de información (Sarah y Peter comparten la etiqueta #OTAN).

Formas de maniobra BEND. El estado final deseado para las operaciones de información varía. Las operaciones de información tradicionales aumentan el apoyo para la narrativa deseada y lo reducen en la contranarrativa. Otras operaciones simplemente buscan fomentar la agitación y reducir la confianza, independientemente de la narrativa. Esta agitación ayuda a crear divisiones entre la sociedad. Cualquiera de los estados finales deseados es apoyado por las formas de maniobra BEND (véase la tabla)[23].

Las formas de maniobra BEND describen cómo un actor puede manipular el mercado de creencias, ideas e información. Estas formas de maniobra amplifican los paradigmas de distracción, consternación, distorsión y rechazo que Ben Nimmo presentó en el Laboratorio de Investigación Forense Digital del Consejo del Atlántico[24]. El modelo BEND categoriza las formas de maniobra por polaridad como también si el objetivo es la *información* o la *red*.

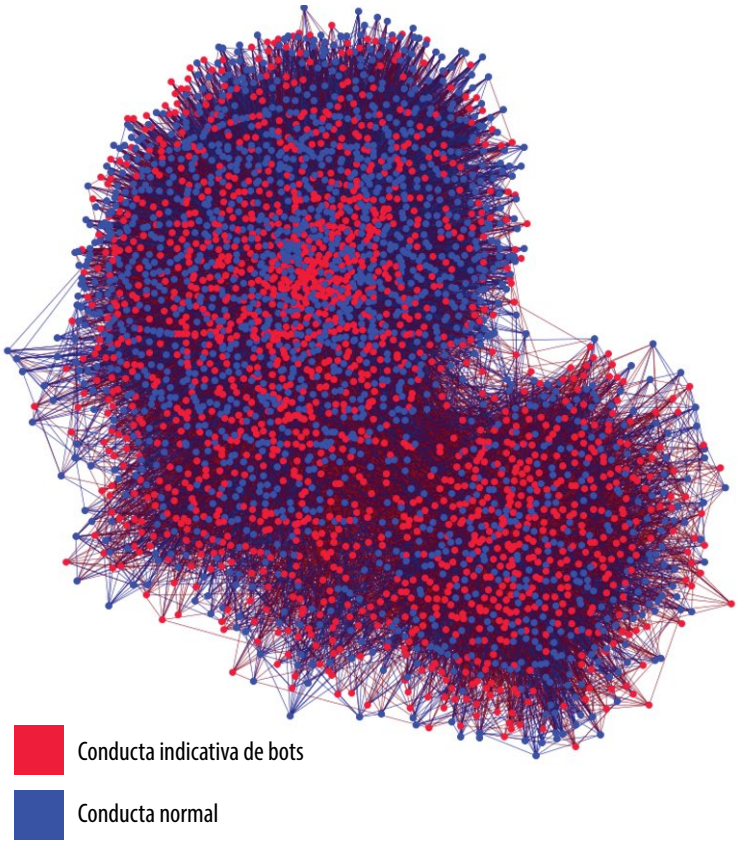
Maniobra de información. La maniobra de información es la manipulación de información y el flujo o relevancia de la información en el ciberespacio. La maniobra de información tiene muchos fines, como por ejemplo:

- Desorientar. Introducir temas polémicos que no están relacionados con un hilo para cambiar el rumbo de la conversación.
- Aprovechar las etiquetas. Vincular contenido y narrativas a temas y etiquetas del momento que no están relacionados.
- Generar una cortina de humo. Difundir contenido (tanto semántica como geográficamente) que oculta otras operaciones.
- Usurpar un hilo. Interrumpir o apropiarse agresivamente de una conversación en línea productiva.

Maniobra de red. La maniobra de red es la manipulación de la red. En estas maniobras, un adversario crea un mapa de una red social (porque se da cuenta una vez más que una red social en línea es la

proyección de vínculos sociales y de conversación en la dimensión cibernética). La maniobra de red se puede utilizar para:

- Usar un líder de opinión. Tener acceso a un líder de opinión en línea y ganar su reconocimiento para aprovechar su influencia y difundir la narrativa propia.
- Construir una comunidad. Construir una comunidad alrededor de un tema, idea u hobby y después inyectarle una narrativa al grupo. Esto fue lo que ocurrió en Ucrania. Se crearon páginas de Internet para juntar jóvenes y crear una comunidad. Esas páginas después fueron inundadas de retórica antiucraniana y prorusa.
- Crear un puente entre las comunidades. Inyectar las ideas de un grupo en otro. En este caso, el adversario identificará dos comunidades, A y B. Al adversario le gustaría inyectar las ideas del grupo B en el grupo A. Para lograrlo, primero hay que infiltrarse en el grupo A y después poco a poco retuitar o compartir ideas del grupo B, para así crear un puente entre las ideas del grupo B y el grupo A.
- Generalizar falsamente. Promover la noción falsa de que una idea representa el consenso de las masas y, por lo tanto, esta idea o creencia debería ser aceptada por todos.



(Figura de los autores)

Figura. La participación de bots en las principales conversaciones políticas en Twitter sobre las elecciones recientes en Suecia

Bots como multiplicadores de fuerza

En el contexto de las operaciones de información, los bots (robots informáticos) son cada vez más empleados como multiplicadores de fuerza. Gracias al aprendizaje automático y a la inteligencia artificial, los bots conducen transacciones de información de forma oportuna y específica a escala y dejan los diálogos con matices críticos a los operadores humanos. En este contexto, los actores humanos a menudo son llamados «troles», denominación que simplemente sirve para diferenciar a los actores humanos que siembran la discordia de los robots o computadoras que hacen lo mismo (p. ej. los bots).

Un bot es definido como una cuenta de medios sociales que utiliza una computadora para automatizar tareas relacionadas con los medios sociales. Por ejemplo, en Twitter, una cuenta bot puede automáticamente tuitear, retuitear, seguir, enviar una solicitud de amistad, responder, citar y gustar algo. El creador del bot puede usar medios creativos para generar contenido, como recopilar información de forma automática de Internet, una técnica llamada *scraping* en inglés, y resumirla, retuitear contenido, manipular contenido de otros usuarios humanos o crear su propio contenido a través de una combinación de datos facilitados por humanos e inteligencia artificial. Después de crear el contenido, el creador del bot puede manipular la publicación de los tuits para que parezcan humanos (y si la apariencia no es esencial para la operación, el bot puede llevar a cabo miles de acciones ininterrumpidamente). Por último, estos bots a menudo son desplegados en redes (a veces son llamados «ejércitos bots» o «bots coordinados») en donde hacen amistades, se siguen y se promueven para parecer populares.

Los bots son usados por varias razones y pueden crear efectos positivos, inoportunos o malintencionados. Algunos ejemplos de bots positivos son los asistentes y las

cuentas personales que notifican al público de los desastres naturales. Los bots inoportunos distribuyen *spam* (correo basura) que incluyen desde publicidad comercial hasta contenido adulto. Los bots malintencionados generalmente lidian con propaganda, supresión de la disidencia, intimidación e infiltración/manipulación de las redes[25].

Aunque muchas veces intentamos clasificar una cuenta como bot o humana, muchas veces esa cuenta tiene cierto grado de automatización. Muchas cuentas no son automatizadas estrictamente (en donde todas las transacciones son ejecutadas por una computadora). Estas cuentas son intervenidas por humanos que contribuyen a un diálogo matizado mientras una computadora ejecuta tareas a escala en el trasfondo. Cuando se combinan con la inteligencia artificial, estos bots conducen un sinnúmero de operaciones a la velocidad de algoritmos (véase la figura).

Conclusión

La guerra de nueva generación será dominada por la información y por las operaciones psicológicas con el objetivo de tener un control superior de las tropas y las armas y para debilitar a la población y a las fuerzas armadas rivales moral y psicológicamente. En la revolución en curso de la tecnología de la información, las guerra de información y psicológica tendrán un papel fundamental en la preparación del terreno para la victoria.

—*Pensamiento Militar* [revista rusa], 2013[26]

Se podría argumentar que la mayor debilidad estratégica de cualquier país es de carácter interno, no externo. Los líderes tienen que entender la ciberseguridad social para proteger estas debilidades internas de la manipulación externa. Como líderes militares, debemos entender que una de las líneas de esfuerzo de la guerra relámpago de información será fomentar la desconfianza entre nosotros y la sociedad que defendemos, además del liderazgo civil que nos guía. Una institución en la que no se confía será infradotada, infrautilizada y de bajo rendimiento.

Si una de nuestras principales misiones es «mantener la influencia de Estados Unidos en el exterior», entonces necesitamos determinar cuál es nuestra función en la promoción de los valores estadounidenses en este mercado internacional de creencias e ideas mediante un esfuerzo interagencial coordinado. Esta influencia incluye desde las interacciones en línea hasta un apretón de manos de un jefe de pelotón en una base avanzada.

Los líderes militares deben adoptar políticas que permitan la libertad de maniobra en los ambientes de información relevantes. Un informe sobre las operaciones de información de la Corporación RAND concluyó que el DoD debe cambiar su política para poder maniobrar éticamente en el dominio de la información[27]. La mayoría de los practicantes de ciberseguridad social (tanto los creadores de bots como los que crean defensas contra ellos) usan las API y tecnología de fuente abierta para acceder a este ambiente de datos y maniobrar en él. En otras palabras, las API son el punto de acceso para las operaciones cibersociales ofensivas y defensivas. En el Ejército, las políticas y las normas para acceder a las API son seriamente limitadas para algunas organizaciones y en otras no son bien definidas. Necesitamos políticas eficaces que faciliten la iniciativa en un ambiente de información dinámico, protejan la privacidad de individuos con buenas intenciones y no infrinjan las normas a las que está sujeto el DoD.

En resumen, debemos educar directamente a nuestra fuerza e indirectamente a nuestra sociedad sobre la naturaleza descentralizada del ambiente de información moderno, los riesgos que existen y las maneras y los medios para verificar individualmente los datos y las opiniones que digerimos y que influyen en nuestras creencias y actitudes. Debemos desarrollar un enfoque multidisciplinar para la ciberseguridad social. Debemos implementar políticas relevantes que permitan la ciberseguridad social. Debemos eliminar la desconfianza artificial entre nuestras Fuerzas Armadas y la sociedad a la que defendemos. Debemos determinar la función del DoD mediante un esfuerzo interagencial para combatir la guerra relámpago de información que enfrentamos en la actualidad. La ciberseguridad social será una disciplina obligatoria en el futuro próximo. ■

Este trabajo fue realizado, en parte, gracias a los premios Multidisciplinary University Research Initiative Award N000141812108 y Minerva Awards N00014-13-1-0835/N00014-16-1-2324, otorgados por la Oficina de Investigación Naval (ONR), y al apoyo del Centro para el Análisis Computacional de los Sistemas Sociales y de Organización (CASOS). Las opiniones y conclusiones de este artículo son de los autores y no representan la política oficial, expresa o implícita, de la ONR o del Gobierno estadounidense.

Notas

1. Kathleen M. Carley y otros, «Social Cyber-Security», en *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP-BRiMS 2018, Washington, DC, USA, julio 10–13, 2018, Proceedings*, ed. Halil Bisgin et al. (Nueva York: Springer, 2018), 389–94.

2. Joshua Yaffa, «Dmitry Kiselev Is Redefining the Art of Russian Propaganda», *The New Republic* (sitio web), 1 de julio de 2014, accedido 14 de noviembre de 2018, https://newrepublic.com/article/118438/dmitry-kiselev-putins-favorite-tv-host-russias-top-propogandist.

3. Stephen Townsend, «Accelerating Multi-Domain Operations: Evolution of an Idea», Modern War Institute at West Point, 23 de julio de 2018, accedido 14 de noviembre de 2018, https://mwi.usma.edu/accelerating-multi-domain-operations-evolution-idea/; Valery Gerasimov, «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): 23–29 [disponible en español en la edición hispanoamericana de marzo-abril 2016 bajo el título «El valor de la ciencia está en la capacidad de prever lo que sucederá o podría suceder en el futuro»].

4. Carley y otros, «Social Cyber-Security».

5. «Legacy Homepage», U.S. Department of Defense, accedido 16 November 2018, https://dod.defense.gov/.

6. Peter Pomerantsev, «Russia and the Menace of Unreality: How Vladimir Putin is Revolutionizing Information Warfare», *The Atlantic* (sitio web), 9 de septiembre de 2014, accedido 14 de noviembre de 2018, https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880/.

7. Gerasimov, «The Value of Science is in the Foresight».

8. Charles K. Bartles, «Getting Gerasimov Right», *Military Review* 96, nro. 1 (enero-febrero 2016): 30–38 [disponible en español en la edición hispanoamericana de marzo-abril 2016 bajo el título «Cómo comprender el artículo de Gerasimov»].

9. Ibíd.

10. Steve Abrams, «Beyond Propaganda: Soviet Active Measures in Putin's Russia», *Connections: The Quarterly Journal* 15, nro. 1 (2016): 5–31.

11. Harold D Lasswell, «The Strategy of Soviet Propaganda», *Proceedings of the Academy of Political Science* 24, nro. 2 (1951): 66–78.

12. Tim Johnson, «Exclusive: 'Little Russian Media Project' Tries to Turn America against Itself», McClatchy, última actualización 10 de junio de 2018, accedido 21 de diciembre de 2018, https://www.mcclatchydc.com/news/nation-world/national/national-security/article213403299.html.

13. Alexander Malkevich (@McCevich), «Periodista. Hombre de los medios de comunicación. Una persona que está interesada en la vida. Y no tiene miedo de trabajar en las regiones de Rusia. Y en nombre de Rusia [traducción del ruso]», Twitter, accedido 21 de diciembre de 2018, https://twitter.com/McCevich.

14. Peter Zeihan, *The Accidental Superpower: The Next Generation of American Preeminence and the Coming Global Disorder* (Nueva York: Twelve, 2014).

15. John Biersack y Shannon O'Lear, «The Geopolitics of Russia's Annexation of Crimea: Narratives, Identity, Silences, and Energy», *Eurasian Geography and Economics* 55, nro. 3 (2014): 247–69.

16. Robert D. Kaplan, «The Revenge of Geography», *Foreign Policy*, nro. 172 (2009): 96–105.

17. James A. Gavrilis, «A Model for Population-Centered Warfare: A Conceptual Framework for Analyzing and Understanding the Theory and Practice of Insurgency and Counterinsurgency», *Small Wars Journal*, 10 de mayo de 2009, accedido 14 de noviembre de 2018, https://smallwarsjournal.com/blog/journal/docs-temp/241-gavrilis.pdf.

18. Bartles, «Getting Gerasimov Right».

19. Lasswell, «The Strategy of Soviet Propaganda».

20. Fabio Rugge, «'Mind Hacking': Information Warfare in the Cyber Age», Analysis No. 319, Instituto Italiano para los Estudios de Política Internacional, 11 de enero de 2018, accedido 14 de noviembre de 2018, https://www.ispionline.it/en/pubblicazione/mind-hacking-information-warfare-cyber-age-19414.

21. Elisa Shearer y Jeffrey Gottfried, «News Use Across Social Media Platforms 2017», Pew Research Center, 7 de septiembre de 2017, accedido 14 de noviembre de 2018, http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/.

22. Robert F. Baumann, «A Central Asian Perspective on Russian Soft Power: The View from Tashkent», *Military Review* 98, nro. 4 (julio-agosto 2018): 50–63 (disponible en español en la edición actual bajo el título «Una perspectiva del poder blando ruso en Asia Central: La perspectiva de Taskent»).

23. El acrónimo «BEND» se deriva de las 16 formas de maniobra presentadas en la tabla: cuatro empiezan con «b» [en inglés], cuatro con «e», cuatro con «n» y cuatro con «d».

24. Ben Nimmo, «Anatomy of an Info-War: How Russia's Propaganda Machine Works, and How to Counter It», *Central European Policy Institute* 15 (2015).

25. Cristian Lumezanu, Nick Feamster y Hans Klein, «#bias: Measuring the Tweeting Behavior of Propagandists», *Proceedings of the Sixth International Conference on Weblogs and Social Media* (Palo Alto, CA: The AAAI Press, 2012), 210–17; John-Paul Verkamp y Minaxi Gupta, «Five Incidents, One Theme: Twitter Spam as a Weapon to Drown Voices of Protest» (presentación, 3rd USENIX Workshop on Free and Open Communication on the Internet, Washington, DC, 13 de agosto de 2013), 1–7; Rosie Alfatlawi, «Thousands of Twitter Bots Are Attempting to Silence Reporting on Yemen», Al Bawaba: The Loop, 22 de noviembre de 2017, accedido 16 de noviembre de 2018, https://www.albawaba.com/loop/original-saudi-bots-yemen-suffering-1051564; Matthew Benigni and Kathleen M. Carley, «From Tweets to Intelligence: Understanding the Islamic Jihad Supporting Community on Twitter», en *Social, Cultural, and Behavioral Modeling: 9th International Conference, SBP-BRiMS 2016, Washington, DC, USA, junio 28–julio 1, 2016, Proceedings*, ed. Kevin S. Xu y otros (Nueva York: Springer, 2016), 346–55.

26. Sergey G. Chekinov y Sergey A. Bogdanov, «La naturaleza y el contenido de la guerra de nueva generación», *Pensamiento Militar* [revista rusa] 4 (2013): 12–23.

27. William Marcellino y otros, «Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in Support of Information Operations» (Santa Monica, CA: RAND Corporation, 2017).