Un bombardeo de eventos y el fin de la inteligencia de fuente abierta en el nivel táctico

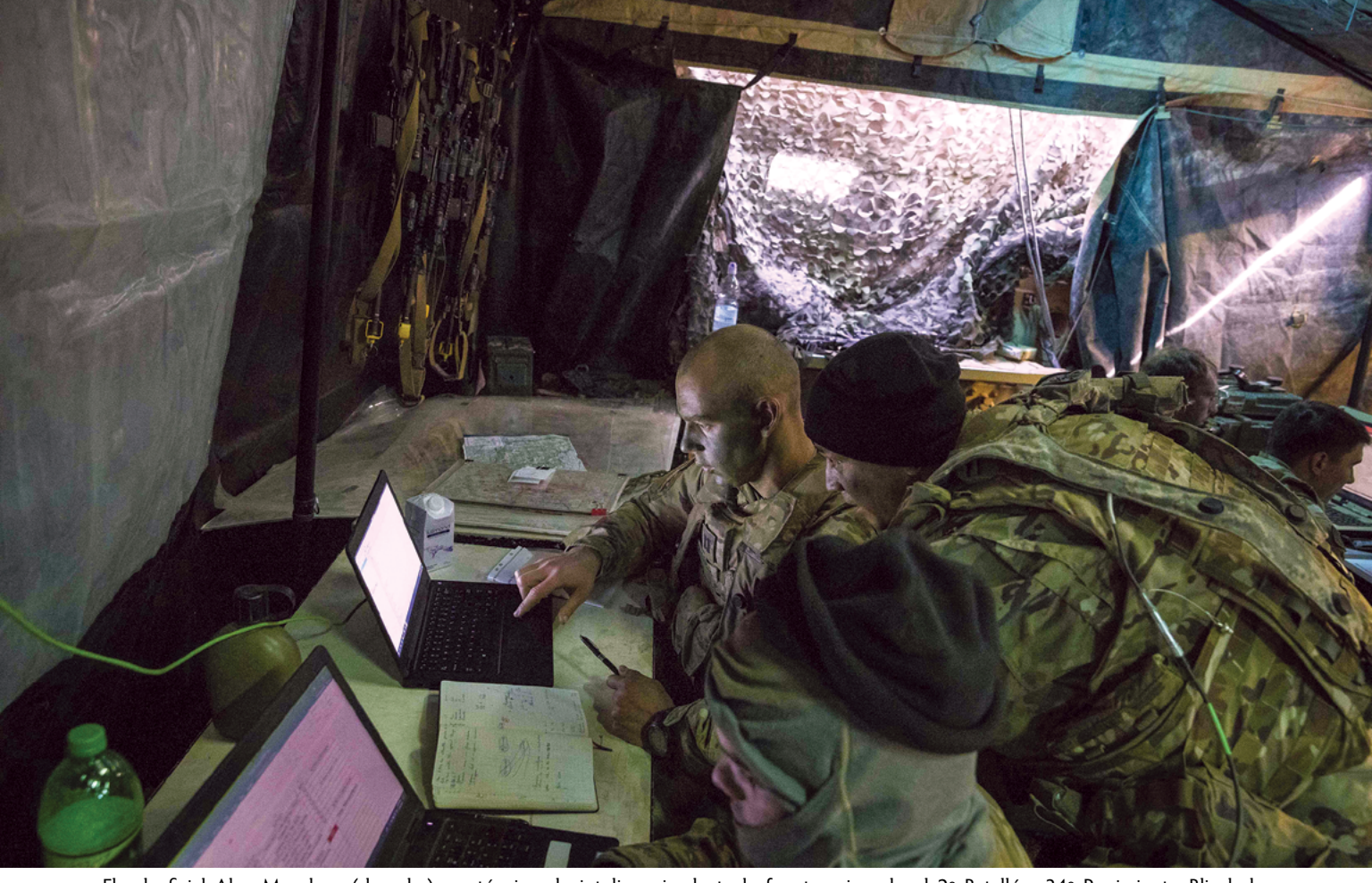
Capitán Michael J. Rasak, Ejército de EUA

Los no combatientes recurren cada vez más a los medios de comunicación social para informar sobre la disposición y composición de las fuerzas militares, la situación de la infraestructura y detalles de los acontecimientos locales en curso, lo que supone un riesgo legítimo para las actividades militares tanto amigas como adversarias. Los Estados nación y grupos adversarios ya han demostrado la capacidad e intención de mitigar y explotar este fenómeno. En un futuro cercano, es probable que los comandantes y analistas amigos sufran una inundación digital por una serie de eventos exagerados o totalmente fabricados en los medios sociales que amenazan directamente las operaciones tácticas en curso o a corto plazo, lo que se denomina un «bombardeo de eventos». En medio de un bombardeo de eventos, y debido a la inminencia de las operaciones de nivel táctico, los comandantes se ven obligados a elegir una de dos opciones indeseables: corroborar sistemáticamente cada suceso o ignorar los medios de comunicación social como plataforma para observar las actividades adversas en su conjunto. Las subsiguientes ramificaciones de los esfuerzos de bombardeo de eventos, secuestro de tendencias y desinformación precisamente dirigida podrían entonces perturbar la toma de decisiones de Estados Unidos a nivel táctico, sobrecargar los medios amigos de reconocimiento, inteligencia, vigilancia y adquisición de blancos (RISTA) y degradar la utilidad de la información de fuente abierta (OSIF). Los Estados nación o los grandes grupos podrían incentivar a sus poblaciones a participar en los eventos de bombardeo, comprometiendo en última instancia la integridad de la inteligencia de fuente abierta (OSINT) como disciplina en general.

El capitán Michael J. Rasak, Ejército de EUA, es el oficial de inteligencia de la 4ª Brigada de Caballería, Primera División del Ejército Este. Recibió su licenciatura de la Michigan State University. Sus asignaciones incluyen dos despliegues en Afganistán, uno como jefe de pelotón de infantería en la 101ª División Aerotransportada (Asalto Aéreo) y otro como oficial de inteligencia de escuadrón en la 3ª División de Infantería.

La inteligencia de fuente abierta a nivel táctico

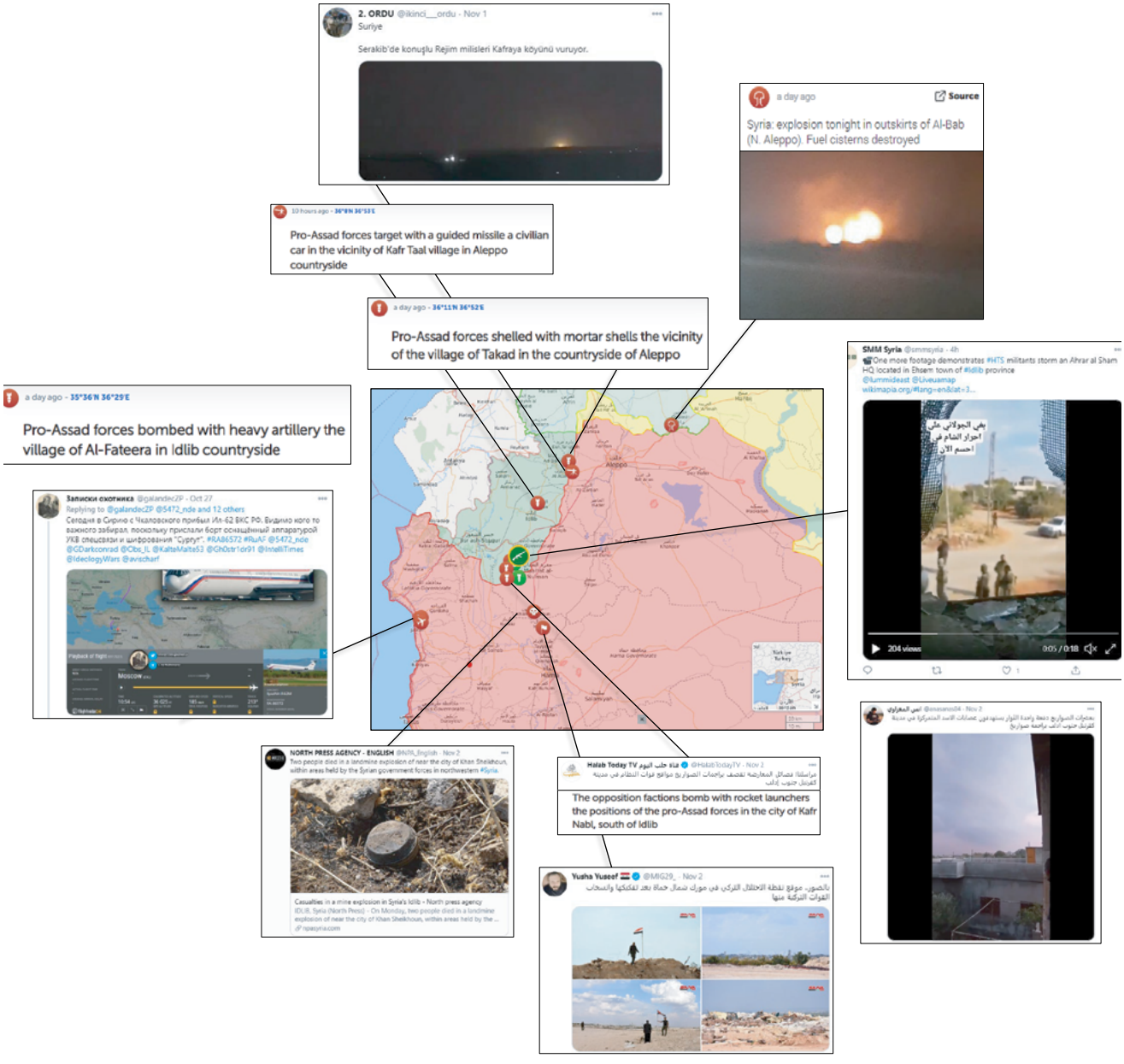
A pesar del ominoso título del presente artículo, la OSINT probablemente no desaparecerá como una disciplina del todo. El gran volumen de información contenida en el dominio de fuente abierta ofrece a los analistas un conjunto de datos



El suboficial Alan Mendoza (derecha), un técnico de inteligencia de toda fuente asignado al 2º Batallón, 34º Regimiento Blindado, 1er Equipo de Combate de la Brigada Blindada, ayuda al capitán Kenneth Russel, el oficial de inteligencia del batallón, el 8 de abril de 2019, durante el ejercicio Allied Spirit X en Hohenfels, Alemania. (Foto: Sgto. Thomas Mort, Ejército de EUA)

disponibles demasiado valiosos como para dejarlos de lado por completo. Solo tenemos que mirar las astutas observaciones de profesionales experimentados que abarcan toda la comunidad de inteligencia y dentro de las filas de las fuerzas armadas. El teniente general Samuel V. Wilson, exdirector de la Agencia de Inteligencia de Defensa, afirma que la OSINT proporciona aproximadamente el 90 % de la información utilizada por la comunidad de inteligencia[1]. Robert Cardillo, director de la Agencia Nacional de Inteligencia Geoespacial, sostuvo que «la información no clasificada ya no debe considerarse complementaria a las fuentes clasificadas, sino que debe ser al revés»[2]. Incluso aquellos que no tienen interés en la seguridad de la nación, como Vice News, han señalado la ilimitada cantidad de información militar valiosa que se puede obtener de fuentes de acceso público[3]. El conjunto de la OSIF disponible, que se manifiesta en el auge de los medios de comunicación social, solo ha fomentado un mayor entusiasmo: el etiquetado geográfico, georreferenciación, web *scraping* [extracción de datos de sitios web], análisis de sentimientos y análisis léxico son algunas de las tecnologías y técnicas emergentes. La OSINT ofrece a los comandantes desde el nivel táctico hasta el estratégico una inestimable comprensión profunda de los entornos no permisivos, que antes solo se obtenían mediante esfuerzos clandestinos. Dotados con esta mayor resolución, los comandantes son más capaces de entender y visualizar el campo de batalla, ofreciéndoles así una ventaja cuando deben describir, dirigir, liderar y evaluar las operaciones.

A nivel táctico, la OSINT ofrece a los comandantes de las fuerzas terrestres información crítica, casi en tiempo real, para apoyar la toma de decisiones. Los medios de comunicación social proporcionan especialmente a los analistas la oportunidad de rápidamente recopilar, monitorear y evaluar los acontecimientos dentro del área de operaciones de un comandante. Innumerables ciudadanos ordinarios dotados con teléfonos inteligentes, dispositivos GPS internos y cuentas de Twitter divulgan, sin saberlo,



(Figura producida por el autor con capturas de pantalla sacadas del Live Universal Awareness Map)

Figura 1. Ejemplo de Live Universal Awareness Map: Siria, 3 de noviembre de 2020

información sobre la disposición, composición y el número de fuerzas enemigas, el estado de la infraestructura, los acontecimientos en curso y el sentimiento general de la población. Además, la inmanencia inherente de las operaciones de nivel táctico (en lugar de las operaciones de nivel operacional o estratégico) hace que la información obtenida de la recolección de la OSINT tenga una importancia aún mayor.

Tomemos, por ejemplo, un pelotón de infantería que está patrullando, operando a solo unos kilómetros de una aldea. Cuando un oficial de inteligencia de un batallón o brigada observa un gran volumen de tuits que indican que los combatientes enemigos se han concentrado en la aldea, ese oficial tiene la obligación de corroborar la información en la mayor medida posible y difundirla al jefe de pelotón en el terreno. Si

no lo hace, el pelotón podría caer en una emboscada o perder la oportunidad de enfrentarse al enemigo en condiciones más favorables.

Los académicos, profesionales militares e integrantes de la comunidad de inteligencia han hablado de la eficacia de la OSINT en el nivel táctico. En «Operationalizing OSINT Full-Spectrum Military Operations» [Hacer operativas las operaciones militares de espectro total con la OSINT], el contramaestre Ron Penninger es autor de un ejemplo fantástico de la eficacia de la OSINT a nivel táctico y de cómo el análisis de los sentimientos y la georeferenciación pueden contribuir directamente a la toma de decisiones de los comandantes de fuerzas terrestres[4]. La Corporación RAND también ha hecho comentarios sobre los efectos de cambio de paradigma de la «OSINT de segunda generación». Heather J. Williams e Ilana Blum argumentan, «Los analistas [...] pueden usar una combinación de Google Maps, Wikimapia, tuits públicamente disponibles, publicaciones en Facebook y videos de YouTube para determinar la ubicación exacta de las acciones militares en curso»[5].

Aprovechar la OSINT para aplicaciones tácticas va mucho más allá de la mera retórica o la palabrería; las fuerzas armadas, organismos gubernamentales, organizaciones no gubernamentales y corporaciones están sacando provecho de ello en este momento. Live Universal Awareness Map (Liveuamap) [Mapa de Concienciación Universal en Vivo] sirve como quizás uno de los mayores ejemplos. En su sitio web, Liveuamap explica que es un «sitio independiente de noticias e información mundial», que tiene por objeto ayudar a las personas a «tomar decisiones conscientes sobre su seguridad»[6]. Basándose principalmente en los mensajes en los medios de comunicación social, el sitio proporciona información casi en tiempo real sobre el movimiento de personal y equipo militar, disturbios civiles, violencia y otras actividades, y superpone estos acontecimientos en un mapa interactivo (véase la figura 1). Por ejemplo, en el momento de escribir el presente artículo, uno de los acontecimientos más recientes en Libia (obtenido por crowdsourcing en Twitter) indica que «seis vehículos antiaéreos tipo Pantsir de fabricación rusa llegaron a Sirte»[7].

Los manifestantes en Hong Kong que utilizaron «HKMap Live» durante las grandes manifestaciones de finales de 2019 y principios de 2020 ofrecen otro ejemplo claro de cuán eficaces pueden ser los no combatientes no entrenados en el seguimiento de los movimientos de las fuerzas gubernamentales. A través del crowdsourcing y los medios de comunicación social, los manifestantes rastrearon la composición y disposición de las fuerzas policiales, comunicaron su intención y concentraron la mano de obra en los momentos y lugares de su elección. Los manifestantes de Hong Kong declararon que sus esfuerzos de rastreo se utilizaron para evitar a las fuerzas policiales, mientras que el Gobierno chino declaró que los esfuerzos de los manifestantes se utilizaron para facilitar la emboscada de las fuerzas policiales. Independientemente de cuál de los argumentos fuera más cierto, los medios sociales claramente facilitaron la ejecución de la doctrina táctica—es decir, lograr y mantener el contacto, romper el contacto o llevar a cabo una emboscada.

Las fuerzas armadas de todo el mundo están aprovechando cada vez más los medios de comunicación social como el primer paso en el proceso de selección de blancos, es decir, para «encontrar» o «detectar» lo que finalmente estará «eliminado» o «enfrentado». Como explicaron Williams y Blum, «muchos analistas de inteligencia de todas las fuentes empiezan con la OSINT y luego agregan material de fuentes clasificadas» y, de esta manera, disminuyen rápidamente el tiempo y la energía necesarios para facilitar las operaciones de selección de blancos[8]. Los batallones, brigadas y divisiones serían negligentes si se abstuvieran de exhibir en las paredes de sus puestos de mando imágenes de las fuentes pertinentes de los medios de comunicación social adyacentes a sus mapas; el conocimiento de la situación que proporciona la OSIF en la era moderna es demasiado importante como para no tenerlo en cuenta. El campo de batalla se ha convertido en un entorno donde los ojos y oídos están en todas partes, para que tanto los amigos como los adversarios puedan recopilar y usarlo como les plazca. Parece que al menos una de las características de las operaciones ofensivas ha sido completamente derrotada: la sorpresa.

Comprender que «cada ciudadano es ahora un sensor» plantea la pregunta, «¿Cómo se puede mitigar esto?» O, invirtiendo la pregunta, «¿Cómo puede usarse como arma?». El resto del presente artículo explorará estas preguntas y abordará algunas de sus implicaciones.

El bombardeo de eventos

Se aconseja a los profesionales capacitados de la OSINT que cuestionen la autenticidad y la credibilidad de la OSIF que proviene de los medios sociales debido a la prevalencia del engaño y el sesgo. Pero, ¿cómo verifica exactamente un practicante la credibilidad y la autenticidad de un mensaje en Twitter? La respuesta habitual es corroborar esta información con información de al menos otra disciplina de inteligencia y, posteriormente, convertir la información de datos brutos de una sola fuente cuestionable en un producto analítico acabado veraz de múltiples fuentes. Aunque este proceso es el estándar de oro, puede ser complejo o difícil—especialmente cuando los analistas están apoyando el rápido ritmo de las operaciones de nivel táctico. A menudo, los analistas dependen de la corroboración a través de múltiples intentos de recopilación del mismo sensor (o similar). Un ejemplo de esto, fuera de la OSINT, podría ser el uso de dos fuentes de inteligencia humana distintas para corroborar una información, o el uso de dos fuentes de vídeo de movimiento completo de sistemas de aeronaves no tripuladas para corroborar una información.

Después de que Pekín intensificara la presión sobre las empresas extranjeras que se considera que prestan apoyo al movimiento prodemocrático de Hong Kong, Apple eliminó la aplicación «HKmap.live», el 10 de octubre de 2019, porque permitía a los manifestantes de Hong Kong seguir los movimientos de la policía. (Foto ilustración: Philip Fong, Agence France-Presse)

Los analistas de OSINT a menudo pueden recurrir, y lo hacen, a la agregación de OSIF de muchas fuentes para realizar un proceso similar. Williams y Blum explican que «[un] solo tuit de Twitter que refleje la opinión de un individuo al azar sobre el Estado Islámico de Iraq y al-Sham (ISIS) no tiene casi ningún valor de inteligencia; sin embargo, sintetizar todos los tuits de las opiniones sobre el ISIS dentro de un área geográfica tiene un gran valor de inteligencia»[9]. Penninger ofrece otro ejemplo al recomendar un rastreo en la web de una zona geográfica (en este caso, un pueblo) antes de una misión para determinar el sentimiento de base de la población—y observar los cambios en el sentimiento mientras las fuerzas de EUA ejecutan su operación. En este caso, Penninger argumenta, los cambios en el sentimiento del pueblo pueden ayudar a los comandantes de las fuerzas terrestres a «tomar decisiones informadas» y a «adaptar sus actos para alcanzar de la mejor manera posible el resultado deseado por el mando superior»[10].

Con el creciente uso de bots (programas automatizados), inteligencia artificial y aprendizaje automático, surge la posibilidad de que los adversarios fabriquen completamente, inflen artificialmente o enmascaren tendencias, patrones, ideas, eventos o acciones existentes. En «Commanding the Trend» de Jarred Prier, se describe la creciente sofisticación y eficacia del «secuestro de tendencias» en las redes sociales. Explica que «las cuentas bot son cuentas no humanas que tuitean y retuitean automáticamente basándose en un conjunto de reglas programadas», que posteriormente inflan una determinada narrativa (véase la figura 2 para un ejemplo)[11]. Además, señala que, en 2017, Twitter estimó que casi el 15 % de sus cuentas eran cuentas de bots[12]. Individuos, grupos o Estados nación enteros pueden dedicar sus recursos al secuestro de

tendencias con el fin que deseen. Por ejemplo, un grupo supremacista blanco anunció en junio de 2020 el inicio del Proyecto SOCH (Solar Orbiting Casaba Howitzer), cuyo objetivo es construir «un sistema de automatización [...] capaz de generar rápidamente

(Captura de pantalla del autor a través de Twitter)

Figura 2. Ejemplo de una red de bots en Twitter

cuentas en las redes sociales con el clic de un botón, facilitando [...] la presencia en plataformas fuertemente censuradas»[13]. Si bien los eruditos como Prier contemplan las implicaciones nacionales y estratégicas del secuestro de tendencias, las mismas preocupaciones pueden filtrarse también al nivel táctico.

Además de los bots, los adversarios también pueden aprovechar la *spoofing* (falsificación de datos) de GPS para generar falsas geoetiquetas asociadas a sus mensajes en las redes sociales. No solo los Estados nación o grupos sofisticados son capaces de *spoofing* por GPS, sino que los no combatientes también pueden hacer lo mismo. Las aplicaciones disponibles en el mercado, como «Fake GPS Location-GPS Joystick», permiten a cualquiera anular los sistemas GPS internos de sus teléfonos inteligentes con solo un poco de esfuerzo. La *spoofing* del GPS también puede organizarse y dirigirse a lugares designados. Janus Rose explica que, en 2016, un grupo «escaneó y muestreó los perfiles de 60 redes Wi-Fi cercanas [... y] retransmitió esas redes» y, en consecuencia, permitió a cualquier persona con acceso a Internet engañar a sus teléfonos haciéndoles creer que se encontraban en la Embajada de Ecuador[14].

Volviendo a nuestro pelotón de infantería que opera en las cercanías de una aldea, es entonces factible que un adversario pueda inflar artificialmente o fabricar directamente una tendencia o «evento» que indique a un analista desprevenido que hay una amenaza emergente en el área. Si nuestro analista que apoya a ese pelotón de infantería geofija sus parámetros de búsqueda para que coincidan aproximadamente con los límites de la aldea, entonces tal vez solo docenas de tuits y retuits podría cambiar fundamentalmente el sentimiento o la amenaza ostensible residente en la aldea. Si nuestro analista no puede corroborar la amenaza emergente con una disciplina de inteligencia independiente, entonces debe depender de la OSIF agregada de los medios sociales y generar un informe OSINT para el comandante de la fuerza terrestre. Al comandante le quedan entonces tres opciones: solicitar el apoyo de RISTA del cuartel general superior, redirigir sus propios sensores o simplemente confiar en la inteligencia que se le ha entregado y reaccionar como corresponde.

Si bien la gravedad de este caso puede parecer relativamente benigna (o simplemente otro ejemplo del «ruido blanco» con el que los analistas están demasiado familiarizados), la ampliación de este conjunto de problemas a su siguiente evolución natural plantea algunas preocupaciones serias. Imaginemos que nuestro analista observa tres acontecimientos emergentes: los combatientes se han concentrado en la aldea al este, un equipo de morteros se ha establecido a cuatro kilómetros al oeste y el puente necesario para la salida al sur ha sido destruido. Pues bien, ahora hay tres eventos que el analista, el cuartel general superior y el comandante de la fuerza terrestre deben confirmar. Se han desarrollado e identificado tres nuevas áreas de interés y requerimientos de inteligencia, tres nuevos eventos necesitan ser corroborados a través de medios distintos de RISTA y el comandante de la fuerza terrestre debe tomar una decisión sobre su siguiente acción. Ahora aumenta el número de eventos de tres a diez. Este método de inundar a una fuerza terrestre con las tendencias posiblemente falsas de OSIF a través de los medios de comunicación social puede denominarse un bombardeo de eventos. Si asumimos que los medios de RISTA disponibles serán redirigidos para responder a estos requisitos de inteligencia emergentes, entonces debemos recordar que estos medios también han sido distraídos de la misión que se les encomendó originalmente, que probablemente era recopilar informaciones sobre los requisitos de inteligencia prioritarios que tenían un mérito genuino. El bombardeo de eventos puede ser utilizado como un medio para poner una tensión increíble en los medios disponibles de RISTA, interrumpir los planes de recolección y enmascarar las fuentes de inteligencia genuinas. En este sentido, el bombardeo de eventos puede considerarse como un medio de fuego no letal, que obstaculiza deliberadamente el ciclo de decisión de los altos mandos, y que tiene como objetivo perturbar las operaciones tácticas en el peor de los casos y neutralizarlas en el mejor.

Un analista o comandante frustrado que descarte por completo la información durante un bombardeo de eventos podría generar problemas aún mayores. Como se discutió en la primera parte del presente artículo, la OSIF y los medios sociales ofrecen a los analistas y a los comandantes una increíble ventaja sobre el terreno. Las fuerzas militares cada vez más son incapaces de maniobrar en el campo de batalla sin ser observadas e reportadas por los ciudadanos común y corrientes. Además, si consideramos que todavía hay personas *reales* que informan *genuinamente* sobre el movimiento de personal —incluso en medio de un bombardeo de eventos— entonces uno (o más) de los eventos emergentes puede ser genuinamente cierto. Y si suponemos que el bombardeo de eventos se compone completamente de eventos inminentes o de alta prioridad, entonces la fuerza terrestre y los analistas de apoyo están así *obligados* a corroborar todo lo que ven para determinar exactamente qué eventos son verdaderos.

Un adversario podría lanzar bombardeos de eventos para hacer algo más que interrumpir las

Elementos gráficos de myriammira and starline via Freepik, www.freepik.com. Gráfico compuesto: Arin Burgess, Army University Press

operaciones de EUA en curso. Pueden utilizarse para enmascarar los movimientos del adversario, impedir que las fuerzas de EUA entren en una zona, complicar la validación de los objetivos, interrumpir las líneas de comunicación terrestres, atraer a las fuerzas de EUA a una zona o aumentar el desarrollo de la zona de combate del adversario. Esto es especialmente cierto si los adversarios toman incluso los pasos más marginales para complementar el bombardeo de eventos en curso fuera de los medios sociales mediante el uso de vídeos generados por computadora, falsificaciones profundas, literatura gris fabricada o informes mediáticos o pequeñas pruebas físicas o electrónicas fabricadas que podrían llevar a una falsa corroboración. Por ejemplo, si un adversario desea interrumpir las líneas de comunicación terrestres, podría realizar un bombardeo de eventos en la zona deseada y hacer que un solo actor perturbe la tierra en ese lugar (para replicar el emplazamiento de un artefacto explosivo improvisado), engañando en última instancia el análisis de las imágenes. Los bombardeos de disturbios civiles podrían corroborarse falsamente mediante vídeos reutilizados (o generados por computadora) y varios neumáticos en llamas. La concentración de guerreros podría corroborarse falsamente a través de una persona con una radio que transmitiera información incorrecta a través de la red para engañar el análisis de las comunicaciones. Aunque estos ejemplos son excesivamente sencillos, el hecho es que el bombardeo de eventos tiene el potencial de convertir los esfuerzos iniciales de engaño de informes de una sola fuente en informes de múltiples fuentes que parecen legítimos.

Como ejemplo de corroboración falsa de eventos de disturbios civiles, considere la confusión que rodea a la Zona Autónoma de Capitol Hill de junio de 2020 en Seattle. Más allá de las narrativas opuestas que se tejen en el submundo de las redes sociales, reportando los «hechos sobre el terreno», los propios medios de comunicación dominantes fueron víctimas (o contribuyeron deliberadamente) al caos. Por ejemplo, Fox News mostró una imagen de guardias armados ocupando la zona, pero retiró la imagen poco después de que el periódico *Seattle Times* señalara que la imagen era de un evento totalmente distinto que tuvo lugar en Minnesota. Aunque Fox News afirmó que la foto formaba parte de un «collage» que «no delinea claramente» las imágenes de Seattle y de otros acontecimientos en todo el país, el hecho es que las líneas entre la realidad digital y la física se difuminaron hasta el punto de oscuridad[15].

La mayoría de estos ejemplos han estado orientados a la contrainsurgencia, pero la aplicación del bombardeo de eventos durante las operaciones de combate a gran escala podría ser igual de eficaz, por no decir más. Considere la tensión adicional que un bombardeo de eventos podría producir en las operaciones ya muy complejas, como una división o brigada que lleva a cabo la recepción, concentración, movimiento hacia adelante e integración; la ejecución de un cruce de brecha fluvial o la realización de un paso de avance de líneas. En estos casos, un Estado nación podría lanzar varios bombardeos de eventos, presentando simultáneamente múltiples dilemas a un comandante en medio del mando y control de una operación ya multifacética. Un grupo o Estado nación con una visión del futuro podría incluso tener múltiples bombardeos de eventos prefabricados y listos (y sus medidas complementarias) para entregarlos en momentos o lugares clave. Los bombardeos de eventos pueden fabricarse con días, semanas o meses de antelación. Las crisis humanitarias, represas rotas, disturbios civiles, puentes destruidos y falsas brigadas blindadas podrían prácticamente aparecer en muchas partes del campo de batalla, sobrecargando los recursos disponibles de RISTA y desviando los esfuerzos de reconocimiento de EUA contra objetivos genuinos. Los bombardeos de eventos «en cascada» podrían desviar cada vez más la atención de EUA de los objetivos genuinos, y el enemigo solo tendría que hacer realidad un bombardeo de eventos ocasional para obligar a Estados Unidos a concentrarse en eventos falsos.

Para llevar a cabo un bombardeo de eventos eficaz es fundamental obtener la participación del mayor número posible de actores cibernéticos distintos. Aunque un ejército de bots controlado por un pequeño grupo de personas tiene el potencial de fabricar y/o inflar un acontecimiento determinado, las técnicas y tecnologías empleadas actualmente suelen poder identificar y, por lo tanto, eliminar o descartar un acontecimiento o una tendencia de aspecto particularmente inauténtico. El análisis léxico avanzado, análisis del uso de palabras clave y perfil de frecuencia de las mismas pueden utilizarse para atribuir un texto escrito a un grupo o sector demográfico específico o incluso a un solo autor[16]. Por

ejemplo, si un conjunto inicial de tuits o artículos en los que se comenta una crisis humanitaria emergente presenta características distintivas de escritura de un grupo nefasto conocido, este hecho puede descartarse como un mero intento de desinformación. Sin embargo, si el evento gana terreno en el público mundial más grande y miles de personas comentan, publican o contribuyen con sus propios textos o imágenes al debate, hay que dedicar más energía y tiempo a filtrar lo que es real y lo que es falso. Consideremos la tendencia #DCblackout de 2020 en Twitter; iniciada por solo tres seguidores, el hashtag explotó en cuestión de horas a pesar de los intentos de Twitter por detener la campaña de desinformación. Medio millón de personas retuitearon el suceso y gran parte del país creyó que el Gobierno cerró la Internet local para reprimir los disturbios civiles[17]. Aunque al final, la ilegitimidad de #DCblackout quedó al descubierto, la confusión inicial producida por el evento sirve como ejemplo convincente de los efectos potencialmente perturbadores que puede tener un bombardeo de eventos en operaciones tácticas optimizadas y rápidas.

No debe subestimarse el potencial de un bombardeo de eventos para convertirse en una doctrina adversaria. Aunque no se le denominaba un «bombardeo de eventos», quizás la primera forma de esta táctica en sus inicios se manifestó en Ucrania en 2014. Aunque el análisis de los acontecimientos en Ucrania ha sido ampliamente cubierto por pensadores políticos y estratégicos de todo el mundo, vale la pena señalar varios puntos clave. Rusia demostró la capacidad de influir en las protestas ucranianas en 2014 con «una red de docenas de grupos de medios sociales [...] utilizados para difundir rumores falsos para socavar las tropas ucranianas o desacreditar a los líderes del ejército»[18]. Los propios soldados ucranianos fueron blancos directos de los «mensajes del Servicio de Mensajes Cortos [SMS], que llegaron a sus teléfonos móviles probablemente desde los sistemas de guerra electrónica rusos»[19]. En último lugar, los actores rusos utilizaron métodos sencillos, como los «trolls en bikinis» que lucían fotos de perfil de mujeres atractivas, para ganar seguidores digitales y derrotar «algunas de las herramientas de análisis de trolls y bots»[20]. Estas características de la entrega digital de eventos informativos, seleccionando de lugares y personas específicas y contrarrestando las herramientas analíticas de búsqueda de engaños son indicadores de una doctrina creciente que podría ser organizada en un nivel táctico.

Otra consideración que debemos tener en cuenta es el análisis coste-beneficio de la realización de un bombardeo de eventos. ¿Merece la pena el coste de los recursos, organización y realización de un evento de este tipo? La mejor manera de plantear esta cuestión es comparando el análisis coste-beneficio con otros tipos de obstáculos, fuegos letales y no letales, y esfuerzos militares de engaño. En primer lugar, como señala Penninger, la Agencia de Investigación de Internet de Mikhail Burchik, una empresa rusa directamente responsable de las continuas campañas de desinformación en Estados Unidos, operó con un presupuesto de «un solo dígito de millones de dólares para un par de años de acoso y perturbación»[21]. Además, RAND señala que en la fábrica rusa de trolls de San Petersburgo, «los empleados cobran al menos US$ 500 al mes por gestionar cuentas falsas, difundiendo propaganda y desinformación»[22]. Combinando estas cifras, parece lógico que un equipo de unos cincuenta actores cibernéticos rusos dedicados podría llevar a cabo una campaña de desinformación continua e integral por unos US$ 40 000 al mes. También debemos recordar que este gasto incluye el coste de la compra de anuncios y el funcionamiento de innumerables servidores y redes de bots relacionadas. Por lo tanto, el coste de un mes de operaciones de esta cohorte relativamente pequeña equivaldría a poco menos de la mitad de un solo misil Hellfire, unos cuarenta proyectiles de obús no guiados, o cuatrocientos proyectiles de 30 mm entregados desde un helicóptero AH-64 Apache. O, el coste de un mes de bombardeo de eventos podría equivaler a solo diez horas de vuelo de un solo MQ-1B Predator[23].

Lanzar un bombardeo de eventos es una forma barata, precisa y rápida de perturbar la toma de decisiones tácticas de Estados Unidos, sobrecargar los recursos de RISTA, generar efectos ventajosos en el campo de batalla y degradar el valor de la OSIF disponible. Generar y lanzar un bombardeo de eventos está ciertamente dentro de la capacidad de la mayoría de los Estados nación modernos, de muchos grupos adversarios, y quizás incluso de actores cibernéticos solitarios armados con formidables ejércitos de bots.

El fin de la OSINT en el nivel táctico

Las consecuencias del bombardeo de eventos, las campañas de desinformación, el secuestro de tendencias y el engaño militar restarán fundamentalmente utilidad a la OSINT a nivel táctico. La información en Internet no es una entidad abstracta e independiente, relativamente maleable, pero sí es capaz de mantener su verdadera forma a pesar de los repetidos esfuerzos de los usuarios interconectados por pincharla, empujarla y manipularla continuamente. Más bien, la información en Internet *son* los usuarios interconectados que habitan ese dominio y su contenido se manifiesta con base en la voluntad y poder de esos usuarios. A medida que Internet crece y se expande, también lo hacen las capacidades de los Estados nación y actores para cambiarla. Al igual que el pelotón de infantería cerca de la aldea, la información obtenida de Internet será cuestionada hasta el punto de ser prácticamente inútil. En lugar de responder a las necesidades de información, la OSIF simplemente servirá para generar *más* necesidades de información. En realidad, ¿hay un disturbio en Kabul? ¿El enemigo acaba de reubicar una de sus baterías Pantsir? ¿Está destruido el puente de mi ruta de salida?

Tal vez no sea demasiado lejos conjeturar que los Estados nación consideren un *deber* de los ciudadanos inundar Internet con información falsa. A diferencia del lema de guerra del siglo XX «labios sueltos hunden buques», podríamos presenciar un mundo en el que los Gobiernos animen a los ciudadanos a inundar el dominio digital con información falsa. Esto no solo serviría para proteger las vidas de los soldados desplegados y/o frustrar los planes del enemigo, sino que también podría llevarlo a cabo cualquier ciudadano con un teléfono inteligente y acceso a Internet, sin importar la distancia geográfica del combate. De hecho, los Gobiernos podrían incluso ofrecer incentivos monetarios o civiles para impulsar a los ciudadanos a realizar campañas de desinformación, quizás en forma de exenciones fiscales o medallas de ciudadanía. Cuanto mayor sea el número de personas que contribuyan a la difusión de eventos y a la desinformación, mayor será la probabilidad de éxito. Un millón de personas diferentes publicando, tuiteando, retuiteando y escribiendo derrotarán los mecanismos destinados a identificar las campañas de desinformación en línea, como el análisis léxico, el análisis de redes o el análisis geoespacial. De hecho, el planteamiento bélico de «toda la nación» podría fomentar la concentración y militarización de la información de fuente abierta a niveles nunca vistos.

Recomendaciones

Existen varias opciones para superar los efectos perjudiciales de un bombardeo de eventos, el secuestro de tendencias y las campañas de desinformación específicas, aunque ninguna es ideal por sí sola: (1) como nación, seguir dedicando recursos y energía al desarrollo de mejores herramientas y procesos de análisis para lidiar con la creciente desinformación en Internet; (2) controlar nuestra dependencia de las redes sociales como medio de seguimiento de las actividades de adversarios en el combate y (3) atacar agresivamente las redes de bots de adversarios, las fábricas de trolls y los actores nefastos conocidos durante las actividades de configuración global y de teatro. Con una combinación de los tres esfuerzos, podríamos ver reducido el riesgo para nuestra fuerza y misión y posiblemente salvaguardar la utilidad de la OSIF.

El desarrollo de herramientas cada vez más avanzadas para hacer frente a las nuevas amenazas cibernéticas ha sido una política de defensa estadounidense desde los albores de la era informática[24]. Sin embargo, podríamos beneficiarnos de la revisión de procesos y procedimientos sencillos. Por ejemplo, el registro de todas las importantes redes de bots, adversarios cibernéticos y sus huellas digitales relacionadas, la consolidación de esa información en un lugar centralizado y filtrable, así como la difusión de esa información a los analistas de nivel táctico para una rápida referencia cruzada podría ayudar a aliviar las implicaciones de la OSIF militarizada[25]. En 2017, en un estudio de la Corporación RAND se señaló la necesidad de que los equipos de combate de brigada aumenten sus capacidades cibernéticas defensivas y ofensivas, en parte debido a la necesidad de los comandantes de brigada de «responder con suficiente rapidez a tales eventos en lo que probablemente sea un entorno dinámico y rico en información»[26]. Sin lugar a dudas, encarar un ciberataque no letal tal como un bombardeo de eventos cuenta como una de estas instancias y se mitigaría, al menos parcialmente, con la sincronización o integración de los profesionales de la cibernética e inteligencia a nivel táctico. Además, la estandarización y refuerzo en el entrenamiento de OSINT para los

analistas de nivel táctico permitiría la difusión de las mejores prácticas y las lecciones aprendidas, e informaría a todas las partes implicadas de las amenazas y tendencias emergentes. Aunque los procedimientos militares convencionales prohíben la práctica de OSINT entre los analistas no entrenados, sería ingenuo suponer que los analistas ignoran por completo la OSIF, especialmente cuando un mayor porcentaje de la población mundial informa deliberadamente de las actividades del adversario. E incluso si los analistas de todas las fuentes se abstienen de incorporar abiertamente la OSIF en sus evaluaciones, su exposición a la información en los medios sociales probablemente contribuirá a formas de sesgo o análisis inherentemente defectuoso.

Además de aumentar el entrenamiento, optimizar el intercambio de información e integrar los expertos cibernéticos en el nivel táctico, también debemos asegurarnos de abordar la OSIF con mayor precaución que la practicada anteriormente. Con el creciente uso de redes de bots y el secuestro de tendencias por parte del adversario, la agregación de OSIF a partir de muestras de pequeño tamaño podría plantear preocupaciones legítimas por los resultados sesgados y, en consecuencia, podría permitir al adversario manipular o predecir futuras acciones militares de EUA. La información obtenida de una muestra de pequeño tamaño geográfica o demográficamente fijada debe tratarse siempre con un alto nivel de escepticismo, y debe darse prioridad a la necesidad de corroboración por parte de disciplinas de inteligencia ajenas a la OSINT. Lamentablemente, muchos adversarios de EUA reconocen este mismo hecho, lo que actualmente está impulsando a países como China y Rusia a desarrollar e instituir su propia intranet nacional o a censurar en gran medida la información que llega a su país desde la Internet mundial[27].

En último lugar, neutralizar las actividades de las entidades adversarias responsables de llevar a cabo bombardeos de eventos y campañas de desinformación debería ser una de las principales prioridades de Estados Unidos durante las fases de configuración y disuasión de cualquier operación militar que prevea el despliegue de tropas. Aunque atacar los esfuerzos de nefastos actores cibernéticos no es ni mucho menos un concepto innovador, es importante señalar cuán difícil sería conseguirlo con eficacia, especialmente si tenemos en cuenta la facilidad con la que algo como un bombardeo de eventos podría proyectarse rápidamente por todo el mundo. Por ejemplo, los controladores de las redes de bots en Rusia podrían, y probablemente lo harán, realizar campañas de desinformación específicas en apoyo de operaciones terrestres en guerras proxy en las que no participan abiertamente. Además, las dificultades para superar los límites jurídicos y políticos internacionales entre los Estados nación podrían suponer un grave problema a la hora de contrarrestar las actividades de actores que viven en otras naciones soberanas. Como hemos visto a lo largo de las últimas décadas, la mera atribución de un actor o actores a un único ciberataque es suficientemente difícil, por no hablar de seguir con un esfuerzo de represalia o de ciberataque preventivo. Sin embargo, debemos a los altos mandos responsables por el bienestar de sus soldados y de la seguridad de esta nación desarrollar y aplicar mecanismos para superar estos obstáculos. ■

Notas

1. Libor Benes, «OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm», *Journal of Strategic Security* 6, nro. S3 (2013): S24, http://dx.doi.org/10.5038/1944-0472.6.3S.3.

2. Heather J. Williams e Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), 3, accedido 22 de octubre de 2020, https://www.rand.org/pubs/research_reports/RR1964.html.

3. Ben Sullivan, «Twitter's the Only Tool You Need for Tracking the Military», Vice News, 24 de abril de 2017, accedido 22 de octubre de 2020, https:// www.vice.com/en/article/wn3g99/twitters-the-only-tool-you-need-fortracking-the-military.

4. Ron Penninger, «Operationalizing OSINT Full-Spectrum Military Operations», Small Wars Journal, 14 de enero de 2019, accedido 22 de octubre de 2020, https://smallwarsjournal.com/jrnl/art/operationalizing-osint-full-spectrum-military-operations.

5. Williams y Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, 34.

6. «About», Live Universal Awareness Map, accedido 22 de octubre de 2020, https://usa.liveuamap.com/about#history.

7. «Libya», Live Universal Awareness Map, accedido 22 de

octubre de 2020, https://libya.liveuamap.com/en/2020/26-june-6-antiaircraft-russianmade-pantsyr-vehicles-arrived.

8. Williams y Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, 37.

9. *Ibid*., 10.

10. Penninger, «Operationalizing OSINT».

11. Jarred Prier, «Commanding the Trend: Social Media as Information Warfare», Strategic Studies Quarterly 11, nro. 4 (2017): 54, accedido 22 de octubre de 2020, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

12. *Ibid*.

13. «White Racially Motivated Violent Extremists Developing Program to Create Bulk Social Media Accounts», Open Source Intelligence Bulletin 20-06-59 (Orlando, FL: Central Florida Intelligence Exchange, 25 de junio de 2020).

14. Janus Rose, «Spoofing Tool Lets You Catch Pokémon from Julian Assange's Embassy Prison», Vice News, 19 de julio de 2016, accedido 22 de octubre de 2020, https://www.vice.com/en/article/53d5pk/skylift.

15. Jesse Drucker, «Fox News Removes a Digitally Altered Image of Seattle Protests», New York Times (sitio web), 23 de junio de 2020, accedido 22 de octubre de 2020, https://www.nytimes.com/2020/06/13/business/media/fox-news-george-floyd-protests-seattle.html.

16. Williams y Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, 24–25.

17. Kate O'Flaherty, «Twitter Suspends Accounts Posting about DC Blackout for Spreading 'Misinformation'» Forbes (sitio web), 2 de junio de 2020, accedido 22 de octubre de 2020, https://www.forbes.com/sites/kateoflahertyuk/2020/06/02/twitter-suspends-accounts-posting-about-dc-blackout-for-spreading-misinformation/#4375b9f8530d.

18. Todd C. Helmus y col., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Monica, CA: RAND Corporation, 2018), 16.

19. *Ibid*.

20. *Ibid*., 23.

21. Penninger, «Operationalizing OSINT».

22. Helmus y col., *Russian Social Media Influence*, 22.

23. Mark Thompson, «Costly Flight Hours», Time (sitio web), 2 de abril de 2013, accedido 22 de octubre de 2020, https://nation.time.com/2013/04/02/costly-flight-hours/.

24. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, diciembre de 2017), 12–13.

25. «Spamhaus Botnet Controller List», Spamhaus, accedido 3 de noviembre de 2020, https://www.spamhaus.org/bcl/. Véase la Lista de Controladores de Redes de Bots como un ejemplo de un planteamiento para consolidar y rápidamente difundir grandes cantidades de redes de bots conocidas.

26. Isaac R. Porche III y col., «Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below» (Santa Monica, CA: RAND Corporation, 2017), 2.

27. Jane Wakefield, «Russia 'Successfully Tests' Its Unplugged Internet», BBC News, 24 de diciembre de 2019, accedido 22 de octubre de 2020, https://www.bbc.com/news/technology-50902496.