El deber de advertir

Cómo ayudar a EE.UU. a luchar contra la desinformación rusa

Mayor William Giannetti

Una evaluación de la comunidad de inteligencia no secreta publicada en enero de 2017 por el Consejo de Inteligencia Nacional (NIC) afirmaba que Rusia interfirió en la elección presidencial de EE.UU. Esta operación de interferencia fue dirigida por el presidente Vladimir Putin y ejecutada por servicios de inteligencia civiles y militares de Rusia: el Servicio de Seguridad Federal y el Directorio de Inteligencia Principal. El informe del NIC siguió a una investigación de la comunidad de inteligencia de EE.UU. en correos electrónicos robados del Comité Nacional Democrático en 2016. Los correos electrónicos contenían comunicaciones sensibles entre líderes del partido demócrata, miembros del personal superiores y el candidato del partido para las elecciones presidenciales, que una vez expuestos, sirvieron para avergonzarlos y desacreditarlos. El NIC evaluó que estos correos electrónicos fueron robados por piratas informáticos rusos asociados con las organizaciones mencionadas antes. Los piratas informáticos entregaron deliberadamente los correos electrónicos a WikiLeaks, un grupo secreto antigubernamental, que publicaron inmediatamente sus detalles comprometedores a los medios de comunicación. La estratagema rusa era una parte de un plan para "denigrar" al candidato del partido demócrata y alejar la opinión del público estadounidense de ella y hacia el oponente republicano.[1]

La evaluación, de ser cierta, detalla una de las ciberoperaciones más elaboradas realizadas por una nación estado contra Estados Unidos y su proceso político. Para denigrar al candidato, agitadores en línea, provocadores llamados "trolls", publicaron desinformación que afirmaba que tenía diversas enfermedades ficticias y una mala salud mental. Las emisoras estatales rusas de habla inglesa, como *Russia Today* (*RT*) y *Sputnik* en línea, publicaron historias que vituperaban a la candidata mientras que presentaban a su oponente como un blanco de una cobertura mediática injusta por parte de emisoras de noticias tradicionales que "servían a un establecimiento político corrupto".[2] Hasta este punto, las ciberoperaciones hostiles supuestamente han sido sinónimas de tácticas de "pesca con arpón", que hacen que las víctimas divulguen códigos de acceso sin sospechas, o con ataques de negación de servicio que pueden interrumpir o degradar sistemas informáticos. De todas formas, si son llevados a cabo de forma habilidosa por sus perpetradores, los ciberoperadores también pueden manipular información, esa materia tan intangible pero valiosa de la que Winn Schwartau escribió proféticamente hace más de 20 años con el fin de desinformar, confundir y desorientar a todo un electorado.[3]

¿Qué puede hacer la Fuerza Aérea acerca de un ataque refinado de esta naturaleza que usa el espacio cibernético como vehículo de llegada? Tiene una doctrina de operaciones ciberespaciales que se concentra principalmente en proteger infraestructura de tecnología basada en la web contra ataques catastróficos y sugiere métodos de sentido común para la defensa de la misma, como mantener cortafuegos o instalar software antivirus para protegerse contra las intrusiones.[4] No obstante, ¿cómo "podemos pasar a la ofensiva" y proteger a la nación contra campañas de desinformación como la descrita en el informe de la comunidad de inteligencia? Tal vez no se requiera una lógica o un código informáticos, sino que probablemente se necesitará un esfuerzo concertado, combinado iniciado por profesionales de la policía, de inteligencia y cibernéticos para combatir el problema. Los países europeos, como Chequia, están preparándose para defenderse examinando el contenido de la web para ver si hay desinformación y haciéndolo saber a su público.[5] No se puede negar que también es un trabajo importante para proteger sistemas informáticos del gobierno y militares; si están en peligro debido a una amenaza nacida del ciberespacio, entonces los guerreros ciberespaciales óptimos de la Fuerza

Aérea tienen el deber de advertir sobre su colapso inminente. Así pues, ¿tenemos todos el deber de advertir cuándo la desinformación llega a nuestro litoral y amenaza con subvertir o descarrilar nuestro proceso político?

El inicio de una nueva época

En 2005, la Fuerza Aérea reconoció abiertamente estar dispuesta a volar, combatir y ganar en el aire, el espacio y el ciberespacio. Esta era una declaración atrevida porque fue la primera vez que un arma, en un lugar, consideró el ciberespacio como un dominio a ser conquistado en una situación presumiblemente bélica. Ese mismo año, la World Wide Web había evolucionado a su estado actual: Web 2.0. Ya son historia los días de los años 90 cuando los sitios web y su contenido eran estáticos e incómodos. En el mundo actual de la Web 2.0, todo, absolutamente todo el contenido es dinámico y está definido por el usuario. No hace falta decir que esta fue una revolución en términos de cómo nos comunicamos entre sí, desde un nivel individual, hasta el fondo de los pasillos del más alto nivel del poder nacional. Un año después, ocurrió una cosa fascinante. En 2006, técnicos del Laboratorio Nacional de Idaho llevaron a cabo un ensayo en un generador industrial diésel con el fin de piratear sus sistemas de control y desactivarlos desde lejos. Los técnicos establecieron una base de operaciones a 160 kilómetros y explotaron la vulnerabilidad en el código de control de la máquina.[6] Su interferencia hizo que los convertidores eléctricos de la máquina de 1 tonelada se encendieran y apagaran en una sucesión tan rápida que empezaron a vibrar, recalentarse y con el tiempo a autodestruirse en medio de una humareda.[7] Las potentes imágenes, cuando se retransmitieron por televisión, fueron un anticipo del tumulto que podría esperarnos. Lo que este ejemplo también demostró es que, en un sentido, las máquinas que nos proporcionan energía y luz estaban casi tan conectadas como lo estaban siendo los seres humanos a nivel individual. Mostró que un generador podría desactivarse usando un código malicioso desplegado remotamente y que nuestros peores temores sobre la vulnerabilidad de nuestra infraestructura crítica en esta nueva época de la interconectividad podrían hacerse realidad. Esta nueva realidad se hizo más palpable en la diminuta nación báltica de Estonia en 2007.

Ese año, Estonia, con una conectividad del 95 por ciento, era presuntamente la nación más conectada del mundo. En abril, se decidió que un monumento de la época soviética dedicado a los soldados rusos que murieron durante la Segunda Guerra Mundial fuera trasladado desde el centro de su capital Tallin hasta las afueras de la ciudad. Los estonios de habla rusa se echaron a las calles ese mes en una protesta masiva. Lo que siguió fue aún más preocupante: una avalancha de ataques de negación de servicio distribuido usando una red de robots refinada de un número estimado de 85,000 computadoras causó una desaceleración abrupta en la infraestructura de comunicaciones y bancos de la nación.

Estonia resistió los ataques durante la fiesta del Día de la Victoria de Rusia ese mayo, que conmemora la victoria soviética sobre la Alemania nacionalsocialista, cuando 58 sitios web se desconectaron a la vez, y los servicios de su institución financiera más grande no estuvieron disponibles durante 90 minutos. Los cortes de corriente continuaron hasta fines de mayo y, aunque los daños políticos, sociales y económicos eran observables, los daños físicos eran "menores".[8] Naturalmente, el origen de los ataques no pudo localizarse y, aunque todo apuntaba a Rusia, Moscú rechazó completamente su participación en los ataques. Inicialmente, la evidencia aportada por las autoridades estonias apuntaba a que el origen de los ataques eran direcciones rusas de protocolos de internet (IP). Los estonios retiraron esta afirmación porque se determinó que la evidencia no era concluyente.

Seguirían otros ataques de esta clase. En diciembre de 2016, en la región de Ivano–Frankivsk de Ucrania, un técnico de una planta eléctrica supuestamente fue testigo de cómo el cursor de su terminal empezó a moverse y, de una manera muy deliberada, empezó a apagar los disyuntores de esta subestación, sumergiendo aproximadamente a 230.000 personas en la oscuridad. El corte eléctrico duró entre una y seis horas y, afortunadamente, las compañías eléctricas ucranianas dañadas por el incidente tenían datos suficientes registrados por sus cortafuegos para reconstruir cómo se produjo la ruptura. Las fases preparatorias del ataque empezaron con una campaña de pesca con arpón clásica,

estilo de las de mediados de los 90, que tenía como objetivo los trabajadores de la planta eléctrica usando un documento de Microsoft Word incluido en un correo electrónico. Para descargar el documento y el malware interior, el usuario tendría que hacer un clic en un mensaje guía, que activaría los macros en su interior. Una vez activados, un guion corto en Visual Basic enviaría un comando a la computadora para buscar y registrar credenciales de conexión. Después de que los atacantes reunieran suficiente información de nombres de usuario y contraseñas, accedieron a los controladores del dominio de Windows de la compañía eléctrica, donde se guardaban más nombres de usuarios y contraseñas, hasta que encontraron credenciales para trabajadores que usaban redes privadas virtuales para conectarse remotamente con la red de Control de Supervisión y Adquisición de Datos de las compañías eléctricas. Desde allí, los piratas informáticos tomaron control remotamente de la estación eléctrica ucraniana prácticamente sin oposición.[9] El virus seguía siendo tan efectivo en 2016 como hace 20 años, aunque su código y medios de diseminación carezcan de originalidad.[10]

¿Guerra cibernética o guerra política?

Fijándose solo simplemente en estos incidentes, se podría concluir que lo que ocurre en las lejanas Estonia o Ucrania podría ocurrir concebiblemente aquí en casa, de modo que el enfoque de la Fuerza Aérea para protegerse a sí misma y a la infraestructura de redes del Departamento de Defensa (DOD) contra las intrusiones ciertamente parece suficientemente justificable. Tiene un interés implícito en proteger públicamente sistemas externos conectados por redes, así como porque al hacerlo se activa "el despliegue de fuerzas, el adiestramiento, el transporte y las operaciones normales".[11] Las actualizaciones rutinarias del antimalware deben llevarse a cabo de modo que se parcheen las últimas vulnerabilidades y las contraseñas para sistemas de control deben ser suficientemente fuertes para mitigar la posibilidad de que podrían resquebrajarse fácilmente.

No obstante, cuando hablamos de redes del DOD o redes públicas, casi no hay salvaguardas para prevenir la propagación de la desinformación, especialmente las que el NIC publicó con detalles deslumbrantes. El debate sobre instituir dichas salvaguardias se ha convertido inevitablemente en preguntas como, "¿Se piratea nuestra elección?" o "¿Fue esto el Pearl Harbor cibernético que las personas han imaginado durante muchos años?"[12] La respuesta a ambas preguntas es, enfáticamente, "no". La verdad es que lo que los rusos desataron no es una guerra cibernética, al menos no según nuestra forma clásica de entender cómo lo ilustran los estudios prácticos breves de arriba. En vez de eso, esta es una guerra política, la clase de guerra que hace uso del ciberespacio como medio de suministrar lo que los oficiales de inteligencia rusos podrían llamar *disinformatsiya* y *kompramat,* o información políticamente dañina.[13] De forma semifrecuente, el Departamento de Seguridad Nacional (DHS) publica boletines referentes a la propagación de códigos maliciosos e indica responsablemente a los ciudadanos y sus empresas cómo defenderse contra ellos. No obstante, lo que hizo que el ICA fuera tan especial fue el primer informe de su clase para alertar al público sobre la campaña de desinformación de Rusia, que fue diseñada para forzar un resultado ostensiblemente a su favor.

Por esa razón, Estados Unidos no es ajeno a las operaciones de desinformación de potencias extranjeras. Uno de los primeros ataques de la era moderna, y supuestamente más exitoso fue perpetrado, no por Rusia, sino por la Coordinación de Seguridad Británica (BSC) del Reino Unido. En su libro *The Irregulars (Los irregulares),* Jennet Conant nos cuenta la historia del BSC, que dirigía su red de espionaje desde Washington DC y el Centro Rockefeller de New York City. La regla general de la BSC en esa época era sacar a la nación de su mentalidad "EE.UU. primero", espolear un cambio en su política aislacionista de no intervención durante la Segunda Guerra Mundial y hacer que ofreciera su apoyo material a Europa. En un plan ingeniosamente engañoso, el jefe de la BSC, un ciudadano canadiense llamado William Stephenson, lideró la producción de un mapa alemán falso que describía refugios en el sur de Cuba, donde se encontraban alijos de equipos, lugares de radio para enviar señales a submarinos alemanes y un plan de posguerra para dividir los territorios del Atlántico Norte en protectorados nacionalsocialistas. Ivar Brice, un agente británico que trabajaba para la BSC en esa época, dijo que

Stephenson avisó a sus contactos de la Oficina Federal de Investigación (FBI) sobre la existencia del mapa y el refugio donde podía encontrarse. El mapa haría sonar la alarma en EE.UU. sobre el hecho de que la amenaza nacionalsocialista estaba más cerca de sus costas de lo que se pensaba anteriormente. "Si se descubriera o capturara de manos enemigas un mapa alemán de esta clase", escribió, "y se publicara. . . entre los partidarios de "América primero" con su creencia de que EE.UU. podía llevarse bien con Hitler, qué conmoción se produciría".[14]

La falsificación fue hallada por el FBI y suministrada a Stephenson, que la pasó al jefe de la Oficina de Servicios Estratégicos, el General William Donovan, quien, a su vez, la entregó al presidente Franklin D. Roosevelt. Como reacción, el presidente declaró en un discurso por radio, en marzo de 1941, que tenía en su posesión un "mapa secreto" que describía el artificioso plan nacionalsocialista e incluía lo que llamó "nuestra gran cuerda salvavidas" al Pacifico, el canal de Panamá. "Ese mapa, amigos míos", dijo el presidente, "pone en claro el diseño nacionalsocialista, no solo para Sudamérica, sino también para Estados Unidos". El presidente Roosevelt prometió que EE.UU. "remaría" ahora a favor de la lucha de Europa contra el fascismo y Alemania.[15]

En los años 60 y 70, antes de la época la Internet, la propaganda y desinformación rusas aparecieron en libros publicados por autores que fueron pagados para tomar parte en las operaciones del entonces Comité para la Seguridad del Estado (KGB) en Estados Unidos llamadas "medidas activas". La KGB financió y usó agentes comunistas como el italiano Carl Aldo Marzani, cuyas editoriales, el Liberty Book Club y el Prometheus Book Club, estaban entre las primeras en tener dudas sobre el hallazgo de la Comisión Warren de que Lee Harvey Oswald actuó en solitario durante el asesinato del presidente John F. Kennedy. Escritores empleados por Marzani, como Joachim Josten, quienes fueron financiados mediante subvenciones del Partido Comunista de la Unión Soviética, escribió libros que acusaban a Oswald de ser "un agente provocador del FBI con unos antecedentes de la CIA [Agencia de Inteligencia Central]."[16] Al hacer esto, según el archivista de la KGB y disidente Vasili Mitrokhin, estableció dos de las falsedades más persistentes del saber popular del asesinato de Kennedy: que hubo una conspiración del gobierno para matar al presidente, y que la CIA participó en ella.

De todos los agentes que aportaron ignominia a las puertas de la CIA en los 70, ninguno fue más dañino que Philip Agee. Agee fue el Edward Snowden de su día, un hombre que escribió tres libros que detallaban operaciones clandestinas de la CIA en todo el mundo y expuso a 2000 oficiales de la CIA. Agee, según Mitrokhin, fue despedido sumariamente de la CIA en 1968 debido a sus malos hábitos financieros y a que bebía en exceso. Como repulsa, primero trató de desertar con un paquete de documentos secretos a la oficina residente de la KGB en Ciudad de México. El profesional a cargo de la oficina de la Ciudad de México en esa época era Oleg Kalugin.[17] Kalugin, al detectar una trampa, rechazó a Agee. No obstante, Agee encontró con el tiempo a una audiencia deseosa en Cuba, cuyo servicio de inteligencia compartió la inteligencia robada con los rusos. La KGB, cuando se publicó la primera memoria de Agee, *Inside the Company (Dentro de la compañía)*, en 1975, no tuvo escrúpulos en atribuirse el mérito de ayudar al autor y a los cubanos a prepararlo. Así pues, no está claro, cuánta preparación o trabajo hizo realmente la KGB en el libro de Agee, pero el potencial desertor reconoció después que el Partido Comunista de Cuba, y el servicio de inteligencia cubano "animaron de forma importante en un momento en que dudé si podría encontrar la información adicional que necesitaba". La CIA, en su publicación *Studies in Intelligence (Estudios sobre inteligencia)*, según Mitrokhin, admitió que el trabajo de Agee fue un "golpe muy duro" para la agencia.[18]

El libro fue aclamado en todo el mundo mientras Agee vivía en el exilio en Londres. Poco después, se enfrentó a la deportación y, a medida que aumentó su reputación de chivato, políticos famosos de Inglaterra y Estados Unidos (incluido un antiguo fiscal de EE.UU.) salieron en defensa de sus acciones. Mitrokhin cuenta en el archivo de la KGB de Agee, que se iniciaron campañas de apoyo para su *causa célebre* en nueve naciones. Al final fue forzado a salir de Londres en dirección a los Países Bajos en 1977, pero la KGB estaba "jubilosa" del caos que había causado todo el asunto, y del bochorno que sufrió la CIA.[19]

Establecer la conexión rusa

En este momento, después de examinar algunas complejidades técnicas dentro de las operaciones cibernéticas y métodos de guerra política rusas, nos concentramos ahora en una breve exploración de las motivaciones de Moscú. ¿Cuál es su razón? Hay un par de teorías. Una teoría es que la intrusión en el partido demócrata fue una retribución por las acciones económicas vergonzantes impuestas a Moscú, sus industrias de defensa e instituciones financieras después de los abusos de derechos humanos que se cometieron durante su campaña combinada con Irán contra militantes del Estado Islámico en Siria. También se impusieron sanciones económicas a Rusia después de la invasión de Ucrania y la anexión de Crimea. Estas cosas, en su opinión, formaban parte de una campaña deliberada llevada a cabo por EE.UU. para deshonrar a los militares rusos que, por lo tanto, pondrían a la opinión pública en su contra.[20] Las sanciones también empujan a Rusia hacia un estado de paria degradando su prestigio en la política mundial y, lo que es más importante, el mercado de armas internacional. Devalúan sus empresas de fabricación de armas, y potencialmente reducen los beneficios de los oligarcas que las dirigen.

Otra teoría enormemente interesante es que el presidente Putin está al mando de un gobierno con servicios e inteligencia compuestos por fuerzas perturbadoras que prosperan en el caos. En una entrevista de mediados de diciembre, poco después de la publicación de la ICA, Gleb Pavlovsky, un antiguo asesor del presidente ruso declaró: "Por supuesto que al Kremlin le gusta dicha atmósfera de caos. Porque somos comerciantes de caos. Lo vendemos, y cuando más caos haya en el mundo, mejor será para el Kremlin".[21] De hecho, este tema del caos se remonta al caso Agee. El caos, desde el punto de vista de Moscú, hace que los adversarios de Rusia reaccionen histéricamente y hagan alegaciones aparentemente infundadas que, según Putin, "distraen la atención del pueblo estadounidense de la sustancia de lo que los piratas informáticos habían sacado".[22] Esta afirmación, cosa rara, asume que los correos electrónicos robados, con todo los agravantes, podrían de alguna manera arrojar luz sobre las deliberaciones políticas estadounidenses que de otra forma estarían ocultas de la vista del público, y que el antiguo oficial de la KGB es cierta clase de defensor de los medios libres. En cualquier caso, Estados Unidos, según esta forma de pensar, desvía la culpa de sus deficiencias del proceso político, y el origen de sus escándalos, hacia Rusia. De forma alternativa, las alegaciones de manipulación indebida de las elecciones tienen el efecto opuesto de hacer que el presidente Putin parezca un operador completamente astuto y provocador que impulsa a sus enemigos a la distracción mientras tratan de hallar el origen de las intrusiones.

Hora de probar algo diferente

En cualquier caso, ahora que sabemos las motivaciones de Rusia y la finalidad de sus acciones, ¿cómo nos defendemos de ellas? Líderes de la Comunidad de Inteligencia de EE.UU., como el antiguo director de Inteligencia Nacional James Clapper y el comandante del Cibercomando de EE.UU., Almirante Mike Rogers anticiparon lo averiguado por la ICA durante el testimonio del Senado del 5 de enero de 2017. El director Clapper dijo que la comunidad de inteligencia tenía que emprender una iniciativa de contrapropaganda para impedir cualquier intromisión futura en el proceso electoral de Estados Unidos. Una recomendación hecha fue resucitar la Agencia de Información de EE.UU. (USIA), una organización de la época de la Guerra Fría que durante un tiempo lideró nuestra diplomacia pública en el extranjero, y comunicó de forma creíble los valores del país, las posiciones oficiales y las políticas para contrarrestar la desinformación comunista.[23] Durante el cuestionamiento, los senadores preguntaron por qué no se había renovado todavía el estatuto de la USIA. El Almirante Rogers dijo, "No creo que tengamos que llegar aún a un reconocimiento completo de la idea que vamos a tener que tratar de hacer algo tan fundamentalmente diferente".[24] El almirante, quien es también director de la Agencia de Seguridad Nacional, añadió, "creo que seguimos tratando de hacer algunas de las mismas cosas tradicionales que hemos hecho y esperamos volver a hacer las mismas cosas una y otra vez, y no obstante obtener un resultado diferente".[25] A principios de los años 90, la USIA había sobre-

vivido su utilidad y cayó en el desprestigio después de la caída de la Unión Soviética. El material de la organización perdió su carácter persuasivo y ya no pareció relevante, dada la disolución de su razón de ser ideológica.

El enfrentamiento y el combate contra la desinformación rusa en Estados Unidos no requerirá necesariamente alejarse de agencias del pasado, ni requerirá un método completamente innovador. De hecho, nuestra doctrina de operaciones ciberespaciales se basa en un principio de guía probado y cierto: el mejor ataque es una buena defensa. El antiguo Jefe de Estado Mayor de la Fuerza Aérea General Norton A. Schwartz recomendó medidas de sentido común para sistemas de la USAF y el DOD en noviembre de 2011, que podrían aplicarse concebiblemente a las redes de los sectores públicos y privados que también son vulnerables a los ciberataques. Para negar a un adversario la libertad de maniobra en el ciberespacio un defensor debe prohibir el acceso a información sensible y sistemas. La importancia de las palabras del General Schwartz es que uno debe construir una conciencia del código malicioso y los actores malignos que tratan de encontrar formas de implantarlo en nuestras computadoras en el trabajo y en casa. Mantener lejos software no autorizado y dispositivos periféricos, como unidades de memoria USB, de nuestras computadoras es un medio por el que las personas podrían impedir la propagación de virus, gusanos o redes de robots. El uso de software antivirus protector es otra. No hacer caso de correos electrónicos que no están firmados digitalmente, o que no contiene anexos con macros ejecutables e hiperenlaces de fuentes sin verificar, son un medio más común pero efectivo de una ciberdefensa sana.[26] Estas medidas parecen comunes hoy, pero están basadas en las experiencias y lecciones duras aprendidas de los orígenes de las intrusiones desde 2005.

En cuanto a proteger la Fuerza Aérea, el DOD o las redes públicas contra los efectos perniciosos de la desinformación, las soluciones no son técnicas ni están claras. Sin embargo, un estudio práctico realizado en Chequia es instructivo porque proporciona un alternativa viable, mínimamente invasora y por tanto razonable. Allí, una pequeña unidad de 15 analistas de medios sociales monitorea activamente Twitter, Facebook, *Sputnik* y sitios de noticias en checo prorrusos habitados por agitadores que suministran desinformación. El grupo, que está encabezado por Benedikt Vangeli, fue establecido para descubrir las llamadas "noticias falsas" que desconcertaba a los checos desdeñando duramente a políticos a favor de la OTAN o la Unión Europea antes de sus elecciones parlamentarias en octubre. En Twitter, la unidad simplemente señalaba fuentes de noticias cuestionables y alertó al público de su falta de autenticidad. "Simplemente enviamos un "tuit" al público diciendo que son informes falsos", dice Vangeli. "Así es cómo contraatacamos. No los quitamos. No censuramos". Se han establecido grupos similares de esta clase en Alemania y Finlandia, y podrían establecerse razonablemente también en Estados Unidos.[27]

En el fondo, el método de Vangeli de una campaña de conciencia pública prudente, que, al igual que las recomendaciones del general Schwartz, se basa en el sentido común y el deber de simplemente advertir al público. Ahora, un cínico podría decir que los militares (la Fuerza Aérea en este caso) no deben decir al público para el que trabajan qué leer o qué pensar. Al hacer eso en Estados Unidos, donde se garantiza la libertad de expresión en su Constitución, significaría que para su ciudadanía se harían realidad todas las pesadillas orwellianas sobre la intervención del gobierno en asuntos de libertad de expresión y pensamiento. Prevenir mensajes dañinos en línea podría también influir en las expectativas de privacidad de los ciudadanos y su libertad de elección al navegar por Internet, o constituirían potencialmente una búsqueda ilegal si las autoridades legales apropiadas no están listas primero. No obstante, las instrucciones de la Fuerza Aérea indican que, sujetos al reglamento del DOD, los aerotécnicos pueden cooperar y ayudar a hacer cumplir la ley durante investigaciones que protegen de "actividades clandestinas" contra Estados Unidos (como el plan ruso aquí contado), y protegen a "empleados, información, propiedad o instalaciones" del departamento.[28] Asumiendo que ya están monitoreando la presencia de desinformación en la web, es completamente posible que las agencias federales de policía que dispongan de las autoridades estatutarias apropiadas tengan que identificar primero las anomalías y después notificar a sus homólogos militares para reunir sus conocimientos expertos en separar la fuente exacta de la información ofensiva hasta la dirección del IP. No obstante,

el agrupamiento de recursos será crítico, y los intereses son altos. Las consecuencias negativas de no advertir al público sobre desinformación serán graves; la fe de la nación en sus instituciones gobernantes podría dañarse de forma irreparable, y lo que es aún peor, su conciencia colectiva podría envenenarse perpetuamente.

Desde el 11 de septiembre, nuestro gobierno y nuestras FF.AA. han aprendido los valores de la colaboración y la cooperación, que nuestros recursos humanos colectivos y conocimientos triunfarán sobre la estrechez mental que sofocaron el reparto de información y la innovación antes de ese terrible día. En pocas palabras, las organizaciones policiales, como el FBI, que tiene autoridad exclusiva para llevar a cabo operaciones de contrainteligencia en EE.UU., y la Oficia de Investigaciones Especiales de la Fuerza Aérea (AFOSI), deben asociarse y liderar una fuerza de tarea de contradesinformación conjunta. Esta fuerza de tarea podría ser pequeña como la de los checos o emular las mayores fuerzas de tarea conjuntas del terrorismo (JTTF) del FBI. Al ser más de 100 en todo el país, las JTTF son el mecanismo óptimo de la nación para la colaboración con el contraterrorismo con una variedad de agencias policiales locales, estatales y federales.[29]

La AFOSI podría representar el patrimonio de contrainteligencia del DOD, mientras que el Equipo de Preparación de Emergencia Informática del DHS puede emplear sus conocimientos para la identificación de las fuentes de desinformación cibernética, las sutilidades de su codificación y las redes de individuos que lo propagan.[30] Sin duda, el contraataque contra la desinformación requerirá una asociación con el sector privado del país. El FBI es el líder de InfraGard: un consorcio de más de 30.000 expertos en temas de una variedad de campos, como ingeniería, tecnología y seguridad informáticas. Por último, con un mandato apropiado del director de inteligencia de la Fuerza Aérea, nuestros aerotécnicos en los campos de carreras cibernéticas e inteligencia pueden salir del banquillo y convertirse en participantes activos en una nueva empresa que podría desenmascarar muy bien futuros propagandistas rusos, exponer la verdad que hay detrás y proteger nuestra nación contra el efecto corrosivo de la guerra política. ❑

Notas

1. Consejo de Inteligencia Nacional, *Assessing Russian Activities and Intentions in Recent U.S. Elections (Evaluación de actividades e intenciones rusas en las recientes elecciones de EE.UU.)* (Washington DC: Evaluación de la Comunidad de Inteligencia, 6 de enero de 2017), 2, https://www.dni.gov/files/documents/ICA_2017_01.pdf.

2. Ibid., Consejo de Inteligencia Nacional, 4.

3. Winn Schwartau, *Information Warfare–Cyberterrorism: Protecting Your Personal Security in the Electronic Age (Guerra informática ciberterrorismo: protección de su seguridad personal en la Edad Electrónica)* (New York: Thunder's Mouth Press, 1996, 2a edición), 35, 638.

4. Centro Curtis E. LeMay para el Desarrollo de Doctrina y Educación, "Anexo 3-12 *Operaciones ciberespaciales*", 30 de noviembre de 2011, 5, https://doctrine.af.mil/DTM/dtmcyberspaceops.htm. La Fuerza Aérea en este pasaje de su doctrina reconoce implícitamente que tiene un interés establecido en proteger los sistemas con redes públicamente porque posibilitan cosas como "despliegue de la fuerza, capacitación, transporte y operaciones normales".

5. Anthony Faiola, "Czech Republic Enlists Unit to Combat Disinformation" (Chequia alista una unidad para combatir la desinformación), *The Washington Post* (23 de enero de 2017), A1, A10.

6. Thomas Rid, *Cyber War Will Not Take Place (No tendrá lugar una guerra cibernetica)* (New York: Oxford University Press, 2013), 46. 7.Para obtener videos de la prueba vea: https://www.youtube.com/watch?v=fJyWngDco3g.

8 . Ibid., 6.

9. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid" (Dentro del astuto ataque sin precedentes de la red eléctrica de Ucrania), *Wired.com*, 3 de marzo de 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

10. Schwartau escribió que el virus macro de Word para Windows era "el virus más predominante" en junio de 1996. En ese momento, dijo que se estaba "propagando todo menos 10 veces más rápido que cualquier otro virus de la historia", y ibid., Schwartau, 21.

11. Centro Curtis E. LeMay para el Desarrollo de Doctrina y Educación, "Anexo 3-12 Operaciones ciberespaciales", 30 de noviembre de 2011, 5, https://doctrine.af.mil/DTM/dtmcyberspaceops.htm.

12. En su libro *Information Warfare (Guerra de información),* Schwartau hace referencia a su testimonio de 1991 ante el Congreso. Advirtió a la legislatura de un futuro "Pearl Harbor electrónico" porque el gobierno obviamente estaba mal preparado para defender las computadoras cada vez más interconectadas del país contra un ataque catastrófico (vea Schwartau, 43). Vea, también, Ralph Peters, "Washington Ignores Cyberattack Threats, Putting Us All at Peril" (Washington hace caso omiso de las

amenazas de ciberataques poniéndonos a todos en peligro), *Wired.com*, 23 de agosto de 2007, https://www.wired.com/2007/08/ff-estonia-america/amp/.

13. Peter B. Zwack, "Russia" (Rusia), en *Charting a Course: Strategic Choices for a New Administration (Trazado de un rumbo: opciones estratégicas para una nueva administración),* ed., R.D. Hooker Jr., 238, Washington DC: Universidad de la Defensa Nacional, diciembre de 2016, http://ndupress.ndu.edu/Portals/68/Documents/Books/charting-a-course/charting-a-course.pdf?ver=2016-12-08-154300-120. Vea, también: "A Russian Word Americans Need to Know: Kompramat" (Una palabra rusa que los estadounidenses necesitan saber: kompramat), *NPR*, 11 de enero de 2017, http://www.npr.org/sections/parallels/2017/01/11/509305088/a-russian-word-americans-need-to-know-kompromat/.

14. Jennet Conant, *The Irregulars (Los irregulares)* (New York: Simon and Schuster, 2008), 94.

15. Ibid., Conant, 95.

16. Christopher Andrew y Vasili Mitrokhin, *The Mitrokhin Archive and the Secret History of the KGB (El archivo Mitrokhin y la historia secreta de la KGB)* (New York: Basic Books, 2009), 226–27.

17. Oleg Kalugin se retiró de la KGB como general de división después de 32 años de servicio. Hoy, sirve en el Consejo Asesor de Directores del Mueso Internacional de Espías en Washington DC. Vea: https://www.spymuseum.org/about/leadership/board-of-directors/.

18. Ibid., Andrew y Mitrokhin, 231.

19. Ibid., Andrew y Mitrokhin, 232.

20. David Filipov, "Putin Uses the Soviet Defeat of Hitler to Show Why Russia Needs Him Today" (Putin usa la derrota soviética de Hitler para mostrar por qué Rusia le necesita hoy), *Washington Post*, 8 de mayo de 2017, https://www.washingtonpost.com/world/europe/putin-is-using-the-soviet-defeat-of-hitler-to-show-why-russia-needs-him-today/2017/05/07/1c390338-2e9e-11e7-a335-fa0ae1940305_story.html?utm_term=.10033df265ff.

21. David Filipov, "'Chaos' Theory Is Working for Putin" (La teoría del caos está dando resultado para Putin), *Washington Post*, 15 de diciembre de 2017, A-1, A-12.

22. Ibid., Filipov.

23. Declaración de James Clapper, director nacional de inteligencia, Comité del Senado de EE.UU. sobre servicios Armados en el Senado, "Hearing to Receive Testimony on Foreign Cyber Threats to the United States" (Audiencia para recibir testimonio sobre amenazas cibernéticas extranjeras a Estados Unidos), 5 de enero de 2017, 112. 24. Declaración del Almirante Mike Rogers, director de la Agencia de Seguridad Nacional, Comité del Senado de EE.UU. en los Servicios Armados en el Senado, "Audiencia para recibir testimonio sobre amenazas cibernéticas extranjeras a Estados Unidos", 5 de enero de 2017, 112.

25. Ibid., testimonio del Almirante Rogers.

26. Centro Curtis E. LeMay para el Desarrollo de Doctrina y Educación, "Anexo 3-12 Operaciones ciberespaciales, Apéndice A: Comentarios de CSAF sobre el ciberespacio", 41, (30 de noviembre de 2011) from: https://doctrine.af.mil/DTM/dtm-cyberspaceops.htm.

27. Ibid., Faiola, A10.

28. Instrucción de la Fuerza Aérea de EE.UU. 14-104, "Oversight of Intelligence Activities" (Supervisión de actividades de inteligencia), *www.epublishing.af.mil.*, 5 de noviembre de 2014. Vea también: Reglamento del Departamento de Defensa (DOD) 5240 1.R, *Procedimientos que regulan las actividades de los componentes de inteligencia del DOD que afectan a personas de Estados Unidos*, e Instrucción del DOD 3025.21, *Apoyo de defensa de agencias de orden público de leyes civiles.*

29. El antiguo director del FBI Robert Muller supervisó la expansión posterior al 11 de septiembre de las fuerzas de tarea conjuntas del terrorismo (JTTF) en cada oficina de campo de la nación. Con fecha de 2014, se crearon 71 JTTF después de los ataques terroristas. Vea también, Bruce Hoffman, Edwin Meese, Tim Roemer y otros, "The FBI: Protecting the Homeland in the 21st Century" (El FBI: protección de la patria en el siglo XXI), Oficina Nacional de Prensa del FBI (25 de marzo de 2015), https://www.fbi.gov/news/pressrel/press-releases/the-fbi-releases-final-report-of-the-9-11-review-commission.

30. El FBI y el DHS, en cooperación con el Equipo de Preparación de Emergencia de Computadoras del Departamento de Seguridad Nacional, publicó un informe no secreto en diciembre de 2016 que dividía cómo los servicios de inteligencia de Rusia usaron una campaña de pesca con arpón enfocada para acceder a correos electrónicos de miembros superiores del personal del partido demócrata en primavera de 2015 y verano de 2016. El informe, que apodaba 28 y 29 las persistentes amenazas avanzadas rusas, dijo que los actores "enmascarados como terceros, ocultándose detrás de personas falsas en línea diseñadas para hacer que la víctima atribuyera de forma errónea el origen del ataque". A diferencia de ICA, el informe del FBI–DHS no va tan lejos como para culpar directamente al presidente de Rusia Vladimir Putin por la intrusión. Vea también, el Informe de análisis conjunto del FBI–DHS, *GRIZZLY STEPPE—Ciberactividad maliciosa rusa* (Washington DC: 29 de diciembre de 2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

Mayor William Giannetti (MS, Universidad de St. Joseph) es un reservista de la Fuerza Aérea asignado al estado mayor conjunto en el Pentágono, Washington DC. Su carrera se extiende 20 años como funcionario civil, oficial de policía de Filadelfia y analista del Departamento de Defensa. Fue miembro del personal de la Comisión de Revisión del 11 de septiembre, que examinó cómo la Oficina Federal de Investigación implementó las recomendaciones de la comisión original. El Mayor Giannetti también sirvió en dos períodos en Afganistán.