Editorial

LAS AMENAZAS GLOBALES QUE DOMINAN LAS AGENDAS DE SEGURIDAD

El continuo incremento de la capacidad nuclear y misilística de Corea del Norte y el vertiginoso desarrollo de las capacidades en materia de ciberespionaje, se han tomado las agendas de seguridad internacional durante las últimas semanas. En ambos casos se han producido retos y desafíos entre los actores involucrados. Es por ello, que nos ha parecido interesante efectuar una revisión de las eventuales consecuencias que de la evolución de estos acontecimientos se pueden derivar.

Iniciamos nuestro análisis con el artículo del Senador republicano Dan Sullivan, quien destaca la creciente inestabilidad que genera el desarrollo nuclear de Corea del Norte y las pruebas de misiles balísticos de largo alcance que han llegado a un punto crítico de elevar las alertas y a la necesidad de aplicar medidas de contención que superen las sanciones económicas y políticas que hasta ahora estaban siendo utilizadas por las potencias mundiales como medidas disuasivas. Como lo sugiere John Glaser, estaría cundiendo la idea de que cada día se está más cerca de una acción militar de carácter preventivo, como complemento del recientemente instalado sistema de defensa antimisiles THAAD de EE.UU. de A. en Corea del Sur. La presencia del Vicepresidente Pence en la zona desmilitarizada entre ambas Coreas, así como sus declaraciones en el sentido que no descansarán hasta que Corea del Norte deje sus armas nucleares, nos dan cuenta de un nuevo paso en esta escalada de la crisis.

Lo previsible es que el desenlace de estas acciones tenga consecuencias importantes para la región Asia Pacífico, donde convergen no sólo los intereses de China y Rusia. Actualmente la zona es el principal destino de las exportaciones de otros países, como es el caso de Chile, por lo que las condiciones de seguridad podrían requerir de las naciones algo más que el mero análisis situacional, siendo imperioso abordar el futuro con una nueva óptica. Lo que ahí suceda no nos puede ser indiferente y lejano. De una u otra forma nos va a afectar.

Por otra parte, mientras estos eventos ocurren, las relaciones interestatales están siendo influidas por un nuevo factor de desconfianza, derivado del desarrollo tecnológico aplicado al ciberespionaje. Al respecto, no solo están de por medio las últimas revelaciones de Wikileaks, que ponen en cuestión los beneficios del concepto "internet de las cosas". La posibilidad de que se esté influyendo en los procesos electorales a partir del espionaje político internacional, supone mayores complejidades a la hora de conformar alianzas o dar estabilidad a las relaciones interestatales.

De esta manera, se instalan temas tan relevantes como la fiabilidad de los sistemas de inteligencia, el impacto de sus elementos vanguardistas, así como también, el tipo de profesionalismo implicado en dicha función. De eso tratan de ilustrar John Walcott y Mark Hosenball, periodistas acreditados en la Casa Blanca, al evaluar las capacidades de las agencias de inteligencia y cómo las nuevas tecnologías han sido utilizadas o bien vulneradas por estas agencias en el ejercicio de sus actividades.

Finalmente, Levi Maxey, analista internacional y productor de tecnologías, nos muestra como las organizaciones, tanto públicas como privadas, pueden verse expuestas a los efectos de los ataques cibernéticos, tomando como ejemplo las estructuras críticas que la India ha identificado, cuestión que deberíamos prestarle una especial atención, considerando que en Chile estamos dando los pasos iniciales en esta materia con la reciente publicación de la Política Nacional de Ciberseguridad.

Como se ve, el escenario internacional es absolutamente incierto. Los retos y desafíos de los actores involucrados tienden a hacer escalar los acontecimientos. Los organismos internacionales se muestran incapaces de actuar y todo esto se ve agravado por el hecho que los principales líderes involucrados: Trump, Putin y Kim Jon-un, si algo tienen en común, es su impredictibilidad.

CIEE - ANEPE

Manteniendo la paz con misiles

Senador Dan Sullivan
Defense One, 7 de marzo 2017

[…] El mes pasado, cuando el primer ministro japonés Abe y el presidente Trump se reunieron para forjar una alianza más profunda entre ambos países, Corea del Norte lanzó un misil balístico al Mar de Japón, que era similar al lanzado anteriormente a una barcaza. El mensaje que envía al mundo es claro: Kim Jong-un continúa su búsqueda de sofisticados sistemas de misiles de largo alcance que pueden ser capaces de llegar a los Estados Unidos y a nuestros aliados más cercanos.

El objetivo que ha declarado de Kim Jong-un es desarrollar un misil balístico intercontinental con capacidad nuclear que pueda golpear a Estados Unidos. Para ser claro, el hombre que mata a sus propios ciudadanos, los condena a inhumanos "campos de trabajo", y que el mes pasado supuestamente tuvo a su medio hermano asesinado en Malasia, es la misma persona que quiere mantener rehenes a ciudades como Nueva York, Los Ángeles y Chicago. Los altos funcionarios militares y de inteligencia han dicho públicamente que ya no se trata de si Kim Jong-un obtiene esta capacidad, sino más bien cuándo lo podría hacer. […] Al principio de su presidencia, el presidente Obama cumplió su promesa de campaña de "reducir las inversiones en sistemas de defensa antimisiles" al recortar miles de millones de dólares en tres años. Luego vino una detonación nuclear adicional y otras "provocaciones irresponsables e imprudentes" de una inestable Corea del Norte. En marzo de 2013, la administración dio un giro en "U", moviéndose para aumentar nuestra capacidad de defensa antimisiles desplegada en un 50 por ciento citando "provocaciones irresponsables e imprudentes" de Corea del Norte.

Cuatro años después, nos encontramos en otro punto de inflexión. Las sanciones y las negociaciones no han frenado las ambiciones nucleares y de misiles balísticos de Pyongyang. Desde 2013, Kim Jong-un ha detonado tres armas nucleares y probado más de 60 misiles - más del doble de armas nucleares y pruebas de misiles que su padre y su abuelo combinados. Y continúa abusando, explotando y empobreciendo a su propio pueblo, hipotecando su bienestar por su impía cruzada por una ojiva nuclear miniaturizada […]La política del gobierno de Obama de paciencia estratégica con Corea del Norte ha fracasado.

[…] Para el final de este año, tendremos 44 interceptores terrestres en Alaska y California, y para 2019 tendremos un nuevo radar y otros medios para permitir a nuestros combatientes controlar y discriminar mejor las amenazas. Además, el Congreso continúa sus esfuerzos bipartidistas para modernizar la defensa antimisiles de la patria y para mandar pruebas anuales del sistema.

Sin embargo, el desarrollo de misiles de Corea del Norte amenaza con superar las defensas estadounidenses a largo plazo. Para enfrentar este desafío, la administración Trump, como parte de la implementación del Memorando Presidencial del 27 de enero sobre la reconstrucción de las Fuerzas Armadas de Estados Unidos, debería considerar al menos cinco caminos para fortalecer nuestra defensa antimisiles.

En primer lugar, la administración debe continuar los esfuerzos para completar un sistema de defensa más eficaz para poder hacer frente a la amenaza Norcorena. Diseñando una barrera para derribar misiles de largo alcance, este nuevo vehículo también será más barato y más fácil de producir - dos cualidades que ayudarán a asegurar que nuestras defensas continúen superando la creciente amenaza.

En segundo lugar, la fuerza del interceptor debe hacerse más eficaz y flexible, como con un refuerzo de etapa seleccionable para dar a los combatientes más espacio de batalla, un nuevo radar y nuevos sensores en el espacio. También podríamos acelerar el desarrollo de un vehículo de destrucción de objetos múltiples, lo que permitiría que un solo interceptor pudiese hacer frente a más de un objetivo.

En tercer lugar, debemos considerar el aumento de nuestra capacidad interceptora, tal vez la expansión hasta los 100 interceptores originalmente planeado para Fort Greely en Alaska. Un informe de abril de 2015 de la Universidad Johns Hopkins encontró que Corea del Norte podría tener hasta 100 ojivas nucleares en 2020. Para el final de este año, tendremos sólo 44 interceptores. Debemos - como mínimo - continuar produciendo interceptores adicionales, crecer en Fort Greely, y mirar la construcción de un nuevo sitio de defensa antimisiles en nuestra costa atlántica.

En cuarto lugar, los Estados Unidos deberían realizar más regularmente pruebas en vuelo de nuestras defensas de misiles. Estas pruebas dan confianza a nuestros combatientes y demuestran a nuestros adversarios que si lanzan contra los Estados Unidos, sus ataques nunca llegarán a nuestras costas.

Por último, los Estados Unidos deben buscar otros medios para derrotar misiles a principios de su vuelo o incluso antes de que sean lanzados. Las tecnologías avanzadas dignas de esfuerzo adicional incluyen los láseres montados en UAVs pequeños para derrotar misiles en su fase de lanzamiento o inicial de vuelo […]

SULLIVAN, Dan. Pick up the peace on Missile Defense. Defense One, Ideas, 7 de marzo 2017. [en línea] [fecha de consulta 6 de marzo 2017] Disponible en:

http://www.defenseone.com/ideas/2017/03/pick-pace-missile-defense/135962/?oref=d-channelriver

Calma por las armas nucleares de Corea del Norte

John Glaser
Defense One, 7 de marzo 2017

[…] El lunes, Corea del Norte volvió a lanzar misiles balísticos, aumentando los temores sobre el progreso del régimen en armas nucleares y lo que podría significar para la seguridad regional. Pero los estadounidenses y sus aliados asiáticos tienen buenas razones para calmar su pánico reflexivo sobre este tema.

El programa de armas nucleares de Pyongyang es ampliamente considerado como el problema de seguridad internacional más urgente hoy. El régimen ha llevado a cabo cinco pruebas nucleares desde 2006 y ha prometido desarrollar un misil balístico intercontinental (ICBM) que puede entregar una ojiva nuclear a tierra de los Estados Unidos. Un alto funcionario de la administración de Trump dijo a periodistas recientemente que el presidente cree que la "mayor amenaza" para los Estados Unidos es Corea del Norte y su programa nuclear. La semana pasada en CNN, el senador John McCain lo describió como un "peligro inmediato", y planteó la posibilidad de una acción militar preventiva porque "no piensan como nosotros" […]

Para algunos observadores, el hecho de que Corea del Norte intente convertirse en una potencia nuclear de pleno derecho es prueba suficiente de sus intenciones agresivas. Si no bloquean el camino de Pyongyang hacia la bomba, argumentan, arriesgan una guerra nuclear con un Estado totalitario inestable, irracional y paranoico.

[…] Pocos expertos llegan a sugerir que Pyongyang iniciará una guerra nuclear con Corea del Sur o los Estados Unidos. El régimen norcoreano tendría que estar ansioso por cometer suicidio, ya que tal acto de agresión desencadenaría una respuesta de represalia que prometía su destrucción total. […]

Hay otro argumento, que dice que si bien es poco probable que Corea del Norte inicie una guerra nuclear, su creciente arsenal le permitirá en última instancia coaccionar e intimidar a otros países. Este argumento también sostiene que las armas nucleares pueden permitir que los Estados actúen de manera más agresiva en el nivel convencional, ya que saben que otros serán disuadidos de toda represalia

[…]En su nuevo libro, los cientistas políticos Todd S. Sechser y Matthew Fuhrmann argumentan que la coerción nuclear no funciona realmente. Ellos analizan múltiples conjuntos de datos de cientos de ejemplos históricos y encuentran que los Estados nucleares no tienen más influencia en el arreglo de disputas territoriales […] En resumen, las armas nucleares no dan a los Estados más capacidad de coacción.

La historia reciente con Corea del Norte parece confirmar esto. En 2013, Pyongyang hizo un intento serio de coerción nuclear. Después de su tercera prueba nuclear, en febrero de ese año, el régimen de Kim Jong-Un amenazó con bombardear Corea del Sur y los Estados Unidos con "armas nucleares más ligeras y más pequeñas". En respuesta, el Consejo de Seguridad de la ONU impuso sanciones económicas adicionales a Corea del Norte. Provocó una amenaza aún más audaz: el Norte anuló unilateralmente el armisticio de 1953 y amenazó con "ejercer el derecho a un ataque nuclear preventivo para destruir los baluartes de los agresores".

Es de suponer que estas amenazas tenían como objetivo hacer más creíble la amenaza de las armas nucleares de Pyongyang y forzar a la comunidad internacional a levantar las devastadoras sanciones económicas. No funcionó. Nadie encontró que las amenazas fueran creíbles, se impusieron sanciones más duras y los ejercicios conjuntos de los Estados Unidos y la República de Corea del Sur proseguían rápidamente.

En realidad, las armas nucleares son buenas para una sola cosa: la disuasión. La determinación de Corea del Norte de obtener la bomba probablemente se debe al temor provocado, entre otras cosas, por las constantes promesas estadounidenses de derrocar un día al régimen. Los formuladores de políticas y los informes de los “think tanks” frecuentemente plantean esto como una opción para resolver el estancamiento de 70 años en la Península Coreana. Un programa de armas nucleares norcoreano plenamente capaz protegería a Pyongyang de la invasión y el derrocamiento, pero no les daría mayor influencia contra los enemigos.

[…] Más armas nucleares en posesión de regímenes autoritarios aislados y que aceptan riesgos no es algo bueno. Sin duda eleva las posibilidades de accidente o error de cálculo. Pero no necesariamente significa una Corea del Norte más poderosa y más agresiva.

GLASER, John. Calm Down About North Korea’s Nukes. Defense One, Ideas, 7 de marzo 2017. [en línea] [fecha de consulta 8 de marzo 2017] Disponible en:

http://www.defenseone.com/ideas/2017/03/calm-down-about-north-koreas-nukes/135934/?oref=d-channelriver

Defensa Antimisiles: apuntando a una solución tecnológica

Will Edwards
The Cipher Brief, 7 de marzo 2017

A pesar de las resoluciones de la ONU y la oposición internacional, Corea del Norte lanzó cuatro misiles balísticos de rango intermedio el lunes que alcanzaron las 200 millas de Japón. La prueba demuestra no sólo el desprecio de Pyongyang por más sanciones, sino también su progreso en la tecnología de misiles. Además de Corea del Norte, Rusia, China e Irán también han dedicado recursos a la adquisición de nuevos misiles con mayor alcance, velocidad y precisión. Esta amenaza evolutiva exige una solución técnica igualmente, si no más avanzada. […]

Un desafío clave para el desarrollo de sistemas de defensa antimisiles radica en la velocidad e imprevisibilidad de un misil ofensivo. El defensor debe reaccionar a la amenaza sin saber con precisión de dónde vendrá el lanzamiento o hacia dónde irá. Por lo tanto, cualquier defensa inevitablemente cambia el tiempo de respuesta de la información - cuanto más tiempo espera el defensor, más información hay sobre dónde va el misil, pero hay menos tiempo para reaccionar. Las soluciones técnicas, por lo tanto, están orientadas a interrumpir un misil en tres etapas diferentes durante su trayectoria de vuelo.

La primera fase, conocida como la fase de impulso del cohete, es la fase más difícil de defenderse. Mientras que el misil es fácil de detectar una vez que los motores están encendidos, su trayectoria-y objetivo final será más compleja de calcular. Actualmente no hay defensas técnicas viables para esta fase, sin embargo los láseres montados en vehículos aéreos no tripulados (UAVs) o aviones podrían ofrecer una solución potencial.

La segunda fase, es la del curso medio, ocurre cuando el misil alcanza su altitud mayor y comienza a disminuir. Defensivamente, esto ofrece el tiempo de respuesta más largo, pero debido a la gran altitud requiere misiles grandes y costosos como la Defensa del Medio de Tierra (GMD) como interceptores.

La fase final, es cuando el misil ha vuelto a entrar en la atmósfera. Mientras que los misiles defensivos y los sistemas de radar pueden ser más baratos y menos potentes en esta etapa, tienen menos tiempo de reacción. Estos sistemas incluyen la Terminal de Área de Alta Altitud de Defensa (THAAD), que se desplegarán en Corea del Sur, y Aegis, un sistema basado en buques desplegados en la Armada de los Estados Unidos.

Estados Unidos emplea varios sistemas de defensa antimisiles diferentes cuyas diversas fuerzas están destinadas a complementarse, pero no son en modo alguno una solución perfecta. […] La amenaza norcoreana ofrece otro ejemplo. Durante el fin de semana, el New York Times publicó un artículo que describía cómo la administración Obama había pasado tres años intentando sabotear el programa de misiles norcoreanos con técnicas de guerra cibernética, lo que coincidió con una caída en la tasa de éxito de las pruebas de misiles norcoreanos.

[…] A partir de 2013, el programa GMD había costado 40.900 millones de dólares en diez años, según un informe de la Oficina de Responsabilidad Gubernamental. THAAD, una opción de fase terminal relativamente más barata, cuesta 1.600 millones de dólares por unidad.

El alto costo de los interceptores de misiles ha dado forma a la tecnología de defensa de misiles en los últimos años. Según un informe del CSIS, el presupuesto de la línea de defensa de la Agencia de Defensa contra Misiles disminuyó un 23,4 por ciento entre 2007 y 2016, mientras que las amenazas sólo empeoraron. El alto costo ha guiado a la MDA y a los contratistas de defensa para centrarse en la evolución, no en la revolución, cuando se trata de la tecnología de defensa de misiles. Un buen ejemplo es la familia Standard Missile, que ha sido mejorada durante 65 años. A diferencia de la mayoría de las defensas de misiles que están destinados a un solo tipo de objetivo, la última versión, el SM-6, puede ser utilizado contra aviones, misiles y buques de superficie. […]

[…] Si bien tales enfoques se suman a las defensas estadounidenses, simplemente no hay suficientes sistemas desplegados para satisfacer las necesidades de defensa de los Estados Unidos. Los EE. UU. tienen menos sistemas GMD, Aegis y THAAD que los necesarios para cubrir las peticiones de los comandantes combatientes. Las nuevas tecnologías, como los láseres o las defensas de misiles hipersónicos, también podrían ampliar las capacidades, pero requerirán más tiempo y dinero para perfeccionarlas. En última instancia, se necesitan inversiones en más sistemas y tecnologías para cubrir más área geográfica y contrarrestar más amenazas.

No hay una tecnología única para la defensa antimisiles. Mientras que las nuevas soluciones maximizan la utilidad de los sistemas existentes, las amenazas más numerosas y más avanzadas requieren una defensa más robusta que sea multicapa para minimizar los riesgos de los misiles balísticos.

EDWARDS, Will. Missile Defense: Targeting a Technological Solution. The Cipher Brief, Columna de Opinión, 7 de marzo 2017. [en línea] [fecha de consulta 8 de marzo 2017]Disponible en:

https://www.thecipherbrief.com/article/asia/missile-defense-targeting-technological-solution-1091

Pence, en Corea del Sur, llama una provocación la prueba de misil de Corea del Norte

Julie Hirschfeld Davis
New York Time, 17 de abril 2017

El vicepresidente Mike Pence describió el domingo que la fallida prueba de misiles realizada por Corea del Norte es "una provocación" que puso nuevamente en riesgo la región como y a Estados Unidos, ya que la Casa Blanca comentó que el presidente Trump tenía a sus fuerzas militares y diplomáticas junto con otras opciones para responder.

"La provocación de esta mañana desde el Norte es sólo el último recordatorio de los riesgos que cada uno de ustedes enfrenta cada día en la defensa de la libertad del pueblo de Corea del Sur y la defensa de América en esta parte del mundo", dijo Pence en una cena de Pascua en la base militar de Yongsan en Seúl, Corea del Sur, donde comenzó una gira de 10 días por Asia. El Sr. Pence señaló que había hablado con el Sr. Trump, quien le pidió que transmitiera a las tropas estacionadas en Corea del Sur que "estamos orgullosos de usted y estamos agradecidos por su servicio".

Durante una visita a la zona desmilitarizada el lunes, a pasos de la línea de demarcación entre Corea del Norte y Corea del Sur, Pence señaló que Estados Unidos estaba comprometido a lograr la seguridad "por medios pacíficos, a través de negociaciones", pero también buscó intensificar la presión en el Norte para cambiar de rumbo, añadiendo "la era de la paciencia estratégica ha terminado" y que "todas las opciones están sobre la mesa" para tratar con Corea del Norte, y pidió a China "hacer más" para ayudar a enfrentar las amenazas de Pyongyang. […]

[…] K. T. McFarland, el segundo asesor de seguridad nacional de Trump, declinó el domingo para decir si los Estados Unidos habían saboteado el lanzamiento de Corea del Norte.

[…] El teniente general H. R. McMaster, asesor de seguridad nacional del Sr. Trump, dijo que Estados Unidos estaba desarrollando una serie de posibles respuestas a la última medida de Corea del Norte, en consulta con China.

"Esta última prueba de misiles sólo encaja en un patrón de conducta provocativa y desestabilizadora y amenazante por parte del régimen norcoreano, y creo que hay un consenso internacional ahora - incluyendo a los líderes chinos. "El presidente ha dejado claro que no aceptará que Estados Unidos y sus aliados y socios en la región estén bajo amenaza de este régimen hostil con armas nucleares, y que "no puede continuar ", dijo el general McMaster en ABC. […]

[…] El funcionario de la Casa Blanca, quien bajo condición de mantener el anonimato señaló que la situación es delicada con la seguridad, dijo que Trump tenía muchas herramientas militares, diplomáticas y de otro tipo a su disposición si decidiera responder al último comportamiento de Corea del Norte. Pero sugirió que una respuesta a la serie de lanzamientos fallidos podría no ser inminente. Una prueba nuclear, sin embargo, sería un caso diferente, agregó el funcionario. "Si hubiera sido una prueba nuclear, entonces se habrían tomado otras acciones de los Estados Unidos", dijo el funcionario.

La inteligencia de Estados Unidos indica que el misil no era un misil balístico intercontinental, sino probablemente de mediano alcance, que fue lanzado desde la misma base naval como un intento del 5 de abril y que falló después de cuatro a cinco segundos.

El gobierno de Trump había estado anticipando la acción este fin de semana porque el sábado era el aniversario del nacimiento de Kim Il-sung, el abuelo del líder norte-coreano, Kim Jong-un, convirtiéndolo en la fiesta más importante del país.

"Esperábamos algo particularmente en torno al cumpleaños de su abuelo, así que no fue una sorpresa", dijo McFarland. "No tengo ningún comentario en particular sobre lo que sucedió con el misil norcoreano, pero fue un fracaso".

El Sr. Trump, que está pasando el fin de semana de Pascua en Florida, no tuvo respuesta directa al lanzamiento, pero el domingo sugirió que China estaba ayudando a los Estados Unidos a formular una estrategia para contrarrestar la amenaza norcoreana, absteniéndose de llamar a Beijing “un manipulador de monedas”, como parte del proceso de cooperación.

HIRSCHFELD, Juile. Pence, in South Korea, Calls North Korea Missile Test ’a Provocation’. New York Time, 17 de abril 2017. [en línea] [fecha de consulta 18 de abril 2017] Disponible en: https://www.nytimes.com/2017/04/16/us/politics/north-korea-missile-launch-mike-pence.html?ref=politics

La CIA y nuestra vida privada, al descubierto

Editorial

El Mundo, 9 de marzo 2017

Una nueva entrega de **WikiLeaks**, el grupo de ciberactivistas comandado por Julian Assange, desentrañó y **difundió el martes lo que presuntamente son los programas que utiliza la CIA para espiar en internet a cualquier persona que tenga un dispositivo conectado a la Red**, sea un móvil, una tableta, un ordenador e incluso una receptor de televisión. La agencia norteamericana aprovecha las posibilidades que ofrece la tecnología incluida en esos aparatos -que los usuarios aceptamos al firmar los términos de uso- para inmiscuirse en las conversaciones privadas de cualquier ciudadano que considere oportuno. El caso que ha llamado más la atención es el de los televisores inteligentes de Samsung, a los que la CIA puede acceder con sus programas para oír y grabar conversaciones incluso cuando están apagados.

WikiLeaks considera que se trata de una filtración muy superior a la que afectó al Departamento de Estado en 2010 y a las filtraciones de la NSA, en 2013. De confirmarse su autenticidad estaríamos ante un **nuevo escándalo del espionaje gubernamental**. […]

Pero sí hay que hacerse eco, en primer lugar, del tremendo ridículo al que WikiLeaks está sometiendo a la CIA al revelar, no el fruto de sus averiguaciones, sino los programas informáticos -los métodos-, que utiliza para realizar su trabajo. **Una de las agencias mundiales clave en la lucha contra el terrorismo ha sido desnudada por completo**. Costará tiempo, trabajo y dinero reparar el daño causado. Si lo difundido en la filtración es cierto, llega además en un momento delicado en Estados Unidos. El presidente Trump ha criticado duramente a los distintos servicios secretos del país por ineficaces y todavía no se ha apagado la polémica sobre el espionaje ruso durante la campaña electoral estadounidense. La filtración da alas a Trump para ordenar cambios radicales en la dirección de la CIA.

Pero este nuevo episodio vuelve a demostrar que las barreras de la privacidad han saltado por los aires. **Hemos dado permiso para que los dispositivos que utilizamos habitualmente recojan nuestras conversaciones** -el asistente de voz *Siri*, de Apple, registra todo lo que oye y lo envía a los servidores de la empresa, por ejemplo- y eso es aprovechado por las agencias de espionaje para interceptar ilegalmente esa información.

Defenderse ante esta invasión no es fácil. Dos de las empresas afectadas, Samsung y Apple, anunciaron ayer que ya están trabajando para evitar esas vulnerabilidades. Microsoft lleva tiempo proponiendo una especie Convención Digital de Ginebra, que establezca los criterios para "proteger a los ciudadanos de ciberataques de los gobiernos en tiempos de paz". Unos criterios en los que quieren participar las compañías tecnológicas, que se consideran fundamentales para "hacer de internet un sitio más seguro". Podrá haber otras soluciones, pero **la existencia del riesgo está perfectamente demostrada** y para reducirlo será imprescindible el concurso coordinado de los gobiernos y las empresas en todo el mundo.

EL Mundo. La CIA y nuestra vida privada, al descubierto. El Mundo, Editorial, 9 de marzo 2017. [en línea][fecha de consulta 10 de marzo 2017] Disponible en:

http://www.elmundo.es/opinion/2017/03/09/58c05303ca4741f9108b45d9.html

Fuente de la última revisión de documentos de WikiLeaks parece ser un Contratista de la CIA

John Walcot
Mark Hosenball
Time Magazine, 10 de marzo 2017

[…] Dos funcionarios que hablaron bajo condición de anonimato dijeron que las agencias de inteligencia han sido conscientes desde final del año pasado sobre la violación de seguridad, que llevó a WikiLeaks liberar miles de páginas de información en su sitio web el martes. Según los documentos, los hackers de la CIA podrían entrar en los iPhones, los dispositivos que ejecutaban el software Android y otros dispositivos para capturar mensajes de texto y de voz antes de que fueran cifrados con un software más sofisticado. La Casa Blanca dijo el miércoles que el presidente Donald Trump estaba "extremadamente preocupado" por la violación de seguridad de la CIA que llevó a la liberación de dichos documentos por parte de WikiLeaks.

Los dos funcionarios dijeron a Reuters que creían que los documentos publicados sobre las técnicas de hacking de la CIA utilizadas entre 2013 y 2016 eran auténticos. Uno de los funcionarios con conocimiento de la investigación dijo que las empresas, que son contratistas de la CIA, han estado comprobando cuáles de sus empleados tenían acceso al material que WikiLeaks publicó, y luego revisar sus registros informáticos, correos electrónicos y otras comunicaciones para cualquier evidencia de quién podría ser responsable. […]

La CIA, que es el servicio de inteligencia civil de los Estados Unidos, se negó a comentar sobre la autenticidad de los documentos de inteligencia. La agencia declaró que su misión era recopilar información de inteligencia extranjera en el exterior "para proteger a Estados Unidos contra la amenaza terrorista, Estados hostiles y otros adversarios." […] La CIA tiene prohibición (mediante vía legal) de vigilar dentro de los Estados Unidos y "no lo hace", agregó el comunicado.

Los Contratistas deben ser "Leales con EE.UU."

Una fuente del gobierno de Estados Unidos familiarizada con el asunto dijo que sería normal que la Oficina Federal de Investigación y la CIA abrieran las investigaciones sobre tales filtraciones. Funcionarios estadounidenses habían confirmado previamente que los fiscales en Alexandria, Virginia durante años han estado llevando a cabo una investigación federal del gran jurado de WikiLeaks y su personal.

[…] Los contratistas han revelado que la fuente de información en los últimos años, especialmente en el caso de Edward Snowden y Harold Thomas Martin, habían sido empleados de la firma consultora Booz Allen Hamilton que prestaba servicios a la Agencia de Seguridad Nacional.

[…] Tanto el Senado de Estados Unidos como los comités de inteligencia de la Cámara de Representantes han abierto o esperan que se abran investigaciones sobre la violación de la CIA, dijeron funcionarios del Congreso. Algunos expertos en ciberseguridad y empresas de tecnología han criticado al gobierno por optar por explotar en lugar de revelar vulnerabilidades de software, aunque un proceso de revisión interinstitucional establecido bajo el ex presidente Barack Obama tenía la intención de entrar por el camino de la divulgación.

Esas preocupaciones crecerían si las autoridades estadounidenses no notificaran a las compañías que los documentos de la CIA que describían diversas técnicas de hacking habían sido comprometidos.

Apple, Google de Alphabet, Cisco Systems y Oracle no respondieron inmediatamente cuando se les preguntó si se les había notificado de una violación de la CIA antes de que WikiLeaks hiciera públicos sus archivos.

En Apple, ninguna de las vulnerabilidades descritas en los documentos provocó pánico, aunque el análisis continuaba, según una persona que habló con ingenieros allí. El director de seguridad de la información y privacidad de Google, Heather Adkins, dijo en un comunicado: "Como hemos revisado los documentos, estamos seguros de que las actualizaciones de seguridad y las protecciones de Chrome y Android (sistemas operativos) ya protegen a los usuarios de muchos de estas supuestas vulnerabilidades, nuestro análisis está en curso y pondremos en práctica cualquier otra protección necesaria".

Un mayor número de Contratistas

Una razón por la que la investigación se centra en una posible fuga de los contratistas en lugar de por ejemplo un hackeo de inteligencia rusa, dijo otro funcionario, es que hasta el momento no hay pruebas de que las agencias de inteligencia rusas trataron de explotar el material antes de ser publicado.

Un funcionario europeo, que habló bajo condición de anonimato, dijo que el material de WikiLeaks podría de hecho conducir a una cooperación más estrecha entre las agencias de inteligencia europeas y contrapartes estadounidenses, que comparten preocupaciones sobre las operaciones de inteligencia rusas.

Las agencias de inteligencia de Estados Unidos han acusado a Rusia de intentar inclinar las elecciones presidenciales del año pasado a favor de Trump, incluyendo hackear los correos electrónicos del Partido Demócrata. Moscú ha negado la acusación.

Uno de los principales problemas de seguridad fue que el número de contratistas con acceso a la información de clasificación de secreto más alto "explotó" debido a las restricciones presupuestarias federales, dijo el primer funcionario estadounidense.

Las agencias de inteligencia estadounidenses no han podido contratar personal adicional necesario para mantener el ritmo de los avances tecnológicos como el "Internet de las cosas" que conecta los automóviles, los sistemas de seguridad, la calefacción del hogar y otros dispositivos a las redes informáticas o bien cancelar salarios competitivos con el sector privado, dijo el funcionario.

[…] En Alemania, el miércoles, la oficina del fiscal federal dijo que revisaría los documentos de WikiLeaks porque algunos sugirieron que la CIA dirigía un centro de hacking desde el consulado estadounidense en Frankfurt. "Iniciaremos una investigación si vemos pruebas de actos criminales. […]

WALCOTT, John and HOSENBALL, Mark. Source of the Latest WikiLeaks Document Dump Appears to Be CIA Contractors: U.S. Official. The Time Magazine, S/f. [en línea[[fecha de consulta 10 de marzo 2017] Disponible en:

http://time.com/4696405/wikileaks-cia-contractors-documents-source/?xid=homepage

¿Qué pasaría si las Agencias de Inteligencia no pueden asegurar sus propias herramientas de hackeo?

Julián Sánchez
Defense One, 9 de marzo 2017

[…] Es un cliché de escándalos políticos que "el encubrimiento es peor que el delito": Los intentos de ocultar la mala conducta, porque son más fáciles de probar y proporcionar evidencia de otra manera elusiva de una mente culpable, a menudo terminan siendo más perjudicial políticamente que la mala conducta. […]

Existen, por supuesto, algunos puntos de interés real en el archivo de documentos, sobre todo en relación con una serie de herramientas de hacking y explotaciones de software desarrolladas o utilizadas por el Grupo de Desarrollo de Ingeniería de la Agencia Central de Inteligencia, y es probable que surjan más como reporteros y analistas A través de más de 8.000 archivos y documentos, hemos confirmado que la CIA ha colgado y explotado al menos un puñado de vulnerabilidades no reveladas en plataformas de software ampliamente utilizadas, incluyendo el iOS de Apple y Android de Google, los sistemas operativos en los que casi todos los smartphones modernos funcionan.

También aprendimos que -como muchos de nosotros esperábamos- los obstáculos a la escucha telefónica convencional que plantea la creciente prevalencia del cifrado han impulsado a las agencias de inteligencia a buscar medios alternativos de recopilación que incluyan no sólo comprometer los puntos finales de comunicaciones como los teléfonos inteligentes sino también buscan la reutilización de estos en dispositivos de vigilancia. […]

Sin embargo, a la luz de lo que ya sabíamos acerca de los propios esfuerzos de la Agencia Nacional de Seguridad en términos similares, gracias a las revelaciones de Edward Snowden sobre la división de Operaciones de Acceso Personalizado de la agencia, esto es, al menos desde una perspectiva de política. Por otra parte, hay poco aquí para sugerir una vigilancia que sea dirigida a los estadounidenses, las características que hicieron las fugas de Snowden sobre la vigilancia de la NSA tan políticamente explosiva.

Uno de los proyectos más ampliamente reportados en el Vault 7, por ejemplo, ha sido el implante "Weeping Angel" de Doctor Who, que puede convertir los televisores Samsung en micrófonos de vigilancia incluso cuando aparezcan apagados. Sin embargo, al menos en el momento en que se escribió la documentación en el comunicado de Wikileaks, Weeping Angel parecía requerir acceso físico para ser instalado, lo que lo hace esencialmente un método extravagante y menos detectable una vez que un agente de la CIA logró acceso al instalar el dispositivo dentro. […] Encontrar maneras inteligentes de espiar a la gente es lo que las agencias de espionaje se supone que deben hacer.

Lo que es realmente vergonzoso para la comunidad de inteligencia, sin embargo, es el hecho de la fuga en sí misma, abarca no sólo miles de páginas de documentación, sino también, según Wikileaks, el código fuente real de las herramientas de hacking que describen esos documentos. […] Peor aún, esto ocurre sólo unos meses después de que la aún más desastrosa filtración de Shadow Brokers, que publicó una serie de "exploits" supuestamente utilizados por el NSA-linked Equation Group para comprometer los routers y firewalls confiados por muchas de las compañías más grandes del mundo para asegurar sus redes corporativas .

Eso es de gran importancia para el debate en curso sobre cómo las agencias de inteligencia deben responder cuando descubren vulnerabilidades en software comercial o firmware ampliamente utilizado. ¿Informan al vendedor que tienen un agujero de seguridad que podría poner a sus usuarios en riesgo, o no mantener la calma y hacer uso de la vulnerabilidad para permitir su propia vigilancia? Si este último, ¿cuánto tiempo esperan hasta revelar? En 2014, el zar de ciberseguridad de la Casa Blanca intentó tranquilizar al público que el mecanismo gubernamental para tomar tales decisiones -un proceso informal de "Equidad de Vulnerabilidad" diseñado para sopesar el beneficio de inteligencia de mantener una explotación contra el interés del público en cerrar los agujeros de seguridad- fue fuertemente sesgada a favor de la divulgación. […] Pero los medios por los cuales lo conocemos deberían fortalecer aún más el caso de la revelación.

Antes de la fuga de "Shadow Brokers", la principal preocupación de los expertos en seguridad había sido que cuanto más tiempo una vulnerabilidad de software fuera mantenida en secreto por las agencias de espionaje, mayor sería el riesgo de que algún agente malintencionado -ya sea un hacker criminal u otra agencia de inteligencia- lo use ahora, sin embargo, necesitamos tener en cuenta la creciente evidencia de que la comunidad de inteligencia no puede asegurar adecuadamente sus propias herramientas de hacking. Y las brechas de este tipo crean riesgos significativamente más altos, porque dan lugar a una amplia circulación, no sólo de vulnerabilidades individuales que pueden ser de uso limitado para un atacante en aislamiento, sino de suites enteras de ellas, ya en forma armada y convenientemente encadenadas […] Y dado que es probable que las agencias de inteligencia extranjeras estén más interesadas en usar armas cibernéticas robadas que regalarlas al mundo, parece razonable inferir que los dos casos conocidos públicamente de filtración a gran escala no son los únicos casos de este tipo.

Eso debería hacer que el público se sienta mucho más nervioso acerca de la perspectiva de que un enfoque miope en el mantenimiento de los accesos de inteligencia está haciendo a todos nosotros significativamente menos seguros en la red. Y debería impulsar una seria reevaluación dentro del gobierno sobre si su pretendido sesgo a favor de la revelación no debería ser mucho más fuerte.

SANCHEZ, Julian. What if Intelligence Agencies Can't Secure Their Own Hacking Tools. Defense One. Ideas, 9 de marzo 2017. [en línea] [fecha de consulta 10 de marzo 2017] Disponible en: http://www.defenseone.com/ideas/2017/03/can-intelligence-community-secure-its-own-hacking-tools/136026/?oref=d-topstory

El potencial cibernético de India: un puente entre oeste y este

Levi Maxey
The Cipher Brief, 5 de marzo 2017

Investigadores y responsables de la política de seguridad en todo el mundo están luchando con el desafío de asegurar las redes digitales que los gobiernos, las empresas privadas y la gente en general dependen cada día. Mientras que los puntos de referencia más comunes a los compromisos en el ciberespacio se encuentran en Estados Unidos, Europa, Rusia y China, otros países rápidamente se dan cuenta de la importancia de proteger las redes críticas del crimen, el sabotaje, la subversión y el espionaje. Como un país con una de las poblaciones y economías de más rápido crecimiento en el mundo, esta percepción está llevando a la India a crecer en este ámbito de manera más rápida.

Entonces, ¿cuál es la actual atmósfera de ciberseguridad de la India, dónde están las principales amenazas y qué papel desempeña el país en los esfuerzos normativos? Para Jonathan Reiber, Senior Fellow del Berkeley Center for Long-Term Cybersecurity y ex Director de Estrategia de Cyber Policy de la Oficina de la Secretaría de Defensa de EE. UU., Señala que "si bien China tiene más de 720 millones de usuarios de internet y Estados Unidos tiene a 460 millones de usuarios de Internet en 2016. Pero lo interesante es que Estados Unidos está en el 90 por ciento de penetración de los usuarios, y para finales de 2015, China e India fueron sólo cerca del 51 por ciento y el 36 por ciento de penetración respectivamente.

"Esto significa que la India, y su populosa vecina China, empequeñecerán a otros países en individuos y organizaciones conectados digitalmente y, por lo tanto, también en vulnerabilidades de superficie de ataque. Cherian Samuel, investigadora en el Centro de Tecnologías Estratégicas del Instituto de Estudios y Análisis de Defensa en New Dehli, señala que ya "India ha enfrentado ataques de actores no estatales, cibercriminales y hacktivistas. Los actores no estatales, respaldados por los sospechosos habituales, han participado en gran medida en el espionaje cibernético mediante la piratería en las redes gubernamentales, mientras que los ciberdelincuentes se han alimentado del paisaje en constante expansión de Digital India. Hacktivists que se identifican como parte de los grandes colectivos anónimos y los llamados hackers patrióticos también se han dirigido a las redes y sistemas de la India".

Ya en 2010, el gobierno de la India señaló que más de 3.600 sitios web fueron hackeados en el lapso de seis meses. El delito cibernético en India subió un 350 por ciento desde 2011 hasta 2014, y justo el mes pasado, las autoridades indias arrestaron a personas involucradas en una estafa en línea que engañó a 650.000 personas enviando $ 550 millones a cuentas controladas por delincuentes. Reiber señala que "India se enfrenta a una gran cantidad de cibercrimen. Ransomware es un gran problema y una gran preocupación para el gobierno de la India, ya que la gente a menudo tiene sus contraseñas robadas y el control de sus dispositivos en poder de los criminales".

Al igual que otros países, aunque quizás en menor medida, los factores geopolíticos de la India influyen en el mundo cibernético. El año pasado, las empresas de ciberseguridad Proofpoint y FireEye revelaron una campaña sostenida de espionaje cibernético dirigida a funcionarios gubernamentales indios, supuestamente el trabajo de un grupo paquistaní. La mayor parte de la actividad aparentemente emanada de Pakistán, sin embargo, parece venir en forma de degradación básica del sitio web. El problema, por supuesto, es la atribución. Según Samuel, "no ha habido ningún medio para verificar si están actuando de forma independiente o bajo la dirección de manos invisibles." Mientras tanto, en 2013 la firma de seguridad cibernética rusa Kaspersky dio a conocer un informe que identifica una campaña de espionaje cibernético chino sostenida focalización instituciones de la India, mientras que en 2015 FireEye sostuvo que China estaba cavando en los cuerpos gubernamentales indios, universidades y compañías para robar información política, militar y económica sensible.

La amenaza de la escalada de ciberataques llevó a los funcionarios indios a pedir la creación de un comando cibernético militar en 2013, con el objetivo de crear una fuerza de 500.000 hombres. La India también ha tratado de establecer un Centro Nacional de Coordinación Cibernética como un mecanismo centralizado para monitorear el tráfico de Internet en cooperación con los proveedores de servicios de Internet locales con el fin de evaluar mejor las amenazas de ciberseguridad - y facilitar variedad de otra colección de inteligencia internacional y nacional similar a la NSA PRISM, revelado en 2013 por el ex contratista Edward Snowden. Los defensores de la libertad en Internet, sin embargo, temen que el nuevo aparato de inteligencia pueda facilitar la vigilancia interna y la censura en la democracia más grande del mundo.

Por otra parte, al igual que las campañas de información que plagaron la elección presidencial de EE.UU durante el 2016. - y los que amenazan la integridad de muchos próximas elecciones europeas - existe el temor de que las redes de bots se podrían utilizar para sembrar la confusión y la duda entre una ciudadanía cada vez más informada india digitalmente. Los actores regionales como China y Pakistán podrían influir indirectamente en la política, mientras que Rusia, a pesar de ser el principal suministrador de equipo militar de la India, podría ganar el favor o simplemente alterar las deliberaciones internas de la India.

Hasta la fecha, la India ha mostrado una estrecha cooperación con los Estados Unidos en el establecimiento de normas internacionales en el ciberespacio. Reiber argumenta que "la India es un país de leyes y democracia, y comparten valores y puntos de vista similares del mundo con los Estados Unidos. Respecto a las normas de las operaciones del ciberespacio, la India sigue en gran medida las leyes del conflicto armado. Estados Unidos también lo hace, y los Estados Unidos quieren asociarse con la India en toda una serie de cuestiones estratégicas que afectan a ambos países".

Un ejemplo de normas compartidas, según Reiber, ha sido que la India expresó su deseo de seguir un modelo de múltiples partes interesadas del gobierno del Internet, similar al modelo de ICANN desde hace mucho tiempo en los Estados Unidos. La adopción envía un mensaje a otros países en vías de desarrollo para que se pueda asegurar Internet sin infringir la libertad de expresión y el comercio. India también ha inyectado la norma en las conversaciones con Rusia y China, mostrando que la India podría actuar como un puente entre Oriente y Occidente en foros internacionales.

Sin embargo, Samuel sostiene que "mientras Estados Unidos y la India han tenido una historia de consultas sostenidas sobre la seguridad cibernética, con una serie de acuerdos que se firmaron entre los organismos competentes de los dos países, entre ellos un acuerdo marco general en el año 2016, estos avances todavía no han logrado diferencia visible en la ciberseguridad de la India". India, al igual que todos los países, tiene un largo camino por recorrer para asegurar sus redes digitales.

MAXEY, Levi. India’s Cyber Potencial: A Bridge Between East and West. The Cipher Brief. 5 de marzo 2017. [en línea] [fecha de consulta 8 de marzo 2017] Disponible en:

https://www.thecipherbrief.com/article/asia/indias-cyber-potential-bridge-between-east-and-west-1092