El líder norcoreano Kim Jong-un inspecciona el Complejo Sci-Tech en Pyongyang, Corea del Norte, 28 de octubre de 2015. (Foto publicada por la Agencia Central de Noticias Coreana de Corea del Norte)

El apoyo cibernético norcoreano a las operaciones de combate

1er Teniente Scott J. Tosi, Ejército de EUA

Hasta el año 2014, algunos expertos cibernéticos occidentales describían las capacidades cibernéticas de Corea del Norte (la República Popular Democrática de Corea) con indiferencia aparente, tales como Jason Andress y Steve Winterfield en *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, quienes caracterizaron la capacidad de Corea del Norte de llevar a cabo ataques cibernéticos como «dudosa, pero puede existir»[1]. El notorio ataque cibernético de noviembre de 2014 atribuido a Corea del Norte, llevado a cabo contra la Corporación Sony como respuesta a la película *The Interview*, ayudó a cambiar las percepciones en Estados Unidos de las capacidades cibernéticas de Corea del Norte—desde una molestia local menor dirigida hacia Corea del Sur (la República de Corea) hasta una gran amenaza estratégica global[2].

Aunque Corea del Norte ha sido considerada una gran amenaza cibernética estratégica desde el ataque contra Sony, también debe darse consideración al posible uso táctico de las capacidades cibernéticas como una extensión de su estrategia de guerra. El menos conocido uso táctico de ataques cibernéticos como medios de guerra presenta una mayor amenaza a Corea del Sur y las fuerzas de EUA que cualquier ataque cibernético estratégico motivado por la política. Se considera el material bélico de Corea del Norte tecnológicamente obsoleto a nivel táctico. Sin embargo, la evidencia sugiere que el Ejército Popular de Corea (EPC) llevará a cabo las operaciones cibernéticas como medios asimétricos para perturbar el mando y control enemigo y compensar por sus desventajas tecnológicas en las operaciones de combate; por lo tanto, EUA y las fuerzas aliadas deben prepararse para enfrentar esta amenaza[3].

La estrategia militar norcoreana

Para comprender cómo Corea del Norte probablemente llevaría a cabo las operaciones cibernéticas tácticas en apoyo de unidades de combate en la guerra, es útil considerar las metas históricas y la supuesta teoría militar de la nación cada vez más aislada y tecnológicamente débil. Después de fracasar en el esfuerzo de unificar la península de 1950 a 1953, *kukka mokp´-yo* —el hacer comunista a Corea del Sur, a través de la fuerza militar si sea necesaria— llegó a ser un objetivo principal de Corea del Norte, y sigue siendo así, según el experto en asuntos coreanos James M. Minnich[4]. Sin embargo, según lo señalado en un informe de 2012 al Congreso de EUA, el verdadero motivo de la política militar y agresividad política de Corea del Norte se ha convertido en un esfuerzo para controlar y sojuzgar a su propia población y guardar el poder en lugar de unificar la Península coreana[5]. No obstante, los acontecimientos tales como el bombardeo de la isla Yeonpyeong en 2010 y el intercambio de fuego de artillería en Yeoncheon en 2015 han demostrado que las provocaciones menores pueden tener la posibilidad de estallar en el combate abierto. Además, el combate podría convertirse en una guerra de gran escala. Ya sea a través de un escalamiento accidental de fuerza o una invasión sorpresiva premeditada, Corea del Norte podría estar completamente dispuesto a ir a la guerra[6].

Después de su fracaso en la guerra de Corea, Corea del Norte aumentó y reorganizó sus fuerzas armadas usando características de las fuerzas armadas rusas y chinas. Subsecuentemente, ha continuado aprovechando influencia, equipamiento y doctrina de Rusia y China, según Minnich[7]. Para evitar el mismo destino que la prolongada invasión que tomó lugar en Corea del Sur, las fuerzas armadas de Corea del Norte parecen haber desarrollado una estrategia conocida como *kisub chollyak*, que exige una guerra rápida y decisiva llevada a cabo con tácticas contra las fuerzas armadas de Corea del Sur y EUA en la península[8]. Este planteamiento ha llegado a ser más intransigente con el transcurso de tiempo debido a la creciente incapacidad económica de Corea del Norte de sostener una guerra prolongada. Por lo tanto, para lograr sus objetivos tácticos lo más rápido posible, Corea del Norte ha organizado sus fuerzas armadas para comenzar el combate con «bombardeos masivos convencionales y químicos de cañones y misiles mientras simultáneamente usa equipos de fuerzas de operaciones especiales», según Minnich[9]. Las estimaciones del número de fuerzas de operaciones especiales varían entre 80.000 y 100.000 soldados que podrían realizar ataques asimétricos en el sur, con la intención de apoyar a las fuerzas de infantería ligera de gran escala que seguirían[10].

Al principio, Corea del Norte probablemente consideró que el bombardeo y las operaciones especiales seguidas por una gran fuerza de invasión serían suficiente para rápidamente desestabilizar, confundir, superar en maniobra o abrumar a las fuerzas de Corea del Sur y

EUA ubicadas en la península antes de que pudieran llegar refuerzos de EUA. Sin embargo, la estrategia fue sacudida a principios de los años 1990, después de la caída de la Unión Soviética y su retirada de apoyo de material bélico. Sin duda alguna, esta sacudida fue amplificada en 1991 por la derrota inesperadamente rápida y fácil del Ejército iraquí de Saddam Hussein a manos de Estados Unidos. El Ejército iraquí intentó usar contra Estados Unidos tácticas y armas similares que Corea del Norte había pensado usar por mucho tiempo contra Corea del Sur[11]. La caída del ejército de Hussein, numéricamente superior a las fuerzas armadas de EUA, con certeza sirvió como una advertencia a China y Corea del Norte, que dependían de fuerzas tecnológicamente inferiores pero numéricamente superiores para abrumar rápidamente a sus enemigos. La tecnología resultó ser superior a los números abrumadores en el combate de fuerza contra fuerza. Al mismo tiempo, la probabilidad de que las fuerzas de Corea del Norte fuesen fácilmente superadas por las ventajas tecnológicas de EUA fue acompañada por una deterioración rápida en los sectores agrícolas y económicos de Corea del Norte, lo que disminuyó aún más su capacidad de proyectar y sostener las fuerzas armadas[12].

La respuesta de Corea del Norte a estos acontecimientos incluyó el establecimiento de su programa nuclear[13]. Mientras el éxito de EUA en la Operación *Desert Storm* sugirió que las fuerzas armadas de Corea del Norte podrían ser derrotadas rápida y decisivamente por Estados Unidos en una guerra convencional, aunque con un posiblemente alto costo de vida de civiles coreanos, el programa nuclear de Corea del Norte introdujo un alto riesgo de destrucción masiva de blancos de Corea del Sur y EUA, en el caso de que Estados Unidos o Corea del Sur provocaran una guerra.

No obstante, aunque el desarrollo de una opción de disuasión nuclear apoyó las metas políticas defensivas de Corea del Norte, hizo poco para avanzar la posibilidad de kukka mokp'yo. Para esto, parece que Corea del Norte ha imitado los cambios doctrinales aparentes de China que se hicieron en las secuelas de la Operación *Desert Storm*.

Después de que Estados Unidos derrotara al Ejército iraquí —el quinto Ejército más grande del mundo en 1990— en solo cinco semanas, las fuerzas armadas chinas aparentemente reevaluaron sus tácticas y estrategia de guerra[14]. En los años 1990, China desarrolló una estrategia de guerra híbrida que dependió de métodos tecnológicos relativamente baratos para denegar la superioridad militar cualitativa de Estados Unidos a través de ataques indirectos. En 1999, la evidencia de la nueva metodología de las fuerzas armadas de China fue publicada en *Unrestricted Warfare: China's Master Plan to Destroy America* (una traducción resumida en inglés basada en una publicación de dos coroneles chinos en 1999), en la cual se describía el uso de varias medidas asimétricas para derrota a Estados Unidos, incluyendo llevar a cabo la guerra de información con el objetivo de denegar las visibilidad del campo de batalla a las fuerzas armadas de EUA a toda costa[15]. Los experto es seguridad nacional Richard A. Clarke y Robert Knake aseveran que esta estrategia ha resultado en la adopción por China de la guerra cibernética de gran escala, que incluye el robo de información tecnológica y la selección de blancos tácticos —medios de inteligencia, reconocimiento y vigilancia— para equilibrar el campo de batalla en cualquier acción de fuerza contra fuerza[16].

Presumiendo que su programa nuclear disuadiría ataques contra su territorio nacional y habiendo sobrevivido la crisis económica y agrícola de los años 1990, Corea del Norte enfrentó un dilema a principios del siglo XXI parecido a lo que China enfrentó en las secuelas de la Guerra del Golfo, cuando llegó a ser aparente que China sería vulnerable a la derrota por la tecnología militar avanzada de EUA. La respuesta general de Corea del Norte a este dilema consistía en tres iniciativas: incrementar el número de fuerzas de operaciones especiales para llevar a cabo la guerra no convencional, aumentar el número de medios de guerra electrónica e inteligencia de transmisiones para realizar operaciones de interferencia radioelectrónica y, de mayor importancia, establecer las operaciones cibernéticas tácticas y estratégicas bajo lo que son conocidos como la Agencia 121, la Oficina Nro. 91 y el Laboratorio 110. Como es el caso con cualquier aspecto de Corea del Norte, es difícil verificar información sobre estas organizaciones.

La organización cibernética norcoreana

Se ha informado que la Agencia 121, Oficina Nro. 91 y Laboratorio 110 son componentes de seis agencias subordinadas a la Agencia General de Reconocimiento (RGB), que se especializa en la

recolección de inteligencia bajo la administración del Departamento de Estado Mayor (GSD). Aunque el Departamento de Estado Mayor es responsable del mando y control del Ejército Popular de Corea, está subordinado al Ministerio de las Fuerzas Armadas Populares (MPAF), según Andrew Scobell y John M. Sanford18. Esta estructura le daría a la Agencia General de Reconocimiento el control operativo directo desde la cima de la cadena de mando y garantiza que el componente cibernético podría llevar a cabo las operaciones de manera independiente y en apoyo del Ejército Popular de Corea basado en la necesidad operativa.

La Agencia 121 supuestamente consta de un componente de recolección de inteligencia y un componente de ataque. Se opina que la unidad opera en Pyongyang, así como en el Hotel Chilbosan en Shenyang, China[19]. Se piensa que la Oficina Nro. 91 opera en Pyongyang para realizar las operaciones de hackeo para la Agencia General de Reconocimiento[20]. Se piensa que el Laboratorio 110 lleva a cabo el reconocimiento técnico, infiltración de redes de computadoras, recolección de inteligencia a través de hackeo y la introducción de virus en las redes enemigas[21].

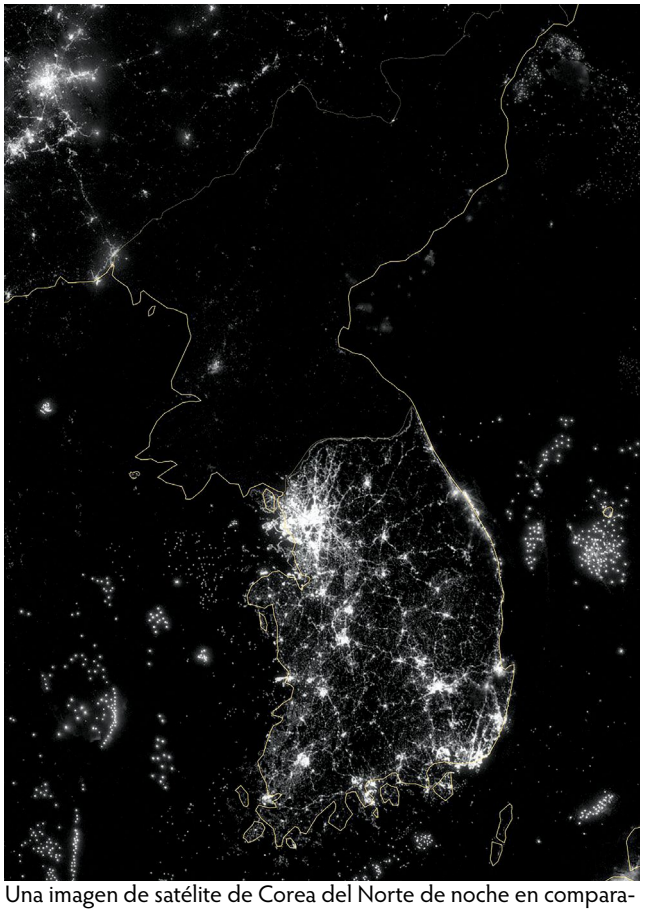
Aunque parece que hay otras numerosas organizaciones cibernéticas en Corea del Norte, las que están fuera de la Agencia General de Reconocimiento se relacionan principalmente con el control político o la difusión de propaganda política a naciones extranjeras. Por lo tanto, su trabajo se relaciona poco con al apoyo cibernético de las operaciones de combate.

Las estimaciones del tamaño de la fuerza cibernética de Corea del Norte han variado de solo 1.800 hackers y expertos de computadoras a casi 6.000, que lo haría la tercera agencia cibernética más grande detrás de Estados Unidos y Rusia[22]. El cálculo más alto

Ha sido ampliamente reportado que los hackers del Ejército norcoreano trabajan en el Hotel Chilbosan (fotografiado el 17 de abril de 2005), en parte propiedad del gobierno de Corea del Norte, en Shenyang, China. Tales informes son creíbles debido, en parte, a las ventajas aparentes de trabajar en China, tal como la disponibilidad de múltiples líneas de comunicación, sin mencionar el equipamiento moderno, entrenamiento, apoyo logístico y una fuente confiable de potencia eléctrica. (Véase, por ejemplo, James Cook, «PHOTOS: Inside The Luxury Chinese Hotel Where North Korea Keeps Its Army of Hackers», página web de Business Insider, 2 de diciembre de 2014, accedido 12 de junio de 2017, http://www.businessinsider.com/photos-chinese-hotel-where-north-korea-keeps-hackers-2014-12). (Foto: tack well, Flicker)

supuestamente es de la inteligencia de Corea del Sur a principios de 2015, pero no puede verificarse el número. Además, no era evidente si se incluían la Oficina Nro. 91 y el Laboratorio 110 en el cálculo, pero dado el deseo de Corea del Sur de influenciar a Estados Unidos

a considerar las amenazas cibernéticas de la DPRC una prioridad, es probable la inclusión de su personal en el número total (algunas personas consideran equivocadas las estimaciones de Corea del Sur debido a su prejuicio). Además, la estimación de Corea del Sur representa datos de 2013 y, como es el caso con mucha de la inteligencia sobre Corea del Norte, probablemente no refleja los números actuales.



Una imagen de satélite de Corea del Norte de noche en comparación con Corea del Sur. El atraso tecnológico supuestamente obliga a los hackers del Ejército norcoreano a buscar lugares fuera de Corea del Norte, tal como el Hotel Chilbosan en China, donde el acceso a la tecnología y las líneas de comunicación está disponible para llevar a cabo ataques cibernéticos. (Imagen: NASA)

No obstante, la falta de conocimientos concretos sobre las organizaciones cibernéticas de Corea del Norte se agrava por la naturaleza del acceso al Internet en el país. Corea del Norte ha divido sus redes en dos componentes. Solo las agencias gubernamentales y militares pueden acceder a la red externa canalizada a través de China, que los hackers usan para realizar los ataques cibernéticos. El otro componente es la *kwangmyong*, una intranet monitoreada de contenido seleccionado por el gobierno[23]. A partir de enero de 2013, se reportó un «café de Internet» en Corea del Norte, en Pyongyang, donde los ciudadanos supuestamente pueden acceder solo a la kwangmyong[24]. El uso de redes chinas para acceder al Internet proporciona un buffer para los hackers norcoreanos para negar la responsabilidad de sus intrusiones y ataques. Además, pueden llevar a cabo ataques externos con seguridad mientras evitan los ataques de entrada de Corea del Sur o Estados Unidos[25].

Sin embargo, el uso de terceros para el acceso externo del Internet también hacen las operaciones cibernéticas de Corea del Norte dependientes de la cooperación constante con China y otros socios. A pesar del apoyo decreciente al Estado aislado en los últimos años, el apoyo de China parece garantizado en tiempos de paz. Sin embargo, no es garantizado si estalla la guerra.

Puesto que el bajo nivel de conectividad funciona como protección de ataques externos, Corea del Norte puede concentrarse en el desarrollo de capacidades cibernéticas ofensivas. Si fueran comprometidos, pocos sistemas o redes de Corea del Norte reducirían sus capacidades de guerra[26]. Los bien conocidos ataques cibernéticos atribuidos a hackers de Corea del Norte han servido motivos en gran parte estratégicos y políticos. Sin embargo, el apoyo cibernético a las unidades de combate en caso de guerra de gran escala probablemente sigue siendo un componente clave de la estrategia norcoreana.

La guerra cibernética es única en el sentido de que una vez que haya sido usada una nueva metodología o técnica en un ataque, la víctima puede crear contramedidas relativamente rápidas para prevenir los ataques futuros. Probablemente por esta razón, Corea del Norte no ha llevado a cabo ataques cibernéticos tácticos u operativos de gran escala contra Corea del Sur o Estados Unidos, ni probablemente no lo haría, a menos que esté en un estado de guerra. En cambio, Corea del Norte solo realizaría el reconocimiento de menor escala y comprobación de metodologías contra las redes enemigas. Este planteamiento reduciría el riesgo de enemigos que desarrollan contramedidas que comprometerían las ventajas que Corea del Norte desea mantener para la guerra de gran escala.

Aunque las fuerzas de EUA y de sus socios saben relativamente poco sobre las capacidades cibernéticas de Corea del Norte, sí se pueden estudiar China y Rusia. China, como el aliado más estrecho de Corea del Norte (y tal vez el único), proporciona no solo las redes externas a las unidades cibernéticas norcoreanas sino también bases de operaciones, tal como el Hotel Chilbosan, y el entrenamiento. Las conocidas acciones cibernéticas chinas se han centrado principalmente en el espionaje tecnológico, un blanco en el cual Corea del Norte probablemente tiene poco interés porque carece de la infraestructura para desarrollar o mantener las armas tecnológicamente avanzadas que tiene China. A la inversa, las actividades cibernéticas de Rusia en la invasión de Georgia en 2008 y la acción militar en Ucrania en 2014 sugieren las probables acciones cibernéticas tácticas de Corea del Norte en caso de guerra en la península coreana.

El apoyo cibernético táctico norcoreano a la conducción de la guerra

Aunque una guerra terrestre, aérea y marítima en la península coreana comenzaría o incrementaría en una fecha y tiempo específico, la guerra cibernética comenzaría mucho antes de que se disparen los primeros tiros[27]. Se puede argumentar que aunque la guerra cibernética con Corea del Norte ya está en curso, necesitaría incrementar la frecuencia e intensidad en el reconocimiento y los ataques cibernéticos antes de una guerra generalizada para apoyar a las unidades de combate con éxito. Antes de una guerra y en sus primeras etapas, las unidades cibernéticas asimétricas norcoreanas atacarían las comunicaciones civiles a través de una simple denegación de servicio.

En 2008, Rusia comenzó su ataque contra Georgia con ataques de denegación distribuida de servicios por semanas antes de que los soldados cruzaran la frontera para comprobar sus capacidades y realizar el reconocimiento de las redes georgianas, con planes de atacarlas luego de nuevo. Rusia atacó las comunicaciones georgianas, paralizando la capacidad del Gobierno para comunicarse y coordinarse contra las fuerzas rusas[28]. Los ataques cibernéticos combinaron la simpleza con la sofisticación en la ejecución y permitieron que Rusia neutralizara el mando y las comunicaciones georgianos con pocos recursos. Lo que hubiera tomado días, si no semanas, de bombardeo y coordinación entre la inteligencia y el poderío aéreo solo llevó minutos desde la seguridad de computadoras rusas, pero logró los mismos resultados. Las fuerzas de EUA y sus socios razonablemente pueden anticipar que, como una nación tecnológicamente inferior con una fuerza aérea y armada obsoleta, Corea del Norte llevaría a cabo ataques similares.

Además, Corea del Norte parece haber demostrado tal capacidad. De 2014 a 2016, Corea del Norte supuestamente hackeó «más de 140.000 computadoras» en Corea del Sur pertenecientes al Gobierno y a empresas e intentó atacar la red de control del sistema de transporte de Corea del Sur[29]. Los ataques, probablemente llevados a cabo por la Agencia 121, permitieron que Corea del Norte ganara el acceso a las comunicaciones del Gobierno y las empresas en Corea del Sur y las monitoreara.

Si esto hubiera ocurrido durante una invasión, Corea del Norte podría haber apagado todas estas computadoras, dejando las comunicaciones de estas organizaciones inoperables. Corea del Norte podría haber apagado o interrumpido el flujo del sistema de transporte de Corea del Sur.

Si incrementan en alcance o agresividad, tales ataques podrían cortar las capacidades de comunicación e intercambio de información entre el Gobierno de Corea del Sur y las fuerzas armadas. Si se hubieran llevado a cabo conjuntamente con ataques contra los sistemas de comunicación físicos en Corea del Sur por parte de las fuerzas de operaciones especiales, Corea del Norte podría neutralizar las comunicaciones de Corea del Sur y EUA, dejando a ciegas las unidades en el campo de batalla. Cortar las comunicaciones en las primeras etapas de la guerra anularía la capacidad de Corea del Sur y EUA de coordinar sus medios aéreos y de artillería, que daría a Corea del Norte tiempo y espacio suficiente para abrumar a las fuerzas de Corea del Sur y EUA en la zona desmilitarizada.

Mientras los ataques contra las comunicaciones y redes críticas en Corea del Sur dificultarían los esfuerzos de Corea del Sur y EUA, los medios de comunicación alternos aún podrían permitir que las dos naciones contrarrestaran la agresión de Corea del Norte. Sin embargo, los vitales medios de comunicación secundarios podrían ser neutralizados con ataques contra la red eléctrica de Corea del Sur,

Alumnos trabajan en computadoras en la Escuela Revolucionaria Mangyongdae en Pyongyang, Corea del Norte, 13 de abril de 2013. La escuela es administrada por las fuerzas armadas y los administradores dicen que fue establecida en 1947 para niños que habían perdido a sus padres durante la lucha por la liberación de Corea de los invasores japoneses. (Foto: Associated Press)

posiblemente denegando la superioridad que tienen Corea del Sur y EUA sobre Corea del Norte al demorar una respuesta coordinada oportuna a la agresión. Hace varios años, tal ataque hubiera sido considerado imposible por una nación tan tecnológicamente retrasada como Corea del Norte. Hoy en día, este tipo de ataque por Corea del Norte en caso de guerra es casi indudable.

Por ejemplo, en diciembre de 2015, los hackers rusos causaron un apagón en Ucrania por medio de un ataque cibernético. Instalaron programas malignos en la red de las centrales eléctricas de Ucrania y remotamente apagaron interruptores para cortar la energía eléctrica de más de 225.000 personas[30]. Entonces, Rusia inundó las líneas de asistencia a los clientes de servicios públicos con llamadas falsas para impedir que la compañía recibiera llamadas de sus clientes[31]. Dado el nivel de sofisticación que parecen haber alcanzado las unidades cibernéticas de Corea del Norte y las relaciones que Corea del Norte mantiene con Rusia, es probable que Corea del Norte haya recibido apoyo de Rusia para posiblemente llevar a cabo ataques contra las centrales eléctricas de Corea del Sur.

Los ataques cibernéticos, en esencia, serían un planteamiento asimétrico para compensar por la fuerza aérea casi inexistente de Corea del Norte. Podrían infligir daños tácticos y operativos en Corea del Sur para perfeccionar los bombardeos de «conmoción y pavor» que probablemente precedan una intervención militar. Con la destrucción de comunicaciones, transporte e infraestructura de apoyo críticos, Corea del Norte podría causar confusión y desorden que facilitaría una acción abrumadora por sus fuerzas de infantería convencionales contra las fuerzas de Corea del Sur y EUA.

No obstante, aunque estos métodos podrían ser eficaces, es poco probable que la Agencia 121 sea capaz de completamente incapacitar la red de Corea del Sur,

pero una interrupción fraccionaria de la red podría impedir gravemente las acciones de Corea del Sur y EUA en el campo de batalla. Para completamente denegar la superioridad tecnológica de Corea del Sur y EUA, Corea del Norte necesitaría usar ataques más sofisticados contra sistemas de posición global, radares y apoyo logístico, así como sistema de adquisición de blancos. Exactamente cómo Corea del Norte llevaría tales ataques está fuera del alcance de la presente discusión. Sin embargo debe tomarse en serio la amenaza, como advierte el Consejo de Ciencia de Defensa, «si Estados Unidos llegara a encontrarse en un conflicto de gran escala con un adversario casi igual... es posible que no funcionen sus cañones, misiles y bombas, o que estos puedan ser dirigidos contra sus propios soldados. El reabastecimiento, incluyendo comestibles, agua, municiones y combustible tal vez no lleguen a tiempo donde se necesiten»[32].

Hackear o incapacitar los radares y sistemas de posición global, aún por algunos días antes de que las fuerzas de Corea del Sur y EUA puedan recuperarse, podría prohibir el uso del poderío aéreo, ofreciendo a las unidades de Corea del Norte la libertad de maniobra en el campo de batalla. Además, la interrupción del sistema de posición global no solo denegaría el uso de sistemas guiados por este sistema, sino más peligrosamente, podría causar que las armas dispararan en las coordenadas incorrectas. El hackeo de satélites de EUA, que China supuestamente ya ha demostrado que puede hacer, podría dejar ciegos los medios de inteligencia de Corea del Sur y EUA con respecto a los movimientos de Corea del Norte en el terreno[33].

Si Corea del Norte hackeara las redes logísticas automatizadas que apoyan a las fuerzas de Corea del Sur y EUA en la península, estas fuerzas tendrían dificultades en el sostenimiento de sus capacidades de guerra. El rastreo, solicitudes y entrega de suministros de guerra esenciales serían interrumpidos por un simple ataque de denegación distribuida que apagaría los sistemas o corrompería datos, causando que se envíen incorrectamente los suministros logísticos. Los soldados de Corea del Sur y EUA podrían encontrarse rápidamente sin los recursos necesarios para luchar.

Por lo tanto, Corea del Norte podría usar ataques cibernéticos para garantizar que su superioridad numérica y volumen abrumador de potencia de fuego triunfe a pesar de su material bélico inferior. Coherentes con las ideales en *Unrestricted Warfare*, cuando esto ataques se combinan con la guerra electrónica y las fuerzas de operaciones especiales actuando tras las líneas de combate, pueden causar que las fuerzas de Corea del Sur y EUA pierdan el ímpetu y mantengan una postura defensiva y reaccionaria.

En *Unrestricted Warfare*, se describe el «número áureo» y la regla «principio-lateral». El concepto es que el número áureo, 0,618 o aproximadamente dos tercios, que normalmente se aplica en las artes, la arquitectura y las matemáticas, puede aplicarse en la guerra. Los autores destacan que una vez que el Ejército iraquí fue reducido por la Fuerza Aérea de EUA a 0,618 de su fuerza original, colapsó y terminó la guerra[34]. La regla principio-lateral, en esencia, es el concepto de que puede ganarse la guerra a través de acciones no bélicas. Cuando se consideran estas dos teorías en conjunto, llega a ser obvio que aunque los chinos posiblemente piensan que no podrían derrotar a Estados Unidos en una guerra a través del combate convencional, probablemente piensan que podrían derrotar a Estados Unidos si se usaran acciones no bélicas para disminuir la fuerza militar de EUA hasta dos tercios de su poder de combate.

Para China, hay numerosas opciones para lograr esto porque tiene recursos crecientes que puede aprovechar para llevar a cabo las acciones no bélicas por largos períodos de tiempo, ya sean cibernéticos, financieros o políticos. Para Corea del Norte, con su meta de kukka mokp'yo y sus recursos muy limitados, hay un menor número de opciones. Corea del Norte probablemente traduciría el número áureo y la regla principio-lateral en una disminución de las fuerzas de Corea del Sur y EUA por un tercio a través de ataques cibernéticos, junto con numerosos otros medios asimétricos. Con sus sistemas fuera de servicio o corrompidos, las capacidades de guerra de EUA y Corea del Sur serían disminuidas o interrumpidas al grado que, teóricamente, Corea del Norte podría lanzar una masiva invasión terrestre. Por lo tanto, el ataque cibernético es un medio por el cual Corea del Norte probablemente atacaría sistemas de apoyo de guerra del enemigo, dándoles, por consiguiente, a sus fuerzas numéricamente superiores el espacio, tiempo y libertad de maniobra para sostener una lucha en la península.

Un ataque cibernético podría incluir un pulso electromagnético producido por una detonación nuclear

que incapacitaría dispositivos electrónicos dentro de un radio de 725 kilómetros[35]. Teóricamente, Corea del Norte podría lograrlo con la detonación de un dispositivo nuclear en la atmósfera a una altura de 48 kilómetros. Este ataque podría negar las ventajas tecnológicas de las fuerzas amigas en la península, dejando inútil todo equipamiento con un componente electrónico. Sin embargo, dada la amenaza de represalia nuclear, así como la mayor probabilidad del apoyo de EUA de una guerra prolongada, que probablemente resultaría en la derrota de Corea del Norte, esta opción seguirá siendo un último recurso y no sería en un ataque nuclear táctico.

Las soluciones para neutralizar las capacidades cibernéticas de Corea del Norte

La jefatura norcoreana probablemente piensa que Corea del Norte podría revertir el equilibrio de poder táctico a lo que existió en los años 1950, a través del uso de sus capacidades cibernéticas para lograr una ventaja. En junio de 1950, las fuerzas terrestres tácticas de EUA fueron penosamente derrotadas por un enemigo numéricamente superior que tuvo menos entrenamiento y equipamiento y que se consideró estar menos preparado para la guerra. Mientras Estados Unidos continúa replegando unidades de combate permanentes de Corea del Sur y revirtiéndose a un rol de apoyo, dejando a sus fuerzas en la península mal preparadas para organizar una defensa de gran envergadura, debería tomar acción para evitar encontrarse en una situación parecida a la de 1950.

Las capacidades cibernéticas de Corea del Norte no son invulnerables. En 2014, como represalia por el hackeo contra Sony, Estados Unidos realizó un ataque tipo denegación distribuida de servicios contra Corea del Norte que tomó la kwangmyong fuera de línea[36]. Sin embargo, este ataque no tomó represalias contra las unidades cibernéticas, que en gran parte opera en China, pero en su lugar tomó la intranet fuera de línea. Este acontecimiento destaca una gran vulnerabilidad de Corea del Norte en tiempos de una guerra de gran escala. La operatividad cibernética de Corea del Norte probablemente estaría a merced del Gobierno chino. Si el Gobierno chino decide que el apoyo constante a Corea del Norte es políticamente insostenible, la capacidad cibernética norcoreana podría ser marginada.

Para mitigar los riesgos de amenazas cibernéticas de Corea del Norte, las fuerzas del Ejército deben asociarse activamente con las fuerzas de Corea del Sur y reevaluar cómo consideran las operaciones cibernéticas. Como medida preventiva, las unidades cibernéticas del Ejército deben monitorear las redes estadounidenses en Corea del Sur y las redes de las unidades que están programadas para ser desplegadas en Corea del Sur porque estas unidades son las que probablemente serán atacadas por los medios cibernéticos de Corea del Norte. En lugar de activamente neutralizar las amenazas cibernéticas de Corea del Norte, los líderes del Ejército deben evaluar los beneficios de inteligencia logrados al permitir la libertad de acción a sus adversarios para analizar sus tácticas, técnicas y procedimientos en el dominio cibernético.

Los líderes del Ejército deben comenzar a estudiar las operaciones cibernéticas como un multiplicador de fuerza y una ventaja tanto ofensiva como defensiva y no solo como un campo de especialidad fuera de los dominios táctico u operativo. Además, las fuerzas del Ejército acantonadas en Corea del Sur deben formular planes de contingencia con las fuerzas de Corea del Sur para anticipar los ataques cibernéticos parecidos a los ataques antes delineados en el presente artículo, y deben entrenar en los ambientes moldeados por la guerra cibernética. De esta manera, las fuerzas de EUA y Corea del Sur podrían mitigar la amenaza significativa presentada por las fuerzas cibernéticas de Corea del Norte. ■

El 1er teniente Scott J. Tosi, Ejército de EUA, es el segundo jefe de la Compañía A, 310º Batallón de Inteligencia Militar del 902º Grupo de Inteligencia Militar. Previamente sirvió como el segundo jefe de la Compañía del Cuartel General del 501er Batallón de Inteligencia Militar en Yongsan, Corea del Sur. Cuenta a su haber con una licenciatura en Historia y Educación de Ciencias Sociales de la Universidad Estatal de Illinois y fue instructor de Historia y Educación Cívica a nivel de escuela secundaria en Bloomington, Illinois.

Notas

1. Jason Andress y Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2ª ed. (Waltham, Massachusetts: Syngress, 2013), pág. 73. Andress y Winterfield citan a Jung Kwon Ho, «Mecca for North Korean Hackers», Daily NK online, 13 de julio de 2009.

2. Clyde Stanhope, «How Bad is the North Korean Cyber Threat», página web Hackread, 20 de julio de 2016, accedido 2 de mayo de 2017, https://www.hackread.com/how-bad-is-the-north-korean-cyber-threat/; Oficina del Secretario de Defensa (OSD), «Military and Security Developments Involving the Democratic People's Republic of Korea: 2015», A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2012, accedido 4 de mayo de 2017, https://www.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF.

3. James M. Minnich, *The North Korean People's Army: Origins and Current Tactics* (Annapolis, Maryland: Naval Institute Press, 2005), pág. 68.

4. *Ibíd*.

5. OSD, «Military and Security Developments Involving the Democratic People's Republic of Korea: 2012», A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2012, 15 de febrero de 2013, accedido 6 de mayo de 2017, http://archive.defense.gov/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf.

6. Daniel Wagner y Michael Doyle, «Scenarios for Conflict Between the Koreas», Huffington Post, 25 de febrero de 2012, accedido 2 de mayo de 2017, http://www.huffingtonpost.com/daniel-wagner/scenarios-for-conflict-be_b_1169871.html.

7. Minnich, *The North Korean People's Army*, págs. 53–54.

8. *Ibíd*., pág. 73.

9. *Ibíd*., págs. 73-74.

10. *Ibíd*.; Blaine Harden, «North Korea Massively Increases Its Special Forces», página web del *Washington Post*, 9 de octubre de 2009, accedido 3 de mayo de 2017, http://www.washingtonpost.com/wp-dyn/content/article/2009/10/08/AR2009100804018.html; OSD, «Military and Security Developments Involving the Democratic People's Republic of Korea: 2015».

11. Joseph Bermudez, *North Korea's Development of a Nuclear Weapons Strategy* (Washington, DC: US-Korea Institute at SAIS [Johns Hopkins School of Advanced International Studies], agosto de 2015), accedido 4 de mayo de 2017, http://uskoreainstitute.org/wp-content/uploads/2016/02/NKNF_Nuclear-Weapons-Strategy_Bermudez.pdf.

12. *Ibíd*.

13. *Ibíd*.

14. James M. Broder y Douglas Jehl, «Iraqi Army: World's 5th Largest but Full of Vital Weaknesses», *Los Angeles Times* en línea, 13 de agosto de 1990, accedido 8 de mayo de 2017, http://articles.latimes.com/1990-08-13/news/mn-465_1_iraqi-army.

15. Richard A. Clarke y Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (Nueva York: HarperCollins, 2010), págs. 28–29; Qiao Liang y Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, resumen de traducción (Panamá, Panamá: Pan American Publishing, 2002).

16. Clarke y Knake, Cyber War, págs. 30–32.

17. Harden, «North Korea Massively Increases Its Special Forces»; Stanhope, «How Bad is the North Korean Cyber Threat».

18. Andrew Scobell y John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle, Pensilvania: Strategic Studies Institute, 2007), págs. 14–16; Hewlett-Packard [HP] Enterprise SR [Security Research]-FI_Team, «Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape», HP Security Briefing, Episode 16, agosto de 2014, página web de HP Enterprise Community, accedido 6 de mayo de 2017, http://community.hpe.com/hpeb/attachments/hpeb/off-by-on-software-security-blog/388/2/HPSR%20SecurityBriefing_Episode16_NorthKorea.pdf.

19. SR_FI Team, «Profiling an Enigma: The Mystery of North Korea's Cyber Threat Landscape».

20. Pierluigi Paganini, «Concerns Mount over North Korean Cyber Warfare Capabilities», página web de Infosec Island, 11 de junio de 2012, accedido 14 de febrero de 2017, http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html.

21. «North Korea Launched Cyber Attacks, Says South», página web de *The Guardian*, 11 de julio de 2009, accedido 4 de mayo de 2017, https://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks.

22. Ju-min Park y James Pearson, «In North Korea, Hackers are a Handpicked, Pampered Elite», página web de Reuters, 5 de diciembre de 2014, accedido 6 de mayo de 2017, http://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205; Darren Pauli, «NORKS Hacker Corps Reaches 5,900 Sworn Cyber Soldiers—Report», página web Register, 7 de julio de 2014, accedido 6 de mayo de 2017, http://www.theregister.co.uk/2014/07/07/north_korea_employs_6000_leet_hackers_source_claims/.

23. Ashley Moreno, «Social Media in North Korea: The AP Bureau Chief from Pyongyang on Cell Service, Instagram, Etc.», página web del *Austin Chronicle*, 11 de marzo de 2013, accedido 4 de mayo de 2017, http://www.austinchronicle.com/daily/sxsw/2013-03-11/social-media-in-north-korea/.

24. Olga Khazan, «»North Koreans Shouldn't Count on Using the New Google Maps», página web del *Washington Post*, 29 de enero de 2013, accedido 3 de mayo de 2017, https://www.washingtonpost.com/news/worldviews/wp/2013/01/29/north-koreans-shouldnt-count-on-using-the-new-google-maps/.

25. OSD, «Military and Security Developments Involving the Democratic People's Republic of Korea: 2015».

26. Duk-Ki Kim, «The Republic of Korea's Counter-Asymmetric Strategy», *Naval War College Review* 65, nro. 1 (invierno de 2012): pág. 68, accedido 8 de mayo de 2016, https://www.usnwc.edu/getattachment/8e487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s-Counter-asymmetric-Strateg.aspx.

27. Para otra perspectiva de la guerra cibernética norcoreana, véase Kim «The Republic of Korea's Counter-Asymmetric Strategy», pág. 58.

28. John Markoff, «Before the Gunfire, Cyberattacks», página web del *New York Times*, 12 de agosto de 2008, accedido 3 de mayo de 2017, http://www.nytimes.com/2008/08/13/

technology/13cyber.html?_r=0.

29. Jack Kim, «North Korea Mounts Long-Running Hack of South Korea Computers, Says Seoul», página web de *Reuters*, 13 de junio de 2016, accedido 14 de febrero de 2017, http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE.

30. Dustin Volz, «U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage», página web de Reuters, 25 de febrero de 2016, accedido 14 de febrero de 2017, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

31. *Ibíd*.

32. Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, enero de 2013), pág. 5, accedido 3 de mayo de 2017, http://www.dtic.mil/docs/citations/ADA569975.

33. Mary Pat Flaherty, Jason Samenow y Lisa Rein, «Chinese Hack U.S. Weather Systems, Satellite Network», página web del *Washington Post*, 12 de noviembre de 2014, accedido 3 de mayo de 2017, https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html.

34. Qiao Liang y Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, págs. 153–69.

35. Andress y Winterfield, *Cyber Warfare*, pág. 147.

36. Cecilia Kang, «North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack», página web del *Washington Post*, 22 de diciembre de 2014, accedido 3 de mayo de 2017, https://www.washingtonpost.com/business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.