Dirigente norte-coreano Kim Jong-un inspeciona o Complexo Científico Tecnológico em Pyongyang, Coreia do Norte, 28 Out 15. (Foto disponibilizada pela Agência Central de Notícias da Coreia do Norte)

O Apoio Cibernético nas Operações de Combate da Coreia do Norte

1º Ten Scott J. Tosi, Exército dos EUA

Ainda em 2014, alguns especialistas ocidentais descreveram as capacidades cibernéticas da Coreia do Norte (República Popular Democrática da Coreia, ou RPDC) com visível indiferença, como Jason Andress e Steve Winterfield em *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, que caracterizaram a capacidade da RPDC para executar ataques cibernéticos como sendo "[...] duvidosa, mas possivelmente existente"[1]. O conhecido ataque cibernético de novembro de 2014, atribuído à RPDC e executado contra a Sony Corporation em resposta ao filme "A Entrevista", ajudou a mudar a impressão que os EUA tinham em relação às capacidades cibernéticas norte-coreanas — de uma insignificante perturbação local dirigida contra a Coreia do Sul (República da Coreia, ou RC) a uma grande ameaça estratégica global[2].

Além do fato de que a RPDC seja vista como uma importante ameaça cibernética estratégica desde o ataque contra a Sony, cabe considerar o potencial emprego tático de capacidades cibernéticas como uma extensão de sua estratégia de combate. O pouco conhecido emprego tático de ataques cibernéticos como um meio de combate representa uma ameaça maior às forças da RC e dos EUA do que seria qualquer ataque cibernético estratégico conduzido por motivos políticos. O material bélico das Forças Armadas da RPDC é considerado tecnologicamente obsoleto no nível tático. Entretanto, as evidências indicam que o Exército Popular da Coreia (EPC) conduzirá operações cibernéticas como um meio de guerra assimétrica para desorganizar o comando e controle inimigo e compensar suas desvantagens tecnológicas durante as operações de combate; portanto, as forças norte-americanas e aliadas devem se preparar para essa ameaça[3].

Estratégia Militar da Coreia do Norte

Para entender o modo pelo qual a RPDC provavelmente conduziria operações cibernéticas táticas em apoio a unidades de combate durante a guerra, vale considerar os objetivos históricos e a presumida teoria militar dessa nação, marcada por um isolamento cada vez maior e pelo declínio tecnológico. Após o fracasso da tentativa de unificar a península coreana entre 1950 e 1953, o lema *kukka mokp'yo* — isto é, a comunização da RC, pelo emprego de força militar, se necessário — passou e continua a ser um dos principais objetivos da RPDC, segundo James M. Minnich, especialista em assuntos coreanos[4]. Entretanto, conforme indicou um relatório elaborado para o Congresso em 2012, o verdadeiro objetivo da política militar e agressividade política da RPDC passou a ser o de controlar e subjugar sua própria população e manter-se no poder, em vez de unificar a península coreana[5]. Não obstante, acontecimentos como o bombardeamento da Ilha de Yeonpyeong, em 2010, e a troca de fogos de artilharia em Yeoncheon, em 2015, demonstraram que pequenas provocações têm o potencial de desencadear um combate aberto. Por sua vez, um combate poderia converter-se em uma guerra em larga escala. Seja por uma escalada acidental de força ou por uma premeditada invasão surpresa, a RPDC pode estar plenamente disposta a iniciar uma guerra[6].

Após seu fracasso na Guerra da Coreia, a RPDC ampliou e reorganizou suas Forças Armadas adotando características das Forças militares soviéticas e chinesas. Subsequentemente, tem continuado a receber influência, equipamentos e doutrina da Rússia e da China, segundo Minnich[7]. Para evitar sofrer a mesma sina que a prolongada invasão da RC, as Forças Armadas da RPDC parecem ter formulado uma estratégia conhecida como *kisub chollyak*, que propõe uma guerra rápida e decisiva conduzida com táticas mistas contra as forças da RC e dos EUA na península[8]. Essa abordagem tornou-se mais intransigente com o tempo, em virtude da crescente incapacidade econômica da RPDC para suportar uma guerra prolongada. Portanto, para alcançar seus objetivos táticos o mais rápido possível, a RPDC organizou suas Forças Armadas para iniciar o combate com "pesados bombardeios de canhões e mísseis convencionais e químicos empregando, ao mesmo tempo, equipes das Forças de Operações Especiais [F Op Esp]", segundo Minnich[9]. Estimativas sobre o efetivo das F Op Esp da RPDC o colocam entre 80 mil e 180 mil militares aptos a conduzir ataques assimétricos no sul, destinados a possibilitar o ataque em larga escala de tropas de infantaria leve que viriam em seguida[10].

Inicialmente, a RPDC provavelmente considerou bombardeios e operações especiais, seguidos de uma força de invasão de larga escala, suficiente para rapidamente desorganizar, confundir, superar em manobra e sobrepujar as tropas da RC e dos EUA baseadas na península antes que reforços norte-americanos

pudessem chegar. Entretanto, a estratégia sofreu um choque no início dos anos 90 após o colapso da União Soviética e a retirada do apoio em material bélico que ela fornecia. Esse choque foi, sem dúvida, intensificado em 1991 com a derrota inesperadamente fácil e rápida imposta pelos EUA ao Exército iraquiano de Saddam Hussein, que tentou empregar táticas e armas semelhantes às que a RPDC há muito planejava utilizar contra a RC[11]. A derrota do exército de Hussein, que dispunha de maior efetivo, para as Forças Armadas dos EUA serviu como um sinal de alerta para a China e a RPDC, que acreditavam que a superioridade numérica de suas forças, apesar de sua inferioridade tecnológica, pudesse sobrepujar seus inimigos rapidamente. Comprovou-se que, no combate entre forças convencionais, a tecnologia era superior a enormes efetivos. Concomitantemente, a probabilidade de que as forças da RPDC viessem a ser facilmente sobrepujadas pelas vantagens tecnológicas dos EUA foi acompanhada de um rápido declínio dos setores econômico e agrícola norte-coreanos, o que diminuiu ainda mais sua capacidade para projetar e manter suas forças militares[12].

A resposta da RPDC a esses acontecimentos incluiu o desenvolvimento de seu programa nuclear[13]. Enquanto o êxito norte-americano na Operação *Desert Storm* implicava que as Forças Armadas da RPDC poderiam ser derrotadas de maneira rápida e decisiva pelos EUA em uma guerra convencional, ainda que a um custo possivelmente alto em vidas de civis coreanos, o programa nuclear norte-coreano introduziu um elevado risco de destruição em massa de alvos da RC e dos EUA, caso estes países provocassem a guerra.

Não obstante, embora apoiasse objetivos políticos defensivos da RPDC, o desenvolvimento de uma opção de dissuasão nuclear contribuiu pouco para a perspectiva de *kukka mokp'yo*. Para isso, a RPDC parece ter imitado as aparentes mudanças doutrinárias da China, efetuadas após a Operação *Desert Storm*.

Após os EUA derrotarem o Exército iraquiano — quinto maior do mundo em 1990 — em apenas cinco semanas, as Forças Armadas chinesas reavaliaram, aparentemente, sua estratégia e táticas de combate[14]. Nos anos 90, a China formulou uma estratégia de guerra híbrida que se apoiava em métodos tecnológicos relativamente econômicos para neutralizar a superioridade militar qualitativa dos EUA por meio de ataques indiretos. Em 1999, evidências da nova abordagem das Forças Armadas chinesas apareceram em *Unrestricted Warfare: China's Master Plan to Destroy America* (uma versão resumida em inglês, baseada em uma publicação de 1999 por dois coronéis do Exército chinês), que descreveu a utilização de várias medidas assimétricas para derrotar os EUA, incluindo a condução de guerra da informação destinada a negar visibilidade do campo de batalha às Forças Armadas dos EUA por todos os meios necessários[15]. [Há uma versão em português intitulada "A guerra além dos limites: conjecturas sobre a guerra e a tática na era da globalização", tradutor desconhecido, disponível em https://www.egn.mar.mil.br/arquivos/cepe/GUERRAALEMLIMITES.pdf, da qual foram extraídos alguns termos. — N. do T.] Os especialistas em segurança nacional Richard A. Clarke e Robert Knake afirmam que essa estratégia resultou na adoção, pela China, da guerra cibernética de larga escala, que incluiria o furto de informações tecnológicas e a seleção de meios de Inteligência, Reconhecimento e Vigilância como alvos táticos para equalizar o campo de batalha em qualquer ação de combate entre forças convencionais[16].

Crendo que seu programa nuclear dissuadiria adversários de atacar seu território e tendo sobrevivido à crise econômica e agrícola dos anos 90, a RPDC enfrentava, no início da década de 2000, um dilema semelhante ao que a China encarou após a Guerra do Golfo, quando ficou claro que ela estaria vulnerável a ser derrotada pela avançada tecnologia bélica dos EUA. A resposta geral da RPDC a esse dilema incluiu três componentes: aumentar a quantidade de F Op Esp para conduzir a guerra não convencional; expandir seus meios de guerra eletrônica e Inteligência de Sinais para conduzir operações de interferência; e, o que é mais importante, criar operações cibernéticas táticas e estratégicas no âmbito das entidades

O 1º Ten Scott J. Tosi, do Exército dos EUA, é o Oficial Executivo da Companhia A, 310º Batalhão de Inteligência Militar, 902º Grupo de Inteligência Militar. Serviu, anteriormente, como Oficial Executivo de Companhia e Companhia de Comando, 501ª Brigada de Inteligência Militar em Yongsan, Coreia. É bacharel em Educação em História e Ciências Sociais pela Illinois State University, tendo lecionado História e Educação Cívica no ensino médio em Bloomington, Illinois.

conhecidas como Bureau 121, Escritório Número 91 e Lab 110[17]. Como no caso de qualquer aspecto da RPDC, é difícil verificar as informações sobre essas organizações sigilosas.

Organização Cibernética Norte-Coreana

Alega-se que o Bureau 121, Escritório Número 91 e Lab 110 fazem parte de seis componentes do Escritório Geral de Reconhecimento (RGB, na sigla em inglês), que se especializa na busca de Inteligência, sob a administração do Departamento do Estado-Maior Geral. Embora o Departamento do Estado-Maior Geral seja responsável pelo comando e controle do EPC, ele se enquadra no Ministério das Forças Armadas Populares, segundo Andrew Scobell e John M. Sanford[18]. Essa estrutura concederia ao RGB direto controle operacional a partir do topo da cadeia de comando e possibilitaria que o componente cibernético conduzisse operações de maneira independente e em apoio ao EPC com base na necessidade operacional.

De acordo com as informações disponíveis, *hackers* do Exército da Coreia do Norte trabalham no Hotel Chilbosan (foto de 17 Abr 05), em Shenyang, na China, o qual pertence, em parte, ao governo norte-coreano. Esses relatos são plausíveis devido, entre outros fatores, às evidentes vantagens de se trabalhar a partir de uma base na China, incluindo a pronta disponibilidade de múltiplas linhas de comunicação, para não mencionar os equipamentos modernos, treinamento, apoio logístico e confiável fonte de energia. (Veja, por exemplo, James Cook, "PHOTOS: Inside The Luxury Chinese Hotel Where North Korea Keeps Its Army of Hackers", Business Insider website, 02 Dec 14, acesso em 12 Jun 17, http://www.businessinsider.com/photos-chinese-hotel-where-northkorea- keeps-hackers-2014-12). (Foto de tack well, Flickr)

O Bureau 121, ao que consta, compreende um componente de busca de Inteligência e um componente de ataque. Acredita-se que ele opere principalmente de Pyongyang e do Hotel Chilbosan, em Shenyang, na China[19]. Aparentemente, o Escritório Número 91 está localizado em Pyongyang e conduz ações de *hacking* para o RGB[20]. Por sua vez, afirma-se que o Lab 110 conduz reconhecimento técnico, infiltração de redes de computadores, busca de Inteligência por *hacking* e introdução de vírus em redes inimigas[21].

Embora pareça haver muitas outras organizações cibernéticas na RPDC, as entidades não pertencentes ao RGB se concentram, principalmente, no controle político interno ou na disseminação de propaganda política a países estrangeiros. Portanto, seu trabalho não está muito relacionado ao apoio cibernético tático ou operacional a operações de combate.

As estimativas sobre a dimensão da força cibernética da RPDC variam entre 1.800 e cerca de 6.000 *hackers* e especialistas em informática, o que a tornaria a terceira

maior agência cibernética do mundo, atrás dos EUA e da Rússia[22]. A estimativa mais elevada teria sido fornecida pelo setor de Inteligência da RC no início de 2015, mas não é possível confirmar o número citado. Também não está claro se os efetivos do Escritório Número 91 e do Lab 110 fizeram parte do cálculo, mas, considerando o desejo da RC de induzir os EUA a priorizarem as ameaças cibernéticas advindas da RPDC, é provável que tenham sido incluídos (alguns consideram as estimativas da RC incorretas em virtude de sua parcialidade). Além disso, a estimativa da RC apresenta dados de 2013 e, como boa parte da Inteligência sobre a Coreia do Norte, já está desatualizada.

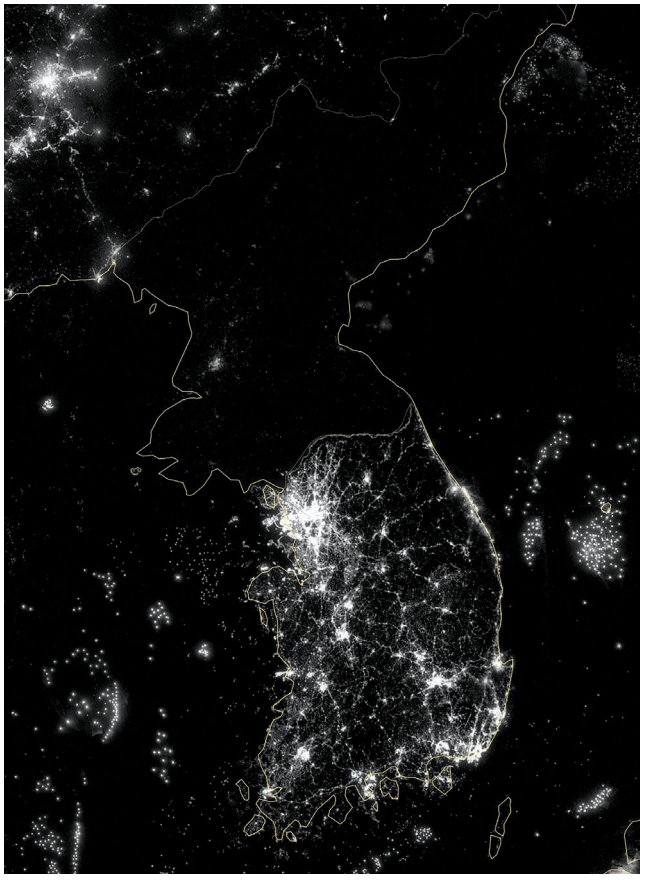

Imagem de satélite da Coreia do Norte comparada à Coreia do Sul à noite. Segundo consta, o atraso tecnológico obriga os *hackers* do Exército norte-coreano a buscar locais fora da Coreia do Norte, como o Hotel Chilbosan, na China, onde o acesso à tecnologia e a linhas de comunicação está prontamente disponível para a condução de ataques cibernéticos. (Imagem cedida pela NASA)

Independentemente disso, a escassez de conhecimentos concretos sobre as organizações cibernéticas da RPDC é agravada pela natureza de seu acesso à internet. A RPDC dividiu suas redes em dois componentes. Apenas os órgãos governamentais e militares podem acessar a rede voltada ao exterior e roteada através da China, que os *hackers* utilizam para conduzir ataques cibernéticos. O outro componente é a rede *kwangmyong*, uma intranet monitorada, com conteúdo selecionado pelo governo[23]. Em janeiro de 2013, foi identificado um "cyber café" na RPDC, em Pyongyang, onde os cidadãos podem, segundo consta, acessar apenas a *kwangmyong*[24]. O uso de redes chinesas para acessar a internet global fornece proteção aos *hackers* norte-coreanos, permitindo-lhes negar responsabilidade por suas intrusões e ataques. Além disso, eles podem conduzir, com segurança, ataques externos ao mesmo tempo que evitam ataques oriundos da RC ou dos EUA[25].

Entretanto, o uso de terceiros para acessar a internet externa também torna as operações cibernéticas da RPDC dependentes de uma contínua cooperação por parte da China e de outros parceiros. Apesar do apoio cada vez menor para o isolado Estado nos últimos anos, o respaldo da China parece estar garantido durante tempos de paz; não está garantido, porém, se a guerra eclodir.

Como o baixo nível de conectividade funciona como proteção contra ataques oriundos do exterior, a RPDC pode se concentrar no desenvolvimento de capacidades cibernéticas ofensivas. Caso comprometidos, poucos sistemas ou redes da RPDC reduziriam as capacidades de combate[26]. Os notórios ataques cibernéticos atribuídos a seus *hackers* têm servido, principalmente, a propósitos estratégicos e políticos. Entretanto, é provável que o apoio cibernético a unidades de combate, no caso de uma guerra em larga escala, continue a ser um importante componente estratégico da RPDC.

A guerra cibernética é peculiar pelo fato de que, uma vez que uma nova metodologia ou técnica tenham sido utilizadas, a vítima pode criar contramedidas relativamente rápido para prevenir futuros ataques. Por essa razão, talvez, a RPDC não conduziu ataques cibernéticos táticos ou operacionais de larga escala contra a RC ou os EUA — e muito provavelmente não conduzirá, a não ser em caso de guerra. Em vez disso, a RPDC conduziria apenas o reconhecimento em pequena escala e testes de metodologias contra as redes inimigas. Essa abordagem minimizaria o risco de que os inimigos

criassem contramedidas que fossem comprometer quaisquer vantagens que a RPDC quisesse conservar para uma guerra em larga escala.

Embora as forças norte-americanas e aliadas saibam relativamente pouco sobre as capacidades cibernéticas da RPDC, a China e a Rússia podem ser estudadas como modelos. A China, na qualidade de mais próximo (e talvez único) aliado da Coreia do Norte fornece não apenas redes conectadas ao exterior às unidades cibernéticas norte-coreanas, como também bases de operações, como o Hotel Chilbosan, e treinamento. As ações cibernéticas chinesas de que se tem conhecimento têm se concentrado, principalmente, na espionagem tecnológica, algo em que a RPDC deve ter pouco interesse, por não contar com a infraestrutura para construir ou manter armas tecnologicamente avançadas como a China. Em contrapartida, as atividades cibernéticas da Rússia durante sua invasão da Geórgia, em 2008, e sua ação militar na Ucrânia, em 2014, indicam quais serão as prováveis ações cibernéticas táticas da RPDC no caso de uma guerra na península coreana.

O Apoio Cibernético Tático ao Combate Norte-Coreano

Enquanto uma guerra terrestre, aérea e marítima na península coreana teria início — ou se intensificaria — a partir de uma data específica, a guerra cibernética começaria muito antes que qualquer tiro fosse disparado[27]. Embora se possa afirmar que a guerra cibernética com a RPDC já esteja em curso, ela teria de aumentar a frequência e a intensidade das ações de reconhecimento e ataques cibernéticos antes de uma guerra geral, para conseguir apoiar unidades de combate convencionais. No período anterior e estágios iniciais da guerra, as unidades cibernéticas assimétricas norte-coreanas visariam as comunicações civis por meio da simples negação de serviço.

Em 2008, a Rússia precedeu sua ofensiva contra a Geórgia com ataques distribuídos de negação de serviço (*distributed denial of service — DDOS*) durante semanas, antes que suas tropas cruzassem a fronteira, para testar suas capacidades e conduzir reconhecimento das redes georgianas, planejando atacá-las de novo posteriormente. A Rússia atacou as comunicações da Geórgia, prejudicando a capacidade do governo para se comunicar e coordenar ações contra as forças russas[28]. Os ataques cibernéticos russos conjugaram simplicidade com sofisticação na execução; permitiram que a Rússia derrubasse, de uma forma econômica, o comando e as comunicações da Geórgia. O que teria levado dias, se não semanas, de bombardeamento e coordenação entre Inteligência e poder aéreo levou minutos, a partir da segurança dos computadores russos, mas produziu o mesmo resultado. Seria razoável para as forças norte-americanas e aliadas presumir que, como uma nação tecnologicamente inferior, provida de uma força aérea e marinha obsoletas, a RPDC fosse conduzir ataques semelhantes.

Além disso, a RPDC parece ter demonstrado essa capacidade. Entre 2014 e 2016, a RPDC, ao que consta, efetuou o *hacking* de "mais de 140 mil computadores" pertencentes ao governo e a empresas na RC, tentando, ainda, atacar a rede de controle de seu sistema de transporte[29]. Os ataques, provavelmente executados pelo Bureau 121, capacitaram a RPDC a acessar e monitorar as comunicações do governo e empresas da RC.

Se isso tivesse ocorrido durante uma invasão, a RPDC talvez houvesse desligado todos os 140 mil computadores, cessando as comunicações dessas organizações. Talvez fosse capaz de paralisar ou gerar o caos na rede de transporte da RC.

Se ampliados em alcance e agressividade, esses ataques poderiam interromper as capacidades de comunicação e compartilhamento de informações da RC com suas Forças Armadas. Paralelamente à destruição de sistemas físicos de comunicação da RC pelas F Op Esp, a RPDC poderia incapacitar as comunicações da RC e dos EUA, deixando as tropas no campo de batalha às cegas. O corte de comunicações nos estágios iniciais da guerra enfraqueceria a capacidade da RC e dos EUA para coordenar meios de artilharia e aéreos, concedendo às forças da RPDC tempo e espaço para sobrepujar as tropas sul-coreanas e norte-americanas na zona desmilitarizada.

Embora ataques contra as comunicações e redes essenciais sul-coreanas fossem dificultar os esforços da RC e dos EUA, meios alternativos de comunicação talvez ainda permitissem que as duas nações respondessem à agressão da RPDC. Contudo, vitais meios de comunicação secundários poderiam ser neutralizados mediante um ataque à rede elétrica sul-coreana, potencialmente anulando as vantagens da RC e dos EUA sobre as forças da RPDC ao retardar uma oportuna resposta coordenada à agressão. Há alguns anos, tal ataque

Alunos operam computadores na Escola Revolucionária de Mangyongdae, em Pyongyang, Coreia do Norte, 13 Abr 13. A escola é administrada pelas Forças Armadas, e seus gestores afirmam que ela foi originalmente estabelecida em 1947 para crianças que haviam perdido os pais durante a luta da Coreia por sua libertação da ocupação japonesa. (Foto da Associated Press)

teria sido considerado impossível para uma nação tão atrasada tecnologicamente como a RPDC. Atualmente, é quase certo que ela execute um ataque como esse no caso de guerra.

Por exemplo, em dezembro de 2015, *hackers* russos provocaram uma interrupção de energia na Ucrânia por meio de um ataque cibernético. Instalaram *malware* na rede de usinas elétricas da Ucrânia e controlaram os disjuntores remotamente para cortar a eletricidade de mais de 225 mil pessoas[30]. Em seguida, a Rússia inundou a central de atendimento da companhia elétrica ucraniana com chamadas falsas para impedir que a empresa recebesse ligações de seus verdadeiros clientes[31]. Considerando o grau de sofisticação que as unidades cibernéticas da RPDC parecem ter alcançado e o relacionamento que ela mantém com a Rússia, é provável que tenha recebido apoio russo para potencialmente conduzir ataques semelhantes contra as usinas elétricas da RC.

Em essência, os ataques cibernéticos seriam uma abordagem assimétrica para compensar o fato de que a força aérea da RPDC é praticamente inexistente. Eles poderiam infligir danos táticos e operacionais à RC para reforçar os bombardeios de "choque e pavor" que provavelmente precederiam uma intervenção militar. Ao destruir infraestruturas críticas de comunicações, transporte e apoio, a RPDC provocaria confusão e desordem, que ajudariam suas tropas de infantaria convencionais a sobrepujar as forças da RC e dos EUA.

Não obstante, ainda que esses métodos pudessem ser eficazes, é improvável que o Bureau 121 fosse capaz de deixar a rede da RC completamente fora de operação, embora uma pequena interrupção pudesse prejudicar gravemente as ações da RC e dos EUA no campo de batalha. Para neutralizar, totalmente, a superioridade tecnológica da RC e dos EUA, a RPDC precisaria empregar ataques cibernéticos mais sofisticados contra sistemas de GPS, radar e apoio logístico e sistemas de

visada de armas. O modo exato pelo qual a RPDC conduziria esses ataques foge ao âmbito desta discussão. Entretanto, essa ameaça deve ser levada a sério, como adverte o Defense Science Board (Conselho Científico de Defesa): "[C]aso os EUA se vejam em um conflito em larga escala contra um adversário com poder de combate equivalente [...] as armas, mísseis e bombas norte-americanos podem não funcionar ou podem ser dirigidos contra nossas próprias tropas. O ressuprimento, incluindo alimentos, água, munição e combustível, pode não chegar quando ou onde necessário"[32].

O *hacking* ou retirada de radares e GPS de operação mesmo que apenas por alguns dias até que as forças da RC e dos EUA pudessem se reorganizar, poderia manter em terra o poder aéreo, conferindo liberdade de manobra às tropas da RPDC no campo de batalha. Além disso, a interferência com o GPS não só impediria o uso de sistemas de armas guiadas com esse recurso, mas, o que é mais perigoso, também poderia fazer com que as armas disparassem com as coordenadas incorretas. O *hacking* de satélites norte-americanos, que a China, ao que consta, já demonstrou ser capaz de realizar, poderia cegar a Inteligência da RC e dos EUA aos movimentos da RPDC no terreno[33].

Se a RPDC invadisse as redes logísticas automatizadas que apoiassem as forças da RC e dos EUA na península, essas forças teriam dificuldade em manter capacidades de combate. O rastreamento, requisição e entrega de aprovisionamentos essenciais de guerra poderiam ser abalados por um simples ataque distribuído de negação de serviço que paralisasse sistemas ou corrompesse dados, fazendo com que suprimentos logísticos fossem enviados incorretamente. Os militares da RC e dos EUA poderiam ver-se rapidamente sem os recursos necessários para combater.

Portanto, a RPDC poderia empregar ataques cibernéticos para garantir que sua superioridade numérica e enorme volume de poder de fogo pudessem triunfar apesar da inferioridade de seus materiais bélicos. Quando aliado à guerra eletrônica e à atuação das F Op Esp atrás das linhas de combate, isso faria — de modo coerente com os ideais descritos em *Unrestricted Warfare* — com que as forças da RC e dos EUA perdessem a impulsão e mantivessem uma postura defensiva e reativa.

O documento *Unrestricted Warfare* descreve a regra da "proporção áurea" e a regra "colateral-principal". A ideia é de que a proporção áurea — 0,618 ou aproximadamente dois terços—, normalmente aplicada à arte, arquitetura e matemática, pode ser aplicada à guerra. Os autores indicam que, depois de ter sido reduzido pela Força Aérea dos EUA para 0,618 de seu efetivo original, o Exército iraquiano entrou em colapso e a guerra teve fim[34]. A regra colateral-principal é, em essência, a ideia de que a guerra pode ser vencida por meio de ações de não guerra. Quando essas duas teorias são consideradas em conjunto, fica evidente que, embora possam não se considerar capazes de derrotar os EUA pelo combate convencional, os chineses provavelmente creem poder derrotá-los se ações de não guerra fossem utilizadas para reduzir o efetivo das Forças Armadas norte-americanas para cerca de dois terços de seu poder de combate.

Para a China, há muitas opções para concretizar essa possibilidade, pois ela vem aumentando os recursos de que pode valer-se para conduzir ações de não guerra por períodos prolongados, sejam elas cibernéticas, financeiras ou políticas. Para a RPDC, com seu objetivo de *kukka mokp'yo* e seus recursos extremamente limitados, há menos opções. A RPDC provavelmente aplicaria a regra da proporção áurea e a regra colateral-principal reduzindo as forças da RC e dos EUA em um terço por meio de ataques cibernéticos, aliados a vários outros meios assimétricos. Caso os sistemas dos EUA e da RC fossem tirados de operação ou corrompidos, as capacidades de combate dos dois países ficariam reduzidas ou prejudicadas a ponto de, teoricamente, possibilitar que o Exército da RPDC iniciasse uma invasão terrestre maciça. Portanto, o ataque cibernético é um meio pelo qual a RPDC provavelmente atingiria os sistemas de apoio ao combate inimigos, o que proporcionaria às suas Forças Armadas numericamente superiores o espaço, o tempo e a liberdade de manobra para sustentar o combate na península.

Um ataque cibernético poderia incluir um pulso eletromagnético por detonação nuclear que desativaria dispositivos eletrônicos em um raio de 450 milhas (cerca de 725 km)[35]. A RPDC poderia, teoricamente, realizar isso por meio da detonação de um dispositivo nuclear na atmosfera a uma altitude de 30 milhas (cerca de 48 km). Esse ataque poderia neutralizar as vantagens tecnológicas de forças amigas na península, inutilizando equipamentos dotados de um componente eletrônico. Entretanto, considerando a ameaça

de retaliação nuclear e a maior probabilidade de apoio norte-americano a uma guerra prolongada, que muito provavelmente resultaria na derrota da RPDC, essa opção tende a permanecer como último recurso antes de um ataque nuclear tático.

Soluções para Neutralizar as Capacidades Cibernéticas Norte-Coreanas

A liderança norte-coreana acredita, provavelmente, que a RPDC poderia reverter o equilíbrio de poder tático para o que existia nos anos 50, empregando suas capacidades cibernéticas para ganhar uma vantagem. Em junho de 1950, as forças terrestres táticas dos EUA foram derrotadas de forma constrangedora por um inimigo em condições de superioridade numérica, mas menos adestrado, menos equipado e considerado menos preparado para a guerra. Ao continuarem a retirar suas unidades de combate permanentes da RC e reassumirem um papel de apoio, deixando suas forças na península despreparadas para organizar uma defesa em grande escala, os EUA deverão tomar medidas para evitar enfrentar uma situação semelhante à de 1950.

As capacidades cibernéticas da RPDC têm suas vulnerabilidades. Em 2014, em represália pelo *hacking* da Sony, os EUA conduziram um ataque distribuído de negação de serviço contra a RPDC que tirou a *kwangmyong* do ar[36]. Entretanto, esse ataque não visou as unidades cibernéticas, baseadas, predominantemente, na China; em vez disso, interrompeu o funcionamento da intranet. Esse fato destaca uma importante vulnerabilidade da RPDC no caso de uma guerra em larga escala. A operabilidade cibernética da RPDC estaria, provavelmente, à mercê do governo chinês. Se o governo chinês chegasse à conclusão de que continuar a apoiar a RPDC fosse algo politicamente insustentável, a capacidade cibernética norte-coreana poderia tornar-se insignificante.

Para mitigar o risco de ameaças cibernéticas da RPDC, os meios do Exército dos EUA devem estabelecer parcerias ativas com as forças da RC e reavaliar o modo pelo qual enxergam operações cibernéticas. Como medida preventiva, seus meios cibernéticos devem monitorar as redes norte-americanas dentro da RC e as redes de unidades prestes a serem enviadas para aquele país, devido à maior probabilidade de que sejam visadas pelos meios da RPDC. Em vez de neutralizarem, ativamente, as ameaças cibernéticas identificadas da RPDC, os comandantes precisam avaliar as vantagens obtidas em termos de Inteligência ao concederem uma limitada liberdade de ação aos adversários, a fim de estudarem suas táticas, técnicas e procedimentos no domínio cibernético.

Os comandantes deveriam começar a estudar as operações cibernéticas como um multiplicador de força de uma perspectiva ofensiva e defensiva, e não como uma disciplina fora do domínio tático ou operacional. Além disso, as tropas do Exército estacionadas na RC devem criar planos de contingência junto às forças sul-coreanas antevendo ataques cibernéticos da RPDC semelhantes aos descritos neste artigo, e devem se adestrar em ambientes caracterizados pelo emprego da guerra cibernética. Dessa forma, as forças dos EUA e da Coreia do Sul poderão mitigar a significativa ameaça representada pelas forças cibernéticas da Coreia do Norte. ■

Referências

1. Jason Andress e Steve Winterfield, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (Waltham, MA: Syngress, 2013), p. 73. Andress e Winterfield citam Jung Kwon Ho, "Mecca for North Korean Hackers", Daily NK online, 13 Jul. 2009.

2. Clyde Stanhope, "How Bad is the North Korean Cyber Threat", Hackread website, 20 Jul. 2016, acesso em 2 mai. 2017, https://www.hackread.com/how-bad-is-the-north-korean-cyber-threat/; Office of the Secretary of Defense (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, acesso em 4 mai. 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, MD: Naval Institute Press, 2005), p. 68.

4. Ibid.

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 Feb. 2013, acesso em 6 mai. 2017, http://archive.defense.

gov/pubs/Report_to_Congress_on_Military_and_Security_Developments_Involving_the_DPRK.pdf.

6. Daniel Wagner e Michael Doyle, "Scenarios for Conflict Between the Koreas", Huffington Post, 25 Feb. 2012, acesso em 2 mai. 2017, http://www.huffingtonpost.com/daniel-wagner/scenarios-for-conflict-be_b_1169871.html.

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

8. Ibid., p. 73.

9. Ibid., p. 73–74.

10. Ibid.; Blaine Harden, "North Korea Massively Increases Its Special Forces", *Washington Post* website, 9 Oct. 2009, acesso em 3 mai. 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], August 2015), acesso em 4 mai. 2017, http://uskoreainstitute.org/wp-content/uploads/2016/02/NKNF_Nuclear-Weapons-Strategy_Bermudez.pdf.

12. Ibid.

13. Ibid.

14. James M. Broder e Douglas Jehl, "Iraqi Army: World's 5th Largest but Full of Vital Weaknesses", Los Angeles Times online, 13 Aug. 1990, acesso em 8 mai. 2017, http://articles.latimes.com/1990-08-13/news/mn-465_1_iraqi-army.

15. Richard A. Clarke e Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), p. 28–29; Qiao Liang e Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, resumo traduzido (Panama City, Panama: Pan American Publishing, 2002). [Há uma versão em português intitulada "A guerra além dos limites: conjecturas sobre a guerra e a tática na era da globalização", tradutor desconhecido, disponível em https://www.egn.mar.mil.br/arquivos/cepe/GUERRAALEMLIMITES.pdf — N. do T.]

16. Clarke e Knake, *Cyber War*, p. 30–32.

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

18. Andrew Scobell e John M. Sanford, *North Korea's Military Threat: Pyongyang's Conventional Forces, Weapons of Mass Destruction, and Ballistic Missiles* (Carlisle, PA: Strategic Studies Institute, 2007), p. 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, August 2014, HP Enterprise Community website, acesso em 6 mai. 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", Infosec Island website, 11 Jun. 2012, acesso em 14 fev. 2017, http://www.infosecisland.com/blogview/21577-Concerns-Mount-over-North-Korean-Cyber-Warfare-Capabilities.html.

21. "North Korea Launched Cyber Attacks, Says South", *The Guardian* website, 11 Jul. 2009, acesso em 4 mai. 2017, https://www.theguardian.com/world/2009/jul/11/south-korea-blames-north-korea-cyber-attacks.

22. Ju-min Park e James Pearson, "In North Korea, Hackers are a Handpicked, Pampered Elite", Reuters website, 5 Dec. 2014, acesso em 6 mai. 2017, http://www.reuters.com/article/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205; Darren Pauli, "NORKS Hacker Corps Reaches 5,900 Sworn Cyber Soldiers—Report", The Register website, 7 Jul. 2014, acesso em 6 mai. 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.", *Austin Chronicle* website, 11 March 2013, acesso em 4 mai. 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", *Washington Post* website, 29 Jan. 2013, acesso em 3 mai. 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, no. 1 (Winter 2012): p. 68, acesso em 8 mai. 2017, https://www.usnwc.edu/getattachment/8e-487165-a3ef-4ebc-83ce-0ddd7898e16a/The-Republic-of-Korea-s--Counter-asymmetric-Strateg.aspx.

27. Uma outra perspectiva sobre a guerra cibernética norte-coreana consta de Kim, "The Republic of Korea's Counter--Asymmetric Strategy", p. 58.

28. John Markoff, "Before the Gunfire, Cyberattacks", *New York Times* website, 12 Aug. 2008, acesso em 3 mai 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", Reuters website, 13 Jun. 2016, acesso em 14 fev. 2017, http://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0YZ0BE.

30. Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage", Reuters website, 25 Feb. 2016, acesso em 14 fev. 2017, http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K.

31. Ibid.

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, January 2013), p. 5, acesso em 3 mai. 2017, http://www.dtic.mil/docs/citations/ADA569975.

33. Mary Pat Flaherty, Jason Samenow e Lisa Rein, "Chinese Hack U.S. Weather Systems, Satellite Network", *Washington Post* website, 12 Nov. 2014, acesso em 3 mai. 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 e Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, p. 153–69.

35. Andress e Winterfield, *Cyber Warfare*, p. 147.

36. Cecilia Kang, "North Korean Web Goes Dark Days after Obama Pledges Response to Sony Hack", *Washington Post* website, 22 Dec. 2014, acesso em 3 mai. 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.