Armas Cibernéticas: Igualando Condições no Âmbito Internacional

Ross M. Rustici

Este artigo foi originalmente publicado na revista *Parameters* (*Autumn 2011*).

UMA DAS MAIORES preocupações de segurança para os Estados Unidos da América (EUA) atualmente é como minimizar sua vulnerabilidade às armas cibernéticas. Nos últimos 20 anos, as ameaças nesse campo evoluíram, passando de *hackers* solitários, motivados pela recompensa financeira e prestígio, para o crime organizado e atores estatais. Sua sofisticação e capacidades crescem em proporção direta ao grau de conectividade da sociedade. Apesar do contínuo desenvolvimento das ameaças cibernéticas, relativamente pouca atenção é dada a determinar como elas irão afetar o combate e o sistema internacional.

A maior parte da bibliografia atual sobre a guerra cibernética a considera, na melhor das hipóteses, como um multiplicador de força. Muitos estudiosos desconsideram seus efeitos como um vetor de ataque independente. Como explicação, citam diversos exemplos, que vão desde as respostas dos EUA no caso de Pearl Harbor e dos ataques de 11 de Setembro até a incapacidade do bombardeio estratégico para subjugar a população civil na Inglaterra e na Alemanha durante a Segunda Guerra Mundial, não fossem as operações militares combinadas. Essas perspectivas estão corretas no sentido de que operações cibernéticas ofensivas serão, de modo geral, inúteis, caso não estejam acompanhadas do poder convencional.

Entretanto, tal abordagem analítica presume que as armas cibernéticas serão utilizadas em um primeiro ataque. As capacidades de ataque de longo alcance da guerra cibernética podem ser extremamente efetivas, quando empregadas como arma contra a coerção. Em essência, uma forte capacidade cibernética constitui uma força dissuasória, que minimizará, em grande parte, a interferência externa em assuntos internos e regionais.

A inexistência de casos confirmados de um ataque cibernético de larga escala sancionado por um Estado obriga os analistas a explorar diferentes sistemas de armas e teorias para ajudar o combatente e o político a entenderem como as armas cibernéticas podem ser utilizadas e que vulnerabilidades são geradas por essa nova categoria. Considerando as características singulares do ciberespaço e das armas cibernéticas, nenhuma tecnologia ou teoria existente será capaz de proporcionar um entendimento adequado. No entanto, é possível obter uma compreensão aproximada das capacidades das armas cibernéticas utilizando os princípios tanto da teoria de poder aéreo estratégico quanto das discussões iniciais sobre a doutrina e dissuasão nuclear.

O conceito de poder aéreo estratégico se transformou, no decorrer do século passado, em um dos princípios centrais da guerra moderna[1]. Os estrategistas entendem suas limitações quando se trata de vencer uma guerra de proporções existenciais, mas o consideram extremamente útil em conflitos de curta duração entre partes desiguais. A superioridade aérea necessária para uma campanha aérea estratégica custaria trilhões de dólares e demandaria uma vasta rede de bases para aeródromos e portos no exterior, que pudessem comportar grupos de batalha de navios-aeródromos. Esse nível de investimento está além das possibilidades da maioria dos Estados. Assim, as armas cibernéticas têm o potencial para se

Ross Rustici é Analista de Pesquisa contratado, que trabalhou junto ao Instituto de Estudos de Segurança Nacional da Universidade de Defesa Nacional, nos Estados Unidos da América. É especialista em relações estratégicas sino-estadunidenses e no Exército de Libertação Popular da China, incluindo suas operações marítimas, dimensionamento da força e transparência da defesa.

tornarem uma força equalizadora, por exigirem uma fração do investimento, mas serem capazes de cumprir a maioria das mesmas missões de um ataque aéreo estratégico.

Além disso, a teoria nuclear se deparou, inicialmente, com muitos dos mesmos problemas que enfrentamos hoje, ao buscarmos entender as armas cibernéticas. Apesar de os EUA e a União Soviética terem chegado à mesma conclusão sobre a verdadeira utilidade das armas nucleares na guerra, foram necessárias duas décadas para tanto. Embora as armas cibernéticas talvez provem ser assustadoras o suficiente para levar a uma nova forma de destruição mútua assegurada (MAD, na sigla em inglês)[2], é bem mais provável que o pensamento inicial, quanto a disparos de demonstração e uma defesa barata se encaixando em uma retaliação maciça, seja mais perspicaz.

Da mesma forma que a revolução industrial ocasionou uma mudança fundamental no combate, a era da informação vem introduzindo uma alternativa nova e econômica para a defesa estratégica. As capacidades de guerra cibernética hoje podem dar conta da maioria das tarefas estratégicas que, no passado, exigiam a supremacia aérea. Segundo analistas estadunidenses, tudo — do sistema de saúde à rede elétrica — constitui um alvo viável para um ataque cibernético[3]. Uma análise superficial dos objetivos de recentes campanhas aéreas estadunidenses demonstra em que medida a infraestrutura civil é visada em uma campanha de bombardeio estratégico. No mundo interconectado da atualidade, tanto a infraestrutura civil quanto as instalações militares estão ficando cada vez mais sujeitas a paralisações provocadas por ataques cibernéticos[4]. Em consequência, o futuro do combate e os limites à coerção internacional têm o potencial para mudarem radicalmente.

Brasão oficial do Comando Cibernético dos Estados Unidos da América.

Este artigo examina como as armas cibernéticas apresentam novos riscos para as sociedades conectadas, explora seu possível impacto sobre os EUA e as implicações dessas novas capacidades e conclui com uma breve discussão das possíveis limitações e problemas relacionados à utilização de armas cibernéticas para a dissuasão. Ele não tem como objetivo apresentar uma análise definitiva nem propor alguma política específica. Visa a ser um primeiro passo para se pensar sobre o emprego de armas cibernéticas na política de defesa de outros países e suas ramificações para a liberdade de ação estadunidense.

Ameaças Cibernéticas Emergentes

Para entender as verdadeiras possibilidades dessas armas, é preciso, primeiro, traçar a distinção entre a Exploração de Redes de Computadores (ERC) e o Ataque a Redes de Computadores (ARC). O ARC consiste em prejudicar, negar, degradar ou destruir redes de computadores, as informações nelas contidas ou os sistemas por elas controlados. A ERC é, essencialmente, uma atividade de busca de Inteligência. A tentativa de conduzir uma ERC pode, eventualmente, até levar a um erro que resulte em prejuízo, negação, degradação ou destruição, mas casos intencionais de ARC são extremamente raros. Apesar de os EUA e o resto do mundo sofrerem milhões de tentativas de ERC todos os dias, existem poucos casos evidentes de um ARC significativo. Ainda que haja guerras de *hackers* quase diariamente, a desfiguração de *sites* dificilmente se qualificaria como um ARC no mesmo patamar de violência sancionada por um Estado. Os incidentes mais divulgados de um ARC significativo — quiçá os únicos casos suspeitos de terem apoio estatal — ocorreram na Estônia, na Geórgia e no Irã. Devido à escassez de estudos de casos reais, os estudiosos do tema são obrigados a analisar o que é tecnicamente viável e a postular a partir disso. Embora o número de casos de ERC

Departamento de Defesa, Cherie Cullen

O então Secretário de Defesa Robert M. Gates profere discurso durante a cerimônia de inauguração do Comando Cibernético dos EUA no Forte Meade, Estado de Maryland, 21 Mai 10.

registrados venha crescendo de modo exponencial, com alvos cada vez mais sigilosos e níveis inéditos de exploração, as capacidades de ARC são, de modo geral, desconhecidas e não comprovadas.

Extrapolando com base nas capacidades de ERC e na escassa documentação existente sobre ARC e armas cibernéticas, sabemos que atores avançados estão aptos a desativar redes elétricas, paralisar sistemas ferroviários, afetar bolsas de valores, danificar estações de tratamento de água, abrir barragens e suspender o funcionamento de refinarias de petróleo[5]. Em sociedades tão conectadas como as dos EUA e da Europa, a maior parte da infraestrutura crítica civil — se não toda ela — está vulnerável a ataques cibernéticos. Considerando a velocidade e a precisão com as quais um ataque cibernético pode ser executado, essas armas podem ser utilizadas para quaisquer fins: desde um disparo de advertência contra um adversário durante uma crise até um ataque catastrófico, que possa custar trilhões de dólares e um sem-número de vidas a um Estado. Sua ampla gama de aplicações lhes confere um caráter único, e o fato de que um arsenal cibernético também é extremamente econômico significa que hoje há uma capacidade destrutiva inédita disponível aos Estados pobres ou fracos.

A capacidade de atacar rapidamente, sem aviso e em tão larga escala faz com que essas armas sejam especialmente assustadoras. Uma campanha cibernética bem executada, aliada a um cuidadoso trabalho de relações públicas, tem o potencial para traumatizar uma sociedade de uma maneira não vista desde Nagasaki[6]. Embora as armas cibernéticas não criem o mesmo espetáculo visual que um míssil nuclear ou até mesmo convencional, os meios pelos quais elas são lançadas fazem com que sejam, intrinsecamente, uma ferramenta de guerra psicológica. Ao contrário de armas convencionais e nucleares, não há aviso prévio para um ataque cibernético iminente. O fato de que uma sociedade não tenha como se fortalecer contra um ataque, devido à sua imprevisibilidade, aumenta a efetividade das armas cibernéticas. Não saber qual será o ataque seguinte ou quando ele irá acontecer exerce um

Um sargento observa um marinheiro ajustar um cabo da rede do Comando de Operações de Defesa Cibernética da Marinha dos EUA.

profundo impacto sobre a vítima, tornando as armas cibernéticas diferentes de todos os possíveis sistemas de coerção.

No entanto, um "Pearl Harbor" cibernético faria pouco sentido para a maior parte do mundo. Mesmo com essas vulnerabilidades flagrantes, a incapacidade convencional dos ataques cibernéticos de explorar uma população confusa e desorganizada provavelmente geraria apoio para o governo e não a sua capitulação. Os acontecimentos na Estônia e na Geórgia ilustram esse fenômeno.

Na Estônia, a comunidade de *hackers* russos paralisou os meios de comunicação, algumas operações bancárias e *sites* do governo durante alguns dias, em retaliação à decisão do governo estoniano de retirar de Tallinn um monumento às Forças Armadas soviéticas. Entretanto, como não houve uma intervenção militar correspondente para tirar proveito dos efeitos da campanha cibernética, o impacto foi, de modo geral, financeiro e de curto prazo[7]. O Estado não recolocou a estátua no local original e, em decorrência dos ataques, a Estônia ficou supostamente mais segura, em virtude de um maior envolvimento e papel de liderança junto à Organização do Tratado do Atlântico Norte (OTAN).

A Guerra da Geórgia é uma outra história, porém. Os ataques cibernéticos foram coordenados com uma operação militar russa, servindo como multiplicadores do poder de combate. Embora os ataques, em si, não tenham tido ramificações duradouras, pode-se afirmar que a demonstração de força devolveu a Geórgia à esfera de influência da Rússia. Em ambos os casos, os *hackers* russos exibiram incrível comedimento na seleção de alvos. A infraestrutura crítica não foi visada em nenhum deles, e os danos de longo prazo foram insignificantes[8]. Ainda que os alvos selecionados tenham sido de valor relativamente baixo, o impacto psicológico e econômico foi considerável.

Considerando o reduzido número de incidentes de guerra cibernética, os analistas são obrigados a especular sobre o emprego e os efeitos de ataques mais amplos e direcionados. Qual seria a reação da população estadunidense às privações causadas por um ataque cibernético estratégico, executado em resposta a uma intervenção do país no exterior? Embora não haja dados confiáveis sobre como os EUA reagiriam a sérias adversidades, provocadas por um conflito, algumas conclusões provisórias podem ser extraídas da forma pela qual a opinião pública moldou o emprego da força nas últimas duas décadas. Os resultados mostram que a aversão do público estadunidense a baixas está diretamente relacionada a duas percepções. Primeiro, é preciso que ele acredite que os interesses em jogo são importantes. Segundo, precisa crer que há uma excelente perspectiva de sucesso. Caso uma dessas duas condições não seja satisfeita, a tolerância a baixas e o apoio à ação militar diminuirão rapidamente[9]. Essa tendência foi observada na campanha no Kosovo. O governo Clinton insistiu em não enviar forças terrestres, em função, principalmente, da reação política adversa vivida após o conflito na Somália. Enquanto eficaz, a campanha exclusivamente aérea demonstra a que extremos os EUA estão dispostos a chegar para evitar baixas.

Essa reduzida tolerância a baixas no exterior[10] deveria corresponder a uma postura ainda mais avessa a riscos no caso de ameaças à população civil no território nacional. Com efeito, segundo relatos de casos, quando há uma catástrofe em âmbito interno, as democracias costumam retirar seu apoio para missões não essenciais no exterior. Um exemplo recente foi a saída da Espanha do Afeganistão. Muitos consideram os ataques terroristas aos trens em Madri como sendo o fator catalisador que ajudou o Partido Socialista dos Trabalhadores a assumir o controle do governo,

resultando na retirada das tropas espanholas do Afeganistão. Pesquisas de opinião realizadas naquele país mostram que o público em geral nunca considerou a Guerra contra o Terrorismo conduzida pelos EUA como algo importante para segurança nacional espanhola[11]. Além disso, as explosões em Madri mostraram que, apesar de três anos de guerra, a probabilidade de alguma forma demonstrável de êxito continuava sendo baixa. Esse caso ilustra o fato de que as populações civis são mais avessas ao risco quando há maior probabilidade de que os custos as afetem diretamente[12].

A justificativa para a Operação *Enduring Freedom* apoia ainda mais esse conceito de proteção do território nacional contra quaisquer riscos. O principal argumento em prol da guerra contra o Iraque era o programa de armas de destruição em massa de Saddam Hussein. Segundo a lógica utilizada, seria preciso invadir aquele país para desarmá-lo e impedir um possível ataque contra os EUA ou seus aliados. A posição oficial contava com o apoio da opinião pública, segundo pesquisas: ainda em maio de 2003, mais de 70% dos habitantes dos EUA seguiam acreditando que a guerra era justificada[13]. Historicamente, o povo estadunidense apoiou políticas intervencionistas justificadas como proteção de seu modo de vida.

A discussão anterior indica quais serão as restrições de política externa a serem enfrentadas pelos EUA no século XXI. Capacidades cibernéticas podem ser utilizadas para provocar grandes perdas econômicas e até mortes. As explosões nos trens de Madri, que alteraram tão radicalmente o rumo da política externa espanhola, poderiam ser reproduzidas com um ataque cibernético. Existe hoje um potencial inédito para um inimigo cibernético avançado gerar o caos em território estadunidense. Desde a Guerra de 1812 que não há um possível adversário que tenha a capacidade de atacar o território continental dos EUA sem representar uma ameaça existencial. As capacidades cibernéticas são de baixo custo, eficazes e podem ser utilizadas a partir de qualquer ponto no mundo, a qualquer momento. A guerra cibernética provavelmente representará um novo paradigma de força, que reduzirá os casos de conflito entre Estados e as intervenções humanitárias armadas, devido aos maiores custos de transação.

Segurança Hegemônica

Desde o final da Segunda Guerra Mundial, a postura estadunidense de defesa global tem sido, predominantemente, a de mantenedor do equilíbrio de poder no exterior. Na visão mais simplista possível, os EUA passaram a Guerra Fria e as décadas subsequentes tentando preservar o equilíbrio em diferentes regiões e impedir que alguma coalizão obtivesse um nível desproporcional de poder. Esse esforço incluiu desde o conflito ativo na Coreia, Vietnã e Iraque até atividades de apoio no Oriente Médio, África e Sudeste Asiático. Desde a Segunda Guerra Mundial, os EUA não combatem em um conflito ou apoiam uma política externa intervencionista em locais onde seus adversários possuam a capacidade militar para afetar gravemente o país. Com efeito, desde a Guerra Hispano-Americana que os EUA não combatem uma força militar com alcance mundial e bases suficientemente próximas de seu território. Os EUA não enfrentam uma força invasora desde a Guerra de 1812. Esse incrível isolamento em relação a conflitos vem diminuindo rapidamente com o avanço da tecnologia. Embora o país tenha tido a capacidade de atuar no âmbito internacional com impunidade — devido, em grande parte, a fatores geográficos —, esse não é mais o caso. As capacidades cibernéticas possibilitam que pequenos Estados, providos de diminutos orçamentos de defesa, estejam aptos, pela primeira vez na história, a infligir graves danos a um inimigo bem mais forte, a grandes distâncias.

Para ser claro, as armas cibernéticas apenas aumentam o custo do conflito para os adversários. É improvável que essas armas afetem a política de segurança nacional quando houver interesses essenciais em jogo. Com exceção dos EUA e do Reino Unido, não há nenhum país com uma capacidade comprovada de projeção de poder em âmbito mundial, apto a tirar proveito da situação criada por um ataque cibernético efetivo fora de seu entorno. Assim, ataques cibernéticos contra uma infraestrutura crítica tornam-se, primordialmente, uma arma defensiva. Essas capacidades podem oferecer considerável segurança a um regime, a uma fração do custo de programa de armas nucleares. Embora seu valor dissuasório talvez seja menor que o de armas nucleares transportadas por mísseis balísticos intercontinentais, um ataque cibernético tem o potencial para infligir danos

suficientes para prevenir uma política externa intervencionista. O custo para que os EUA atuem como um agente de equilíbrio no exterior ou uma força policial mundial aumentará drasticamente. Isso provavelmente diminuirá a tolerância do público estadunidense às ramificações de uma intervenção, a não ser em circunstâncias mais extremas.

Implicações

Cabe ressaltar a importância do equilíbrio assimétrico convencional de forças entre os EUA e o resto do mundo, que é um dos fatores determinantes fundamentais desta análise. Conforme discutido em seções anteriores, as capacidades cibernéticas assemelham-se, de modo geral, às repercussões das campanhas de bombardeio estratégico dos EUA. Armas cibernéticas dirigidas contra infraestrutura crítica terão a capacidade de retribuir o resultado de ataques aéreos tradicionais de um modo nunca experimentado antes pelos EUA. É assim que essas armas podem restringir o emprego de força estadunidense no exterior.

O surgimento de armas cibernéticas eficientes tem três possíveis implicações. A primeira é uma redução da coerção interestatal. Decorrente dela, a segunda é o impacto adverso no projeto de segurança humana, conforme proposto por defensores da "Responsabilidade de Proteger". Por fim, as armas cibernéticas apresentam a possibilidade de alterar radicalmente as estruturas de força convencionais.

O impacto mais provável das armas cibernéticas será uma redução drástica do emprego de violência sancionada entre Estados. De modo semelhante a forças convencionais eficientes e de grande porte, as armas cibernéticas representam um forte dissuasor para um agressor em potencial. As armas cibernéticas são uma forma econômica de desenvolver uma capacidade de ataque em âmbito mundial contra Estados conectados. Embora os Estados Unidos talvez sejam o único Estado fora do Oriente Médio capaz de lançar bombas em Bagdá, em breve, qualquer país com uma conexão em rede poderá estar em condições de paralisar a capital de um país. Em decorrência dessa capacidade, políticas externas intervencionistas se tornarão excessivamente caras, não apenas em termos de recursos e vidas de forças armadas, mas no setor civil também. Os novos perigos gerados por esse quinto domínio do combate significam que apenas as questões mais fundamentais de segurança nacional valerão o risco de possíveis ataques retaliatórios.

Isso leva a uma séria reconsideração dos conceitos de segurança mundial e de projeto de segurança humana, causando, ao mesmo tempo, uma retração do clássico sistema westfaliano, centrado nos Estados. Se o Iraque ou a Iugoslávia houvessem contado com capacidades cibernéticas avançadas, a probabilidade de ataques aéreos contra instituições estatais teria sido drasticamente reduzida. O custo da intervenção cresce com a capacidade de um Estado-alvo lançar um bem-sucedido ataque cibernético estratégico. Quantos Estados estarão dispostos a prevenir crises humanitárias, caso tal esforço implique uma redução de 5% a 7% do seu produto interno bruto (PIB)[14], além dos gastos necessários para executar a ação militar? Além disso, ao contrário de hipotéticos primeiros ataques com armas convencionais ou nucleares, o caráter flexível e desenraizado do ciberespaço faz com que seja impossível ter um determinado nível de confiabilidade quanto à efetividade de um ataque. Diferentemente dos outros quatro domínios, é impossível ver uma arma cibernética ser neutralizada no ciberespaço. Nem medidas ofensivas nem defensivas poderão aliviar os altos custos de transação com algum grau de certeza.

Por fim, as armas cibernéticas são capazes de reduzir tremendamente a necessidade de uma vasta força aérea global. Isso é especialmente verdade no caso de potências emergentes ou das que enfrentam a necessidade de modernizar sua frota. Embora a superioridade aérea continue a ser necessária para uma invasão e — ao menos no futuro próximo — para operações convencionais, sua utilidade como arma estratégica está diminuindo rapidamente. As armas cibernéticas apresentam diversas vantagens em relação a ataques aéreos. A primeira e mais convincente diz respeito ao custo. As armas cibernéticas representam uma fração do custo de mísseis e não exigem plataformas de lançamento complicadas e caras. Qualquer indivíduo que disponha de um *laptop* pode lançar um ataque cibernético, ao passo que bombardeiros invisíveis custam bilhões de dólares. Além do fator custo, o caráter

temporário dos ataques cibernéticos faz com que eles sejam bem mais interessantes, quando se contempla a reconstrução pós-guerra. Se um combatente fosse capaz de desativar uma rede elétrica por quatro dias para, em seguida, reativá-la imediatamente, isso sairia muito mais barato (e tornaria os esforços de reconstrução mais fáceis) que bombardear uma usina elétrica e reconstruí-la. Além disso, embora possa haver repercussões dentro das próprias redes, os ataques cibernéticos eliminam quase toda a probabilidade de danos colaterais.

Essas implicações significam que o futuro do combate e os limites à coerção internacional devem mudar radicalmente. A dissuasão cibernética é capaz de reduzir os incidentes de violência no sistema internacional. Entretanto, é provável, também, que ela transforme o mundo em um lugar mais seguro para regimes corruptos e abusivos. O valor dissuasório das armas cibernéticas não se equipara ao das armas nucleares, mas elas têm o potencial para se tornarem uma força dissuasória maior que os sistemas convencionais. Seu valor dissuasório talvez não importe entre adversários que estejam disputando um interesse nacional central, mas terá um peso muito maior quando houver interesses secundários em jogo. As capacidades cibernéticas têm o potencial de aumentar o custo da guerra a ponto de fazer com que os EUA (ou qualquer sociedade avançada) fiquem bem menos dispostos a empregar força no exterior com base em ideais ou em uma percepção de fraco equilíbrio de poder regional.

Problemas para a Dissuasão

Existem, porém, problemas flagrantes quanto à dissuasão no ciberespaço. Ao contrário das armas nucleares ou de qualquer capacidade convencional, é quase impossível demonstrar o poder cibernético. Além disso, é muito fácil desenvolver essa capacidade com um espaço mínimo. O caráter técnico das armas cibernéticas requer que já exista um problema em um *software* específico ou que se tenha a capacidade de assumir a identidade de um usuário de confiança, para executar um ataque. No ciberespaço, qualquer tipo de ataque leva à criação — em uma questão de dias ou, no máximo, meses — de

Força Aérea dos EUA, Raymond McCoy

Cadetes da Academia da Força Aérea participam do exercício de defesa cibernética da Agência de Segurança Nacional, em 17 Abr 12.

uma defesa quase perfeita contra sua reutilização. Ao contrário dos sistemas convencionais, armas cibernéticas dependem de vulnerabilidades provocadas pelo homem. Elas não exercem uma força destrutiva física. Seriam mais como a água que corra por uma represa mal construída. A água só poderá passar se houver rachaduras. Da mesma forma, as armas cibernéticas só poderão penetrar as defesas de uma rede se houver falhas passíveis de serem exploradas. Um ataque distribuído de negação de serviço (*Distributed Denial of Service — DDoS*), como os conduzidos contra a Estônia e a Geórgia, é comparável ao transbordamento de água por cima de uma barragem. Se os que o estiverem sofrendo interromperem o fluxo de atividades na internet, o DDoS será bloqueado. Uma vez executado, é possível impedir que as máquinas utilizadas para conduzir o ataque acessem a internet novamente. Isso significa que qualquer ataque, mesmo os conduzidos para fins de demonstração, acaba sendo um sistema de armas irreproduzível. Assim, a dissuasão cibernética é obrigada a apoiar-se quase que totalmente em um estranho jogo de cabra cega.

Os EUA não têm condições de saber se um adversário potencial dispõe de capacidades cibernéticas para provocar graves danos à infraestrutura crítica ou de determinar em que ponto ele irá utilizá-las. Com a proliferação desse tipo de arma, ficará cada vez mais perigoso para os EUA tentarem moldar ativamente o ambiente internacional por meios coercitivos. Além disso, os formuladores de política estadunidenses não terão uma indicação clara quando à dimensão da ameaça representada por outros países.

Existem, porém, alguns indicadores gerais sobre o possível grau de avanço de um ataque. Por exemplo, operações de Inteligência e programas simples são frequentemente utilizados para a obtenção de informações sobre a interação de redes. O mapeamento da rede elétrica visada e de outros elementos da infraestrutura crítica é extremamente útil, mas desnecessário para um bem-sucedido ataque cibernético. O *worm Stuxnet* demonstrou que, contanto que tenha a capacidade de testar uma arma cibernética contra um sistema de composição semelhante ao alvo, um Estado poderá ter bastante sucesso. Assim, seria possível construir uma arma cibernética cujo único rastro fosse a documentação de compra de sistemas de controle comerciais.

Marinha dos EUA, Sgt Jennifer R. Hudson

Um sargento opera a conexão de internet via satélite a bordo do navio de assalto anfíbio USS Bonhomme Richard *(*LHD 6*), 20 Jul 08.*

Como a maior parte da tecnologia necessária para o desenvolvimento de armas cibernéticas sofisticadas está disponível comercialmente e não está sujeita a regulamentação, é impossível criar e implantar regimes tradicionais de controle de tecnologia e armas. Isso torna quase impossível rastrear o desenvolvimento de armas cibernéticas. Com efeito, o único modo de estimar, atualmente, as capacidades cibernéticas de outro ator é medir a frequência e a sofisticação de ataques oriundos de um Estado[15].

A relativa facilidade com que Estados — ou até mesmo indivíduos — podem desenvolver essas capacidades é suficiente para dar o que pensar aos especialistas em segurança[16]. Quando aliada a uma incapacidade geral de avaliá-las com precisão, é quase certo que os Estados Unidos, ou quaisquer outras grandes potências militares convencionais, julgarão mal o oponente e pagarão caro pelo erro. Uma vez que o mundo atravesse esse "Rubicão" particular, não haverá mais volta.

Conclusão

As doutrinas militares estratégicas descritas anteriormente podem fornecer um roteiro de desenvolvimento concreto para o emprego de armas cibernéticas. Dada a semelhança entre o poder aéreo e o poder cibernético no que diz respeito à seleção de alvos, é fácil apontar analogias e acolher a doutrina de poder aéreo estratégico como princípio orientador para os primeiros estágios de desenvolvimento das armas cibernéticas. Nesse mesmo sentido, os debates iniciais sobre armas e dissuasão nucleares são relevantes à forma como a guerra cibernética é vista atualmente. Apesar da existência de pontos em comum, o caráter singular das armas cibernéticas faz com que a aplicação de teorias existentes seja uma proposta perigosa, que dificulta nossa compreensão sobre como tais armas podem ser e serão utilizadas. Elas têm a capacidade de mudar as relações internacionais de maneira sem precedentes. A dissuasão cibernética é, de fato, uma defesa de baixo custo. Um orçamento de defesa de centenas de milhões de dólares pode ser suficiente para gerar uma dissuasão efetiva contra um da ordem de centenas de bilhões de dólares. Além disso, não existe, atualmente, uma regra internacional contra a aquisição ou o emprego dessas armas.

Por fim, não se deve subestimar o impacto psicológico particular das armas cibernéticas. A incapacidade de uma sociedade para se fortalecer contra um ataque aumenta muito o dano que este pode lhe causar. A convergência desses fatores gera uma situação em que é relativamente fácil adquirir armas de dissuasão, a um preço acessível, no sistema internacional existente. Com isso, aumenta a probabilidade de que as ações internacionais por países poderosos fiquem mais restritas. Sem uma defesa cibernética eficaz, o poder militar ofensivo será uma forma menos confiável de induzir mudanças. As sociedades conectadas serão bem mais cautelosas ao propor alguma intervenção humanitária, uma mudança de regime, o estabelecimento de zonas de exclusão aérea e outras operações de segurança não essenciais. Quando houver interesses fundamentais em jogo, é improvável que o potencial dano físico e psicológico constitua um dissuasor forte o suficiente para prevenir um conflito. O alto custo associado ao conflito provavelmente fará com que os atores envolvidos ajam com extrema cautela e esgotem todas as alternativas antes que ele se torne uma opção viável.

Caso as armas cibernéticas evoluam dentro desses moldes, os EUA e outros Estados avançados perderão algumas vantagens importantes. Diferentemente das armas nucleares e da Guerra Fria, nenhum país será capaz de desenvolver poder ofensivo suficiente para dissuadir possíveis adversários do emprego de armas cibernéticas em ataques retaliatórios. O próprio caráter da dissuasão cibernética, conforme descrito anteriormente, vem sendo impulsionado por uma grande inferioridade em capacidades convencionais. O desenvolvimento de capacidade ofensiva adicional só aumentará a probabilidade de que um Estado pequeno recorra a ataques desproporcionais mais cedo em uma crise, em vez de ser dissuadido. Além disso, no caso da eclosão de um conflito, não haverá qualquer esperança de uma dissuasão cibernética mútua. Ao contrário do limiar nuclear, as mesmas vulnerabilidades que permitem que a dissuasão cibernética funcione temporariamente são os objetivos prioritários de campanhas aéreas. Uma vez que um ataque aéreo incapacite ou danifique a infraestrutura crítica, não há nada que impeça o Estado atacado de lançar uma retaliação cibernética.

Isso deixa os EUA e demais países avançados com considerações difíceis a serem feitas na formulação de políticas. Embora não sejam mutuamente excludentes, nenhuma das alternativas apresentadas a seguir constitui uma solução satisfatória. Primeiro, os Estados que dependam de redes podem, em uma tentativa de criar defesas adequadas, recorrer a rígidos controles, passando a monitorar todos os dados transferidos em uma escala ainda maior que a atualmente vista na maioria dos regimes repressores. Segundo, os Estados podem adotar uma estratégia exclusivamente de contraforça, o que permitiria que eles conduzissem operações militares, mas restringiria suas ações a ataques contra equipamentos militares. Embora isso fosse reduzir muito a capacidade de um Estado para combater efetivamente, também ajudaria a criar um tabu contra ataques à infraestrutura civil. Ajudaria, também, a minimizar a vulnerabilidade às armas cibernéticas dos Estados conectados, continuando a permitir-lhes, porém, certa liberdade para intervir no ambiente internacional.

A última opção é simplesmente aceitar que o custo da guerra aumentou. Nenhuma dessas opções é interessante para um país que queira maximizar sua flexibilidade para lidar com os acontecimentos em âmbito mundial. Não obstante, as armas cibernéticas — se desenvolvidas nos moldes descritos anteriormente — forçarão os Estados a buscar, em variados graus, todas as alternativas enumeradas.

Embora seja cedo demais para determinar se qualquer uma dessas tendências potenciais se tornará realidade, essas questões merecem uma análise mais detalhada. É bastante provável que o valor das armas cibernéticas ficará entre o de um ataque nuclear estratégico e o das forças convencionais avançadas otimizadas pela Força Aérea dos EUA. Embora os teóricos de segurança tenham o hábito de dizer que algum novo sistema de armas é algo transformador, esse potencial realmente existe, no caso das armas cibernéticas. Elas têm a capacidade latente para introduzir uma nova ordem internacional, apoiada em uma garantia de destruição mútua baseada em *bytes*. No entanto, como no caso de todos os sistemas anteriores, os terríveis efeitos sobre a ordem mundial só serão compreendidos depois que forem empregados e que o mundo possa ver seus efeitos em primeira mão. A próxima década será fundamental para o desenvolvimento de armas cibernéticas e seu emprego pelos diversos Estados. Enquanto nós, como nação e parte da comunidade global, não compreendermos totalmente a aplicação das armas cibernéticas no sistema mundial, não seremos capazes de formular uma política efetiva.***MR***

REFERÊNCIAS

1. Uma discussão da evolução do poder aéreo estratégico consta de CONVERSINO, Mark J. "The Changed Nature of Strategic Air Attack" *Parameters* 27, no. 4 (Winter 1997-98): p. 28-41.

2. Em um recente depoimento ao Congresso, o General Alexander afirmou que algum tipo de dissuasão baseada em vulnerabilidades mútuas talvez já exista entre as nações mais poderosas.

3. Uma discussão mais aprofundada dos alvos já afetados consta do relatório de McAfee "In the Crossfire: Critical Infrastructure in the Age of Cyberwar", disponível em: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, acesso em: 17 abr. 2011; LYNN III, William J. "Defending a New Domain" *Foreign Affairs*, p. 89:5; Gershwin, Lawrence. Statement for the Record to the Joint Economic Committee on Cyber Threat Trends and US Network Security, 21 Jun. 2001, disponível em: http://www.dni.gov/nic/testimony_cyberthreat.html, acesso em: 17 abr. 2011.

4. CLARKE, Richard A. *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010). Além disso, o Secretário Panetta, em um depoimento perante o Comitê de Inteligência da Câmara de Deputados dos EUA, ressaltou, recentemente, que ataques cibernéticos têm o potencial para paralisar o país.

5. Essa lista tem fins de ilustração apenas. Tudo o que for controlado ao menos em parte por um computador está vulnerável a armas cibernéticas. Os sistemas com acesso à internet são alvos mais fáceis. Contudo o caso do *worm Stuxnet* mostra que até sistemas isolados (*air-gapped*) são vulneráveis.

6. Uma campanha cibernética hipotética poderia desenrolar-se da seguinte forma: 1) colisões em pleno voo de aviões de companhias aéreas do setor privado, aliadas a descarrilamentos dos trens da empresa ferroviária estatal estadunidense e dos metrôs; 2) interrupções do serviço de telefonia celular; 3) ruptura de gaseodutos, paralisação de refinarias de petróleo e abertura de represas por meio das válvulas de descarga de emergência; 4) lançamento de ataque cibernético por um Estado que anuncie sua responsabilidade; 5) corte da rede elétrica nacional. A consequente perda de vidas e recursos financeiros e a sensação de estar sendo vitimado têm o potencial para destruir a vontade de um Estado para prosseguir com uma ação ofensiva.

7. ASHMORE, William C. "Impact of Alleged Russian Cyber Attacks", *Baltic Security & Defence Review*, Volume 11, 2009.

8. No caso da Estônia, os principais alvos foram os *sites* do governo, dos maiores meios de comunicação e de bancos. A modalidade principal de ataque foi o DDoS. No caso da Geórgia, os principais alvos foram os *sites* do governo e de meios de comunicação. A infraestrutura crítica (como os sistemas de Controle de Supervisão e Aquisição de Dados — SCADA que controlam o oleoduto Baku–Tbilisi–Ceyhan) permaneceu intacta. Parece que a finalidade principal dos ataques cibernéticos foi a guerra psicológica.

9. LARSON, Eric V.; SAVYCH, Bogdan. "American Public Support for U.S. Military Operations from Mogadishu to Baghdad" (Santa Monica, CA: RAND Corporation, 2005), p. 219.

10. A conexão entre baixas no exterior e privações em âmbito nacional é acentuada pela transição para uma força militar totalmente voluntária. A inexistência do serviço obrigatório transfere o ônus do serviço militar da sociedade em geral para segmentos das minorias. O fato de que ela ainda reage de modo tão negativo à morte de militares estadunidenses apesar de estar isolada, em grande parte, dos custos, demonstra a séria aversão dos EUA a baixas.

11. Pesquisa conduzida na Europa pelo Instituto Gallup International após a guerra no Iraque, em 2003: na opinião de 63% dos respondentes, as ações militares no Iraque e no Afeganistão tornaram o mundo mais perigoso.

12. Cabe ressaltar o paradigma de ação-reação quando se considera o caso da Espanha. Ao contrário dos ataques de 11 de Setembro, a população espanhola enxergou os ataques em Madri como resultado direto de seu papel no Afeganistão, levando à suspensão das atividades de combate. O fato de a população ligar a política externa à ocorrência de uma catástrofe dentro do país demonstra uma aversão geral a riscos. No caso dos atentados de 11 de Setembro, os estadunidenses se viram como vítimas de um ataque não provocado. Essa distinção na relação entre causa e efeito é fundamental para se compreender como uma democracia reagirá a um ataque cibernético de larga escala.

13. MILBANK, Dana; VANDEHEI, Jim. "No Political Fallout for Bus on Weapons", *The Washington Post*, 17 May 2003, disponível em: http://www.washingtonpost.com/ac2/wp-dyn/A1155-2003May16, acesso em: 2 abr. 2011.

14. Estimativas baseadas na apresentação de Scott Borg durante o 19º Simpósio Anual de Segurança USENIX, intitulado "How Cyber Attacks Will Be Used in International Conflicts" ("Como os ataques cibernéticos serão empregados em conflitos internacionais", em tradução livre).

15. Esse método é rudimentar e, com frequência, bastante duvidoso, considerando que o máximo que a ciência forense pode fazer, em geral, é rastrear um ataque até um computador específico. Isso não fornece informação alguma sobre o usuário do computador. O fato de um ataque ser oriundo de um país não prova, de maneira confiável, que o governo esteja envolvido. Assim, é possível sobrestimar ou subestimar a capacidade real de um Estado com base nesse indicador bastante simples.

16. Uma pesquisa rápida na internet resulta em inúmeras reportagens detalhadas sobre ataques por regimes perigosos com capacidades avançadas, *hackers* adolescentes que utilizam métodos relativamente rudimentares para adquirir o controle de infraestrutura crítica e esquemas de extorsão cibernética que afetam as redes elétricas e as refinarias de petróleo. Um recente teste da segurança de TI de uma estação de tratamento de água mostrou vulnerabilidades fatais e facilmente exploráveis. Os ataques contra infraestrutura crítica e sistemas governamentais estão ocorrendo com uma frequência preocupante. A única razão para que nós não tenhamos ainda assistido a um grande incidente cibernético talvez seja a capacidade limitada de *hackers* mal financiados para executar suas atividades, por motivos intelectuais ou monetários. Com base nesses incidentes, não é um grande salto projetar o que um Estado bem organizado e provido de recursos seria capaz de fazer.