"Treino de Sombra": A Guerra Cibernética e o Ataque Econômico Estratégico

Segundo-Tenente Soren Olson, Força Aérea dos EUA

Este artigo foi originalmente publicado na revista *JFQ* (Issue 66, 3rd Quarter 2012).

Ataca a estratégia do adversário na raiz. Depois, rompe suas alianças. Em seguida, ataca seu exército. A pior política consiste em atacar as cidades.

—Sun Tzu, *A Arte da Guerra*

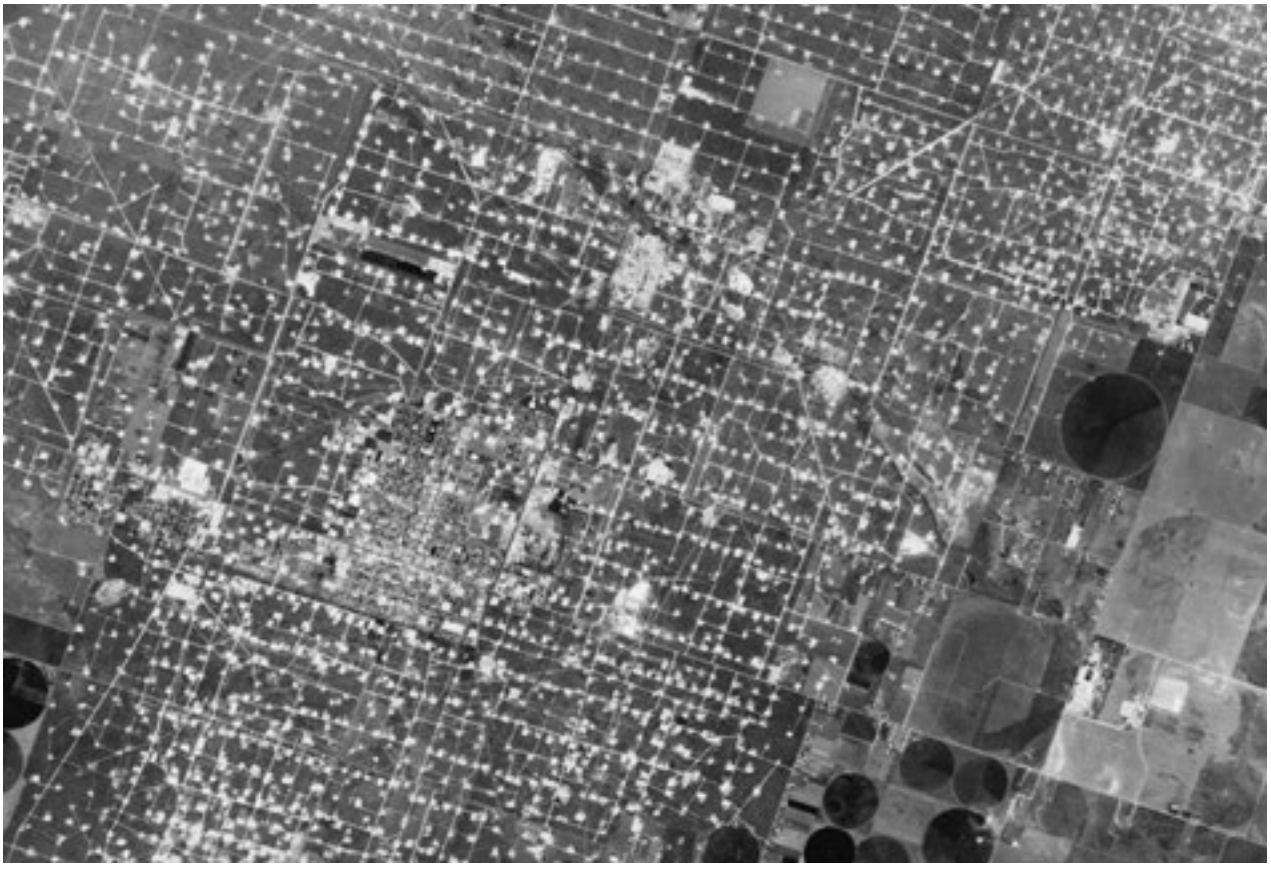
A INFRAESTRUTURA E OS recursos essenciais dos Estados Unidos da América (EUA) estão sujeitos a ataques cibernéticos "inteligentes e persistentes". Esses ataques poderiam afetar drasticamente a cadeia de suprimento de nosso recurso mais estratégico: o petróleo. Durante duas décadas, alertas sobre as vulnerabilidades cibernéticas inerentes à infraestrutura estadunidense foram efetivamente ignorados. Estruturas burocráticas, como o Comando Cibernético dos EUA (USCYBERCOM), criam a ilusão de segurança, mas não tratam do verdadeiro problema. Enquanto nos concentramos em produzir efeitos no inimigo, ignoramos, de modo geral, os efeitos que ele pode nos causar. Nossa cultura de "modas" estratégicas (ex.: guerra híbrida, de quarta geração ou irregular, contrainsurgência e contraterrorismo) e nossa análise de ameaças centrada em Forças indicam que mudanças no caráter da guerra e suas respectivas implicações podem passar despercebidas. O caráter da guerra hoje inclui, inegavelmente, ataques contra a infraestrutura econômica e nacional, e os métodos cibernéticos serão as armas de preferência.

Como os sistemas de infraestrutura nacional e econômico não estão tão em evidência quanto os sistemas de armas, sua proteção não é devidamente priorizada no planejamento estratégico. Os Departamentos de Defesa e de Segurança Interna e outros órgãos do setor estratégico dos EUA já começaram a responder à ameaça apresentada pela guerra cibernética, mas há mais a ser feito. É preciso que se tomem medidas, ainda que os referidos sistemas sejam operados por civis e estejam fora da tradicional esfera de competência do Departamento de Defesa.

Complicando ainda mais a questão de jurisdição há o programa *Stuxnet*. Ele demonstrou, de maneira conclusiva, que armas cibernéticas desenvolvidas por nações vêm sendo voltadas contra objetivos civis para a obtenção de efeitos estratégicos. Além disso, o fato de que dois dos três maiores efeitos do *Stuxnet* no *software* da Siemens permanecem sem reparo, anos depois do ataque, deixa em dúvida a disposição de empresas privadas em proteger sistemas de infraestrutura crítica[1]. Essas duas observações sugerem que a guerra cibernética não respeitará a alocação tradicional de responsabilidades institucionais. Com efeito, é preciso ponderar se seria imprudente deixar a defesa contra ataques de cunho estratégico — por outros países ou atores — a cargo de empresas privadas e do aparato de segurança interna.

Muitos autores empregam a classificação pré- e pós-11 de Setembro para caracterizar uma

O Segundo-Tenente Soren Olson, da Força Aérea dos EUA, é formado pelo Departamento de Estudos Militares e Estratégicos, da Academia da Força Aérea dos EUA. Participa, atualmente, do adestramento de pilotos na Base Aérea de Columbus.



NASA-JSC

Recursos petrolíferos e hídricos subterrâneos perto de Denver City, no Estado do Texas, formam padrões distintos de uso do solo.

mudança na forma como se vê o terrorismo. Antes de setembro de 2001, ele era, de modo geral, considerado um comportamento criminoso[2]. Depois que seu impacto ficou demonstrado, ele passou a ser uma questão de defesa nacional. Da mesma forma, é preciso discernir dois períodos diferentes quando se considera a segurança cibernética: antes e depois do *Stuxnet*. A tendência de enxergar o emprego de armas cibernéticas como um ato criminoso deve ser substituída pela visão de que seu uso contra quaisquer interesses dos EUA representa um ato hostil.

Evolução de uma Arma

De todos os desafios diante dos estrategistas estadunidenses, o mais traiçoeiro é, provavelmente, a tendência a ignorar vulnerabilidades inerentes à infraestrutura nacional. O excesso de autoconfiança com que as vulnerabilidades cibernéticas são vistas é bem ilustrado pela citação a seguir:

> Os ataques cibernéticos têm um papel potencialmente importante contra adversários despreparados e desafortunados, que sejam sofisticados o bastante para adquirir e tornar-se dependentes de sistemas de informática, mas não o suficiente para defendê-los contra um ataque inteligente e persistente[3].

A infraestrutura dos EUA é dependente de tecnologias cibernéticas[4]. Descartar ou restringir as ameaças cibernéticas a conceitos existentes de guerra nos deixará despreparados e desafortunados.

Muitos asseveram que avanços tecnológicos transformam radicalmente nosso mundo. Da mesma forma, quando se observam novas tecnologias, armas e táticas, muitos estrategistas as designam de Revoluções em Assuntos Militares (RAM). Essas RAM supostamente mudariam a forma de conduzir a guerra[5]. Independentemente da utilidade das RAM como conceito, alguns avanços no combate, como a tecnologia, armas

ou métodos, alteraram, com efeito, o caráter da guerra. A guerra cibernética é um deles.

Transformações no caráter da guerra são sempre visíveis depois do fato — o que não é o caso do desenvolvimento das tecnologias e métodos que lhes servem de base. Muitas vezes, as raízes de mudanças no combate já estão presentes e em evolução durante anos antes de seu primeiro emprego decisivo. O uso de ferrovias, comunicações telegráficas e ataques frontais contra posições fortificadas durante a Guerra Civil prenunciou as operações na Primeira Guerra Mundial[6]. Os alemães testaram a coordenação de elementos terrestres e aéreos durante a Guerra Civil Espanhola, anos antes de empregá-la em larga escala contra os poloneses e franceses na Segunda Guerra Mundial[7]. Da mesma forma, a Guerra do Yom Kippur, em 1973, utilizou o poder aéreo para fixar e devastar formações terrestres — uma técnica que seria utilizada quase 20 anos depois na Operação *Desert Storm*[8]. Em cada um desses exemplos, os anos entre o desenvolvimento inicial e a implantação em larga escala serviram apenas para aumentar a letalidade do produto final. A guerra cibernética foi desenvolvida e testada de forma parecida, e os relatórios advertem constantemente contra o perigo apresentado por esse tipo de combate.

Em 1991, o Conselho Nacional de Pesquisa dos EUA afirmou: "Muitos desastres podem resultar de ataques intencionais contra sistemas, mas seria possível preveni-los, detectá-los ou recuperar-se deles por meio de maior segurança"[9]. O relatório apontou a necessidade de uma estratégia coerente. Seis anos depois, um comitê presidencial constatou que ainda não havia um órgão de coordenação, como havia sido recomendado. Extraordinariamente, ao contrário do relatório de 1991, o comitê afirmou que a natureza das ameaças cibernéticas ainda era mal compreendida[10]. Em 2001, os argumentos sobre os relativos pontos fortes de defesa e ataque nesse novo campo[11] eram tão indecisos que um subcomitê do Congresso recomendou que a segurança cibernética da infraestrutura e redes essenciais dos EUA fosse deixada a cargo da indústria privada[12].

Os partidários dessa ideia devem lembrar-se de que nem sempre se pode contar com o meio empresarial para servir aos interesses nacionais. As empresas privadas são indubitavelmente patrióticas e responsáveis, mas os estrategistas não devem esquecer-se dos nomes de projetos, companhias e indivíduos que são um sinônimo do foco de curto prazo: o Ford Pinto, a Enron, Fannie Mae/Freddie Mac e Bernie Madoff. Os estrategistas tampouco podem ignorar a possibilidade de que uma empresa privada mantenha, intencionalmente, vulnerabilidades cibernéticas a serem exploradas para seus próprios fins ou por ordem de alguma outra potência. À luz dessas preocupações, seria imprudente colocar a defesa nacional a cargo da indústria privada, particularmente quando houver graves consequências em jogo e a capacidade ou disposição de uma companhia em se defender contra armas cibernéticas (como a Siemens, no caso do *Stuxnet*) for duvidosa.

Apesar dos erros passados, não há dúvida de que as capacidades cibernéticas estadunidenses estejam crescendo, particularmente com a recente criação do USCYBERCOM. Entretanto, os apologistas dos atuais esforços de defesa cibernética devem considerar esta avaliação recente pelo tribunal de contas estadunidense (denominado Government Accountability Office):

> O Comando Estratégico dos EUA constatou que o efetivo cibernético do Departamento de Defesa está subdimensionado e despreparado para enfrentar a atual ameaça. (...) Ainda não está claro se essas insuficiências serão resolvidas, uma vez que o Departamento de Defesa não conduziu uma avaliação mais abrangente das lacunas em capacidades cibernéticas nem estabeleceu um plano de implantação ou estratégia de financiamento para solucionar quaisquer discrepâncias que venham a ser identificadas[13].

Vinte anos de desastres, investigações e mudanças de política levaram, repetidas vezes, aos mesmos lamentáveis resultados.

O aprimoramento da guerra cibernética continuou mesmo enquanto se desenrolava essa combinação tragicômica de preocupação e inação.

Em 1999, um funcionário da Defesa afirmou que o FBI estava investigando uns 6.080 ataques diários, registrados nos sistemas computacionais do Departamento de Defesa[14]. Em 2001, pesquisadores da Universidade Dartmouth previram que os ataques cibernéticos seriam a arma assimétrica de preferência para grupos e países hostis por um bom tempo[15]. Em 2003, o jornal *The Guardian* observou que organizações federais estadunidenses estavam sofrendo um número tão grande de ataques cibernéticos a redes essenciais que eles receberam o codinome de *Titan Rain* ("Chuva de Titãs")[16]. A essa altura, o governo federal começou a ponderar se as redes cibernéticas comerciais deveriam ser consideradas parte da infraestrutura crítica e, assim, protegidas, mas tomou poucas medidas significativas. Em 2005, um comitê presidencial constatou que "os computadores que controlam instalações críticas, infraestrutura e serviços essenciais dos EUA podem ser visados, a fim de desencadear falhas em todo o sistema, e são frequentemente acessíveis de praticamente qualquer lugar do mundo pela internet"[17].

Em março de 2009, a revista *Forbes* descreveu um grupo de espionagem cibernética conhecido por *GhostNet*. Acredita-se que ele tenha infiltrado as redes governamentais de 117 países[18]. Tais intrusões demonstram a capacidade de agressores estrangeiros para penetrar redes essenciais protegidas no decorrer de longos períodos. Por fim, foi descoberto, em julho de 2010, o *worm Stuxnet*, exemplo de que a guerra cibernética atingiu a maioridade. Em uma situação em que um ataque militar tradicional seria politicamente impraticável, afirma-se que essa complexa série de "uns" e "zeros" causou graves danos ou até atrasou o programa nuclear iraniano[19].

Apesar de sua capacidade comprovada para produzir efeitos cinéticos, a verdadeira importância da guerra cibernética está em seu emprego estratégico. A guerra cibernética corresponde de modo ideal à ordem de ataque definitiva de Sun

Departamento de Defesa, Cherie Cullen

Ten Brig C. Robert Kehler, Comandante do Comando Estratégico dos EUA.

Tzu ao engajar o inimigo: "Ataca a estratégia do adversário na raiz. Depois, rompe suas alianças. Em seguida, ataca seu exército. A pior política consiste em atacar as cidades. (...)"[20].

...o anonimato da guerra cibernética possibilita ataques coordenados contra os aspectos físicos e cibernéticos da cadeia de suprimento de petróleo dos EUA.

Um adversário que pretenda atacar a estratégia dos EUA deve, primeiro, determinar o que ela busca proteger. A segurança dos recursos energéticos é a prioridade máxima da atual política externa estadunidense, tendo sido gastos trilhões de dólares da Defesa para manter o acesso aos estoques de petróleo do Oriente Médio[21]. É uma ironia cruel que, apesar desse investimento, contínuas vulnerabilidades na cadeia de suprimento de petróleo demonstrem que o compromisso dos EUA para com a defesa de recursos essenciais continua a ser deficiente[22].

A Ameaça ao Petróleo Bruto

Os EUA são o maior consumidor de petróleo do mundo, mas não são capazes de suprir sua demanda com as fontes nacionais. Assim, cerca de 36% do petróleo importado advém de rotas marítimas e outros 27% são transportados para o território continental dos EUA via oleodutos terrestres[23]. Até o petróleo doméstico depende do sistema interno de oleodutos. A capacidade em atacar ou defender essa rede mundial e nacional de suprimento de petróleo se baseia em sistemas computacionais[24]. Os guardiães comerciais de recursos essenciais, como a infraestrutura petrolífera, foram incapazes até de se manter em dia com as vulnerabilidades reveladas nos sistemas de Controle de Supervisão e Aquisição de Dados (SCADA, na sigla em inglês)[25]. Não estão preparados para o violento ataque que, segundo determina a história, será várias ordens de magnitude maior do que qualquer outro ataque cibernético executado anteriormente.

Historicamente, os países que importam energia de fontes propensas a ataques invisíveis não se saem bem. Na Segunda Guerra Mundial, submarinos estadunidenses visaram, propositadamente, as importações de petróleo do Japão[26]. Depois de dois anos de ataques invisíveis, menos de 28% do petróleo transportado chegou até aquele país[27]. Além disso, a "perda de matérias-primas e petróleo e a incapacidade de transportar suprimentos para as linhas de frente estavam no cerne da decrescente capacidade japonesa para manter um efetivo poder de combate"[28]. Diante de um ataque contínuo e coordenado, é quase impossível defender completamente uma rede vasta contra um inimigo invisível.

No caso da guerra cibernética, o verdadeiro perigo está na capacidade que um inimigo tenha para coordenar e empregar diferentes atores contra interesses mundiais e, simultaneamente, atacar a infraestrutura petrolífera dos EUA. No final do século XVI, a Inglaterra utilizou corsários contra a economia espanhola, atacando embarcações carregadas de ouro, oriundas da América Central. Exemplos mais recentes incluem a utilização dos "contras" e dos mujahedins pelos EUA durante a Guerra Fria e o apoio soviético aos guerrilheiros da América Central. Quanto ao emprego de intermediários ou "fantoches", o uso de hackers "patrióticos" pela Rússia contra os sistemas bancário e de comunicações da Geórgia, em 2008, é bastante relevante[29]. Esses exemplos destacam o fato de que grupos independentes podem ser controlados por uma grande potência.

O valor da utilização de "fantoches" na guerra cibernética é que eles complicam ainda mais a possibilidade de atribuir responsabilidade. Uma potência pode identificar e mapear vulnerabilidades e, em seguida, coordenar ataques usando intermediários. Mapeamentos passados de vulnerabilidades de rede e infraestrutura não foram tratados como um ato de guerra. Assim, contanto que a potência hostil utilize "fantoches", haverá poucas medidas diretas que os EUA poderão tomar, ainda que se conheça a fonte de informações que possibilita os ataques.

Atualmente, a disseminação de grupos ligados à Al Qaeda e outras organizações armadas

resulta em mais "fantoches" dispostos a atacar os interesses estadunidenses. Esta é a oportunidade que um Estado-nação coordenador ofereceria a esses grupos:

> Deve ficar claro que a infraestrutura energética dos EUA é sua força vital e, como tal, é uma das mais críticas. Os recursos da indústria de petróleo e gás são, portanto, alvos evidentes para um *jihad* econômico[30].

Piratas somalis já vêm utilizando informações internas de companhias marítimas para se apossarem de embarcações na costa do Chifre da África[31]. Esses grupos piratas se mostram dispostos a agir com base em informações obtidas quanto às vulnerabilidades de companhias marítimas ocidentais. Os danos causados por piratas modernos munidos de informações privilegiadas são relativamente pequenos, se comparados à devastação que um ator estatal anônimo e mal-intencionado poderia gerar com uma campanha coordenada. Entretanto, ataques físicos diretos, reforçados por informações obtidas mediante a guerra cibernética, representam apenas uma parte da ameaça: "A dependência em relação a tecnologias cibernéticas gera a oportunidade para comunicações interrompidas, transações falsas ou enganosas, fraude ou quebra de contratos e pode resultar na perda de serviços ou da confiança das partes interessadas ou no colapso da própria empresa"[32].

Da mesma forma, o anonimato da guerra cibernética[33] possibilita ataques coordenados, à semelhança de submarinos, contra os aspectos físicos e cibernéticos da cadeia de suprimento de petróleo dos EUA. A proliferação de grupos armados ao longo de rotas marítimas talvez permita que um ator anônimo coordene uma campanha de submarinos equivalente contra as conexões físicas da cadeia mundial de suprimento de petróleo. Essa campanha de interrupção no abastecimento do recurso seria facilitada por ataques cibernéticos diretos contra os sistemas SCADA que controlam os centros logísticos do setor petrolífero nos EUA.

Os centros logísticos servem como portas de entrada para o abastecimento regional. São caracterizados por interconexões entre muitos oleodutos e, com frequência, outras modalidades de transporte (como navios-tanque e barcaças; ferrovias, às vezes; e normalmente caminhões-tanques, especialmente os utilizados para o transporte local), que permitem que o recurso passe de um sistema para outro entre municípios, Estados e regiões, em uma progressão entre diferentes centros logísticos[34].

Ao analisar-se a disposição da infraestrutura petrolífera estadunidense, constata-se que a concentração de oleodutos controlados por sistemas SCADA em centros logísticos forma evidentes gargalos internos. Há seis principais centros nos EUA, que são vulneráveis a uma sabotagem cibernética dirigida contra os sistemas SCADA ou contra sua rede elétrica, conforme ficou demonstrado em 2007, quando uma "tempestade de gelo provocou a interrupção de energia no centro de Cushing, Oklahoma, paralisando quatro dutos de petróleo bruto [e] o transporte de cerca de 770 mil barris por dia"[35].

Embora pouco conhecido atualmente, o ataque cibernético estadunidense contra o oleoduto transiberiano, em 1982, utilizou um programa "cavalo de Tróia" para provocar uma explosão equivalente a uma arma de 3 quilotons: "Os EUA conseguiram interromper o suprimento de gás e consideráveis receitas em divisas da União Soviética durante mais de um ano"[36]. Embora esse exemplo demonstre que os efeitos cinéticos da guerra cibernética podem ser terríveis, eles não são necessários para causar danos econômicos desastrosos.

Medo do Medo?

Já houve ataques planejados por Estados-nação contra alvos econômicos, utilizando uma combinação de armas tradicionais e armas cibernéticas. O acréscimo de meios cibernéticos e da seleção de alvos econômicos ao caráter da guerra foi demonstrado pela primeira vez pelos russos:

> Quando a Rússia invadiu a Geórgia, grande parte de suas operações militares concentrou-se em tomar não as áreas habitadas por russos étnicos, e sim os portos e instalações georgianos do setor de petróleo e gás. As instáveis condições no terreno, intensificadas por ataques cibernéticos,

Força Aérea dos EUA, Lou Hernandez

Refinaria de Petróleo de Anacortes, Estado de Washington.

> logo fizeram com que todos os oleodutos georgianos não parecessem confiáveis. Enquanto isso, dois dias depois do início da invasão, o trecho turco do oleoduto Baku-Tbilisi-Ceyhan foi atacado por militantes locais, supostamente por iniciativa deles. Uma consequência desses acontecimentos foi a mudança efetuada pela BP Azerbaijão, que transferiu seu transporte de petróleo para o oleoduto Baku-Novorossiysk, embora isso acarretasse o dobro do custo dos oleodutos georgianos[37].

A guerra cibernética foi empregada para maximizar um alvo puramente econômico. A BP transferiu seus contratos com base em uma impressão. Não foi necessário comprometer fisicamente o oleoduto georgiano. Devido à influência da percepção, a Geórgia sofreu graves prejuízos econômicos, sem que houvesse destruição física de sua infraestrutura.

Dada a facilidade com que danos econômicos podem ser infligidos a um único alvo (nesse caso, um oleoduto), pode-se ver como o sistema mundial no qual os Estados Unidos se apoiam está em risco. Ademais, a proliferação de "fantoches" tornaria fácil para uma potência utilizá-los para coordenar ataques contra as rotas marítimas e os centros logísticos terrestres utilizados para o transporte de petróleo. Seria necessário que apenas alguns desses ataques tivessem sucesso para minar a base do sistema energético internacional e o transporte confiável:

> Em 2007, a produção mundial de petróleo totalizou cerca de 85 milhões de barris por dia. Cerca da metade, ou mais de 43 milhões de barris por dia, foi transportada por navios-tanques em rotas marítimas fixas. O mercado energético internacional depende do transporte confiável. O bloqueio de um

gargalo, ainda que temporariamente, pode levar a um considerável aumento dos custos totais de energia. Além disso, gargalos deixam os navios-tanques vulneráveis ao roubo por piratas, a ataques terroristas e à agitação política na forma de guerras ou hostilidades, assim como a acidentes marítimos[38].

...serão necessários anos para que a defesa ativa de sistemas de infraestrutura se equipare às armas ofensivas modernas.

Um comentarista afirma que os ataques cibernéticos também buscam por "gargalos digitais", como a rede elétrica. Ele explica: "O ciberespaço é um terreno complexo, mas a mesma ideia se aplica: estrangular um ponto vulnerável"[39]. Assim como o combate de submarinos, a guerra cibernética é ideal para fechar gargalos. Essa abordagem foi empregada com sucesso pelos EUA contra os japoneses. Os planejadores precisam considerar a possibilidade de um ataque semelhante contra a cadeia de suprimento de petróleo estadunidense, no mínimo por seu potencial para danos catastróficos. Um incidente que fechasse o Estreito de Malaca, ainda que temporariamente, desviaria 50% do transporte marítimo no mundo, gerando mais dúvidas sobre a confiabilidade do transporte no setor energético. O potencial prejuízo econômico de uma campanha cibernética coordenada por uma grande potência contra gargalos nos sistemas mundiais (ou nacionais) seria incalculável[40].

Teatro de Sombras

Armas cibernéticas, possíveis "fantoches" e vulnerabilidades na cadeia de suprimento: todos esses elementos existem. Resta analisar o que poderia motivar um ator a coordenar tal campanha. Sun Tzu e Carl von Clausewitz indicam o que poderia levar a uma campanha dessas contra os estoques de petróleo estadunidenses. Primeiro, considere-se a assertiva de Clausewitz de que fortificações poderosas impelem o inimigo para outros locais. Mesmo em meio a um declínio econômico, as Forças Armadas dos EUA demonstraram sua capacidade para combater em três conflitos no outro lado do mundo[41]. Esse poder de combate obriga os adversários potenciais a encontrar um ângulo de ataque mais efetivo, como um eixo de suprimento vulnerável, que forneça um recurso estratégico vital. Segundo, a utilização da cibernética contra recursos estratégicos está em conformidade com a máxima de Sun Tzu de derrotar o inimigo sem combater e, quando necessário, vencer primeiro e depois combater. Esses dois conceitos apoiam a ideia de remover um recurso estratégico por meios assimétricos e anônimos. Mesmo não sendo anônimo, o referido ataque de submarinos na Segunda Guerra Mundial, que interditou recursos estratégicos, mostra como a capacidade de um adversário invisível em visar alvos econômicos pode subjugar uma grande potência.

Entretanto, a guerra cibernética prenunciada pelo *Stuxnet* e contemplada neste artigo exigiria recursos em uma escala disponível apenas a atores estatais[42]. Além disso, uma abordagem indireta como essa é claramente contrária à típica estratégia ocidental[43]. Quem empregaria a guerra cibernética contra os interesses estadunidenses? Logicamente, o país que mais provavelmente desafiaria a superpotência reinante seria aquele com a motivação e intenção mais claras.

A ideia de utilizar a guerra cibernética para atingir alvos imprevistos, como os recursos estratégicos, está perfeitamente alinhada com o conceito chinês de guerra conhecido por *shashoujian*[44]: "Uma vez identificados e avaliados, os pontos fortes poderão ser evitados e as fraquezas, visadas para o ataque, utilizando *shashoujian*"[45].

Desde 2004, a China conduziu pelo menos 14 grandes ataques cibernéticos, incluindo *Titan Rain* e *GhostNet*, contra objetivos que incluíram desde a ExxonMobil e a chanceler alemã até redes militares da Índia e do Departamento de Defesa dos EUA[46]. Foram observados sinais do desenvolvimento de armas, e os especialistas chineses propuseram a geração de armas econômicas: "É necessário apenas que nos desabituemos a tratar as gerações, usuários e combinações de armas

como sendo algo fixo, para sermos capazes de tornar algo apodrecido em algo milagroso"[47]. Esses autores oferecem, em seguida, um exemplo do que poderia ser obtido com tal abordagem:

> Em 19 Out 87, navios da Marinha dos EUA atacaram uma plataforma de petróleo iraniana no Golfo Pérsico. Notícias do ocorrido chegaram até a Bolsa de Valores de Nova York, desencadeando, imediatamente, a pior quebra do mercado de ações na história de Wall Street. Esse acontecimento, que ficou conhecido como "Segunda-Feira Negra", provocou a perda de US$ 560 bilhões em valor contábil no mercado de ações estadunidense[48].

Embora essa alegação seja incorreta, sua validade é irrelevante, na medida que em que os chineses acreditam que ela é verdadeira.

Um ataque pelos chineses contra as conexões internacionais da cadeia de suprimento de petróleo estadunidense prejudicaria, reconhecidamente, sua própria economia[49]. Por essa razão, parece improvável que eles as ataquem, salvo como prelúdio de uma guerra em larga escala contra os EUA[50]. Entretanto, a teoria de interdependência econômica não deve ser utilizada como escudo para descartar a possibilidade de um ataque cibernético econômico. Antes da Primeira Guerra Mundial, circulava a teoria de que os países não entrariam em guerra, porque a devastação econômica seria grande demais, mas ela se mostrou incorreta.

Guerra de Sombras

O potencial destrutivo da guerra cibernética nos campos econômico, social e físico exige que os estrategistas lhe confiram o mesmo grau de respeito e estudo que o dedicado às armas nucleares. Defender-se contra ataques cibernéticos é como defender-se contra armas nucleares: os ataques podem tomar praticamente qualquer forma e originar-se de qualquer lugar, e as defesas passivas podem ser sobrepujadas mediante um lançamento em massa ou não convencional. Ao contrário das armas nucleares, o caráter anônimo e difuso da guerra cibernética pode impossibilitar a dissuasão.

Algo que complica ainda mais a possibilidade de sucesso na defesa é a proliferação de potenciais "fantoches", que possam ser manipulados de maneira invisível por meios cibernéticos. Quando isso se alia ao êxito de repetidas infiltrações do inimigo (*Titan Rain*), ao alcance mundial das infiltrações (*GhostNet*) e aos efeitos cinéticos (*Stuxnet*), não se pode esperar que defesa alguma resista a um ataque cibernético coordenado. A guerra cibernética está bem desenvolvida, e serão necessários anos para que a defesa ativa de sistemas de infraestrutura se equipare às armas ofensivas modernas. A defesa ativa não deve ser o foco primário. Em vez disso, deve-se priorizar a condução da defesa passiva, a avaliação de vulnerabilidades, a criação de sistemas de *backup*, a identificação das capacidades cibernéticas dos adversários e a solução do problema de atribuição de responsabilidade por um ataque.

O problema de jurisdição sobre a defesa cibernética e o dilema enfrentado pelo Departamento de Defesa dos EUA (que tem a responsabilidade pela defesa nacional, mas está sujeito a uma proibição contra operações no âmbito interno) não são questões que possam ser solucionadas por estrategistas. Essas complicações só poderão ser resolvidas mediante a legislação nacional, uma vez que foram geradas por ela. Entretanto, essa incapacidade de corrigir de imediato um problema não deve impedir que os estrategistas considerem as incômodas implicações de uma infraestrutura que seja indefensável contra armas cibernéticas modernas e que possa não ser confiável no caso de conflitos limitados ou no espectro completo.

É preciso reconhecer que, embora haja consideráveis vulnerabilidades entre as conexões na cadeia de suprimento de petróleo dos EUA, elas são apenas os sintomas de um problema maior. Há anos que se ouvem advertências sobre a guerra cibernética, mas — evocando outra grande falha da defesa antes do 11 de Setembro — as medidas tomadas continuam a ser insuficientes. À luz desses fatos, enfrentamos a incômoda verdade de que a China, assim como outros países, possui uma arma, e nossa melhor defesa contra ela consiste em lutar com sua sombra.***MR***

REFERÊNCIAS

1. ROBERTS, Paul. "Many Stuxnet Vulnerabilities Still Unpatched", *Threatpost.com*, Kaspersky Lab Security News Service, 8 Jun. 2011.

2. BIDDLE, Stephen D. *American Grand Strategy after 9/11: An Assessment* (Carlisle, PA: U.S. Army War College Strategic Studies Institute, 2003), p. 25.

3. LIBICKI, Martin C. "Cyberwar as a Confidence Game", *Strategic Studies Quarterly* 5, no. 1 (Spring 2011), p. 134.

4. *Cyberspace Policy Review* (Washington, DC: The White House, May 2009), p. 3, disponível em: <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

5. KREPINEVICH JR., Andrew F. *The Military-Technical Revolution: A Preliminary Assessment* (Washington, DC: Center for Strategic and Budgetary Assessments, 2002, from Office of Net Assessment, 1992), p. 3, disponível em: <www.csbaonline.org/wp-content/uploads/2011/03/2002.10.02Military-Technical-Revolution.pdf>.

6. GRIFFITH, Paddy. *Battle Tactics of the Civil War* (New Haven, CT: Yale University Press, 1989), p. 20.

7. WAELDE, Rainer. *The Experience of the Japanese-Chinese War and of the Spanish Civil War for the Development of the German "Blitzkrieg Doctrine" and Its Lessons for the Transformation Process* (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2003), p. 25, disponível em: <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA419865&Location=U2&doc=GetTRDoc. pdf>.

8. BAXTER, Steven. "Arab-Israeli War October 1973: Lessons Remembered, Lessons Forgotten" (Master's thesis, Naval War College, 1994), disponível em: <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA279557&Location=U2&doc=GetTRDoc.pdf >.

9. National Research Council, *Computers at Risk: Safe Computing in the Information Age* (Washington, DC: National Academies Press, 1991), p. 2–3.

10. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington, DC: The White House, October 1997), p. 78, disponível em: <www.fas.org/sgp/library/pccip.pdf>.

11. Professionals for Cyber Defense, letter to President George W. Bush, 27 Feb. 2002, disponível em: <www.uspcd.org/letter.html>.

12. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges for Developing National Capabilities*, report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, Apr. 2001, disponível em: <www. gao.gov/new.items/d01323.pdf>.

13. Government Accountability Office, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, report to Congressional Requesters, Jul. 2011, disponível em: <www.gao.gov/new.items/d1175.pdf>.

14. "Guarding Cyber Pentagon", *CNN.com*, disponível em: <http://articles.cnn.com/1999-03-05/ tech/9903_05_pentagon.hackers_1_pentagoncomputers-computer-attacks-computer-hackers?_s=PM:TECH>.

15. VATIS, Michael. *Cyber Attacks During the War on Terrorism: A Predictive Analysis* (Dartmouth, NH: Institute for Security Technology Studies, 24 Sept. 2001), disponível em: <www. dtic.mil/cgi-bin/GetTRDoc?AD=ADA395300>.

16. NORTON-TAYLOR, Richard. "Titan Rain: How Chinese Hackers Targeted Whitehall", *The Guardian*, 4 Sept. 2007, disponível em: <www.guardian.co.uk/technology/2007/sep/04/news.internet>.

17. President's Information Technology Advisory Committee, *Cyber Security: A Crisis of Prioritization* (Arlington, VA: National Coordination Office for Information Technology Research and Development, February 2005), p. 17, disponível em: <www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.>

18. MAIDMENT, Paul. "GhostNet in the Machine", *Forbes.com*, 29 Mar. 2009, disponível em: <www.forbes.com/2009/03/29/ghostnetcomputer-security-internet-technology-ghostnet. html>.

19. BROAD, William J.; MARKOFF, John; SANGER, David E. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", *The New York Times*, 15 Jan. 2011.

20. TZU, Sun. *The Art of War*, trans. Samuel B. Griffith, ed. (Oxford: Oxford University Press, 1973), p. 77–78. [Neste artigo, utilizou-se a tradução de Sueli Barros Cassal (Porto Alegre: L&PM, 2011) — N. do T.]

21. YERGIN, Daniel. "Ensuring Energy Security", *Foreign Affairs* 85, no. 2 (March–April 2006), p. 82.

22. MEAD, Walter Russell. "The Serpent and the Dove", in *Special Providence: American Foreign Policy and How It Changed the World* (New York: Routledge, 2002), p. 110.

23. U.S. Energy Information Administration, "How Dependent Are We on Foreign Oil?" *Energy in Brief* (Washington, DC: Department of Energy, 24 Jun. 2011), disponível em: <www.eia.doe.gov/energy_in_brief/foreign_oil_dependence.cfm>.

24. LINDQVIST, Ulf. "Securing Control Systems in the Oil and Gas Infrastructure", *Oil & Gas Processing Review* (London: Touch Briefings, 2005), disponível em: <www.touchbriefings.com/pdf/1713/ACF1A57.pdf>.

25. ROBERTS.

26. Navy Department, *Section III: Japanese Anti-Submarine Warfare and Weapons*, War Damage Report, no. 58 (Washington, DC: U.S. Hydrographic Office, 1 Jan. 1949), p. 8, disponível em: <www.ibiblio.org/hyperwar/USN/rep/WDR/ WDR58/WDR58-3.html>.

27. HOLMES, W.J. *Undersea Victory: The Influence of Submarine Operations on the War in the Pacific* (Garden City, NY: Doubleday, 1966), p. 425.

28. POIRIER, Michel T. "Results of the American Pacific Submarine Campaign of World War II", U.S. Navy, 30 Dec. 1999, disponível em: <www.navy.mil/navydata/cno/n87/history/paccampaign.html#N_19>.

29. HOLLIS, David. "Cyberwar Case Study: Georgia 2008", *Small Wars Journal*, 6 Jan. 2011, p. 2, disponível em: <http://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf>.

30. FOREST, James J.F. *Homeland Security: Protecting America's Targets, Vol. III: Critical Infrastructure* (Westport, CT: Greenwood Publishing Group, 2006), p.136.

31. TREMLETT, Giles. "This Is London—The Capital of Somali Pirates' Secret Intelligence Operation", *The Guardian*, 11 May 2009, disponível em: <www.guardian.co.uk/world/2009/may/11/somalia-pirates-network>.

32. National Petroleum Council, *Securing Oil and Natural Gas Infrastructures in the New Economy* (Washington, DC: Department of Energy, June 2001).

33. U.S. Naval Institute and CACI International, Inc., "Cyber Threats to National Security: Symposium I—Countering Challenges to the Global Supply Chain", 2 Mar. 2010, disponível em: <http://asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf>.

34. Allegro Energy Group, "How Pipelines Make the Oil Market Work: Their Networks, Operation and Regulation", a memorandum for the Association of Oil Pipelines and American Petroleum Institute's Pipeline Committee, 1 Dec. 2001, p. 7.

35. "Ice Storm Trips Power, Paralyzes Key U.S. Oil Hub", *Reuters*, 11 Dec. 2007, disponível em: <www.cnbc.com/id/22200736/Ice_Storm_Trips_Power_Paralyzes_Key_US_Oil_Hub>.

36. BYRES, Eric J. "Cyber Security and the Pipeline Control System", *Pipeline & Gas Journal* 236, no. 2 (February 2009), disponível em: <http://pipelineandgasjournal.com/cyber-security-and-pipeline-control-system>.

37. U.S. Cyber Consequences Unit (US-CCU), special report, *Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008*, disponível em: <www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-CyberCampaign-Overview.pdf>.

38. Energy Information Agency, *World Oil Transit Chokepoints* (1 Jan. 2008), 1, disponível em: <www.eia.gov/cabs/world_oil_transit_chokepoints/Full.html>.

39. BAY, Austin. "Grab the Planet By the Throat", *RealClearPolitics* (22 Apr. 2009), p. 8, disponível em: <www.realclearpolitics.com/articles/2009/04/22/grab_the_planet_by_the_throat_96106.html>.

40. Energy Information Agency, p. 4.

41. Referência ao Iraque, Afeganistão e Líbia.

42 STARK, Holger. "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War", *Der Spiegel Online*, 8 Aug. 2011, disponível em: <www. spiegel.de/international/world/0,1518,778912-2,00. html>.

43. MURAWIEC, Laurent. "China's Grand Strategy Is to Make War While Avoiding a Battle", *Armed Forces Journal* 143 (Nov. 2005), disponível em: <www.armedforcesjournal. com/2005/11/1164221/>.

44. Geralmente vertido para o inglês como "Assassin's Mace" ("Bastão do Assassino"), refere-se à busca chinesa por armas que sejam indetectáveis antes do emprego e que provoquem danos de tal dimensão que venham a impossibilitar uma retaliação pela vítima.

45. BRUZDZINSKI, Jason E. "Demystifying Shashoujian", in *Civil-Military Change in China: Elites, Institutes, and Ideas after the 16th Party Congress*, ed. Larry Wortzel and Andrew Scobell (Carlisle, PA: U.S. Army War College, Strategic Studies Institute, 2004), disponível em: <www.mitre. org/work/best_papers/04/bruzdzinski_demystify/bruzdzinski_demystify.pdf>.

46. STIENNON, Richard. "A Brief History of Chinese Cyberspying", *Forbes.com*, 2 Feb. 2011, disponível em: <www.forbes.com/sites/firewall/2011/02/11/a-brief-history-of-chinesecyberspying/>.

47. LIANG, Qiao; XIANGSUI, Wang. *Unrestricted Warfare: China's Master Plan to Destroy America* (Beijing: PLA Literature and Arts Publishing House, February 1999), p. 20.

48. Ibid., p. 190.

49. A menos que o ataque afetasse apenas a rede nacional de distribuição de petróleo dos EUA.

50. Os países que exportam petróleo ou têm pouca participação no sistema internacional (Irã, Venezuela, Rússia e Coreia do Norte) poderiam executar campanhas contra todas as conexões da cadeia de suprimento sem se prejudicarem muito. Com efeito, a instabilidade resultante no mercado de petróleo poderia ser economicamente vantajosa para esses atores.