Considerações para as Operações Cibernéticas Ofensivas

CC Kallie D. Fink, Marinha dos EUA;
CC John D. Jordan, CFN dos EUA; e
Maj James E. Wells, Força Aérea dos EUA

A Capitão de Corveta Kallie D. Fink, da Marinha dos EUA, é oficial de guerra de informação no Comando de Operações de Informações da Marinha, Maryland. Concluiu o bacharelado em Alemão pela University of Minnesota e o mestrado em Inteligência Estratégica pela National Intelligence University. Serviu, anteriormente, como secretária executiva adjunta do Subcomandante de Operações Navais para o Domínio das Informações (N2/N6).

O Capitão de Corveta John D. Jordan, do Corpo de Fuzileiros Navais dos EUA, integra a Divisão de Desenvolvimento da Força Conjunta, Estado-Maior Conjunto, como analista de pesquisa de operações em projetos cibernéticos. Concluiu o bacharelado em Engenharia Aeroespacial pela University of Virginia e o mestrado em Pesquisa de Operações pela Naval Post Graduate School. É piloto de CH-46E, tendo, anteriormente atuado em missões de evacuação de baixas no Iraque, de assistência humanitária no Comando do Pacífico dos EUA, e como controlador aéreo avançado no Afeganistão.

O Major James E. Wells, da Força Aérea dos EUA, atua na National Geospatial-Intelligence Agency como chefe dos programas de requisitos conjuntos. Concluiu o bacharelado em Comunicações e o mestrado em Relações Humanas pela University of Oklahoma. Serviu, anteriormente, como chefe de exercícios e planos da 3ª Ala, Base Conjunta de Elmendorf-Richardson, Alasca.

As Operações Cibernéticas Ofensivas (Op Ciber Ofs) se tornaram onipresentes ao longo da última década, e sua inclusão no planejamento deliberado, ou planejamento conjunto para contingências, tem aumentado [Entende-se por *deliberate planning* o planejamento de operações conjuntas para uma contingência militar hipotética. Veja *Joint Publication 1-02 — Department of Defense Dictionary of Military and Associated Terms* — N. do T.] Contudo, essa inclusão é, em grande medida, uma formalidade, já que as Op Ciber Ofs são inescrutáveis para quem não as conhece bem. Além disso, o ciclo conjunto de seleção de alvos não leva em consideração suas características específicas. Uma melhor percepção institucional quanto ao tema e a integração dessas operações no ciclo conjunto de seleção de alvos permitiria que os comandantes das forças-tarefas conjuntas (FT Cj) tirassem máximo proveito dessa poderosa capacidade durante o planejamento deliberado.

Entretanto, dois problemas centrais dificultam a efetiva inclusão das Op Ciber Ofs no planejamento operacional deliberado. O primeiro deles é que os estados-maiores de planejamento têm noções equivocadas com respeito às capacidades e limitações das Op Ciber Ofs em um ambiente operacional. Além disso, os estados-maiores não se sentem à vontade com os aspectos altamente sigilosos e tecnicamente complexos do domínio do ciberespaço por não entendê-los. O segundo problema é que as Op Ciber Ofs não se encaixam perfeitamente no ciclo conjunto de seleção de alvos, e sua incorporação no planejamento deliberado requer trabalho e tempo adicionais.

Conceitos Errôneos e Desafios ao Emprego Operacional das Op Ciber Ofs

Entre os diversos conceitos errôneos sobre as Op Ciber Ofs, dois são especialmente importantes. O primeiro é que elas são meios de apoio não letais, que desempenham um papel mínimo nas operações. O segundo é que, como seus detalhes são inescrutáveis em função de sua complexidade técnica ou inacessíveis por sua classificação de grau de sigilo, não vale a pena tentar empregá-las em um nível operacional.

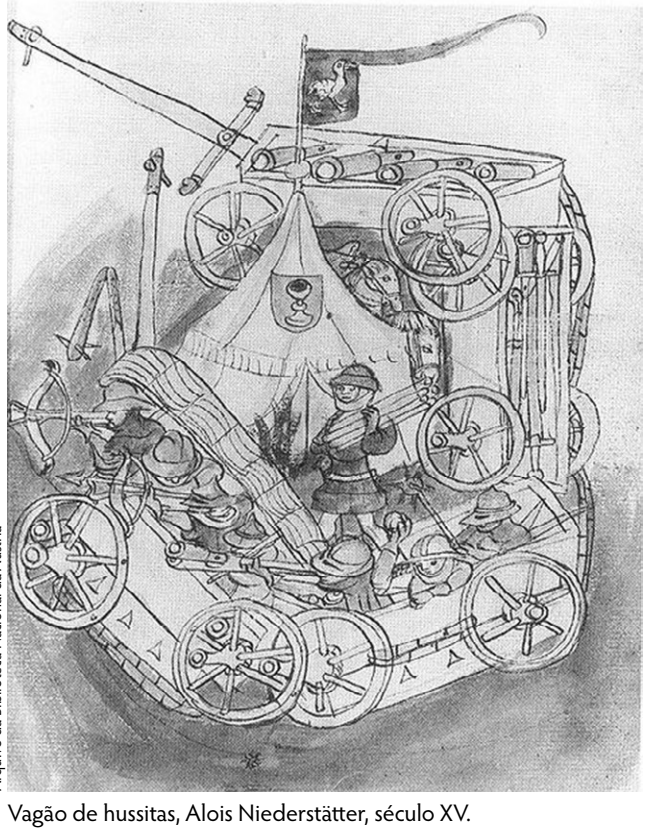
Conceito errôneo: "São apenas computadores." Uma noção comum entre planejadores é a de que as Op Ciber Ofs são meios não letais de atacar as redes de um adversário, com poucos efeitos físicos. Entretanto, ao longo da última década, as Op Ciber Ofs se tornaram mais que apenas um meio de apoio não letal como a guerra eletrônica. Sua natureza e potencial não se transformaram consideravelmente; mas nosso entendimento mudou.

Um sistema de armas revolucionário normalmente tem início como uma arma assimétrica que pode, em condições favoráveis, ser utilizada para enfrentar formas tradicionais de poder militar. Um exemplo histórico é o emprego de armas a pólvora nas mãos dos hussitas, dissidentes religiosos do século XV, que utilizaram armas de fogo primitivas para derrotar cavaleiros com armaduras[1]. No século XXI, as capacidades cibernéticas ofensivas podem oferecer aos atores estatais e não estatais um nova arma assimétrica, a ser utilizada contra sedes de poder tradicionais.

Alguns consideram um incidente ocorrido na Estônia, em 2007, como a primeira ação cibernética ofensiva contra um país. Teve início depois que o governo estoniano removeu um monumento soviético em homenagem à vitória russa sobre os nazistas na Segunda Guerra Mundial[2]. O governo estoniano suspeitou que a Rússia possa ter coordenado ataques cibernéticos de represália contra a infraestrutura digital, comando e controle do governo, instituições financeiras e redes da mídia[3]. Os ataques maciços bloquearam a troca de e-mails dos órgãos governamentais, publicaram documentos falsos e restringiram consideravelmente o acesso à internet. O "bombardeio" digital durou duas semanas e obrigou um importante banco, o Hansabank, a suspender seus serviços *on-line* por mais de uma hora. Suas perdas foram estimadas em cerca de US$ 1 milhão[4]. A negação de acesso e paralisação das redes financeiras, da mídia e do governo provocaram confusão e caos sem danos físicos ou destruição. O ataque causou grande prejuízo econômico à Estônia. Foi

muito difícil coordenar uma resposta defensiva porque o ataque foi extremamente disperso. Não havia uma autoridade estoniana que fosse responsável pela defesa de tantos meios cibernéticos diferentes[5].

Como novas armas assimétricas são integradas em um arsenal militar convencional. Após utilizarem uma nova arma assimétrica com êxito, as Forças militares às vezes a adotam como um complemento ao arsenal militar tradicional. Por exemplo, no século XVI, os exércitos empregaram mosquetes juntamente com lanças e cavaleiros com armaduras. Durante a Guerra Russo-Georgiana, em 2008, alguns especularam que as Forças russas integraram as Op Ciber Ofs a operações tradicionais para aumentar sua efetividade operacional geral. Os russos, evidentemente, conduziram vários ataques cibernéticos, que deixaram as redes do governo e da mídia da Geórgia inoperáveis[6]. Esses ataques abalaram gravemente o comando e controle militar georgiano. Foram sincronizados com a entrada das tropas russas pela fronteira com a Geórgia[7]. Eli Jellenc, especialista em cibernética, afirmou que esse evento representou o "nascimento da verdadeira guerra cibernética operacional", já que pareceu ser o primeiro emprego coordenado de ataques cibernéticos e convencionais contra um Estado-nação[8].



Arquivo da Biblioteca Nacional da Áustria

Vagão de hussitas, Alois Niederstätter, século XV.

Uma arma complementar pode evoluir e transformar-se em uma arma principal. No início do século XVIII, por exemplo, o mosquete provido de um encaixe de baioneta substituiu a lança como arma universal da infantaria. Em 2010, um *worm* conhecido como *Stuxnet* foi utilizado como arma ofensiva principal para gerar efeitos operacionais tangíveis. Apesar de sua origem desconhecida, o *Stuxnet* foi um programa do tipo "fire and forget" ("dispare e esqueça"), considerado o primeiro "míssil cibernético" do mundo[9]. O programa foi lançado, aparentemente, para sabotar as centrífugas de produção de combustível nuclear iranianas, que poderiam ser utilizadas na fabricação de urânio de qualidade militar mediante a alteração da corrente elétrica[10]. Segundo o pesquisador alemão Ralph Langner, o objetivo do ataque pode ter sido destruir o rotor da centrífuga com a vibração — o que poderia provocar sua explosão — ou apenas degradar a produção com o tempo (ao desacelerar e acelerar o motor)[11]. Embora lançado por meio de um domínio considerado como não físico e não letal, o *Stuxnet* obteve efeitos decididamente físicos ao danificar as instalações nucleares iranianas.

Os exemplos do Irã e da Geórgia mostram a gama de efeitos produzidos pelas Op Ciber Ofs, que englobam desde operações não físicas de inquietação e de informação até danos físicos à infraestrutura crítica. Sem forças ou armas com um contato físico direto, as Op Ciber Ofs podem gerar efeitos operacionais não físicos e físicos. Podem desativar nossos sistemas de defesa antiaérea e nós de comando e controle, abrir ou fechar as comportas de uma represa e destruir ou danificar máquinas industriais, como centrífugas nucleares[12]. Assim como as tradicionais armas letais e tangíveis, as capacidades cibernéticas ofensivas podem ser as "flechas" na "aljava" do comandante de uma FT Cj. Podem capacitá-lo a lidar com uma gama de alvos eficientemente, por si só ou em conjunto com outras armas.

Conceito errôneo: "Não as entendo" ou "Não tenho acesso". As capacidades cibernéticas, especialmente as Op Ciber Ofs, costumam ser envoltas em segredo. São altamente sigilosas porque, por sua natureza, a divulgação dessas operações pode revelar intenções estratégicas e operacionais. Caso obtivesse dados sobre um único alvo de Op Ciber Ofs em desenvolvimento,

Foto AP/Vahid Salemi

Técnico iraniano trabalha na Usina de Conversão de Urânio no entorno da Cidade de Esfahan, 400 quilômetros ao sul de Teerã, 03 Fev 07.

uma potência hostil poderia descobrir muitas informações sobre as capacidades cibernéticas norte-americanas e sobre as operações de um comando combatente. [Comandos Combatentes são "Comandos Conjuntos diretamente subordinados ao Secretário de Defesa e ao Comandante em Chefe [...]". Veja Douglas Bassoli, "Nivelando Conhecimentos sobre o Sistema de Defesa dos Estados Unidos da América", *Military Review*, versão brasileira, Setembro-Outubro 2011 — N. do T.] Caso descobrissem ser um dos alvos de um plano de operações que incluísse um ataque cibernético contra um nó de infraestrutura, certos inimigos poderiam utilizar a doutrina militar norte-americana para obter algum entendimento do plano. Além disso, caso dados técnicos fossem comprometidos, um adversário poderia utilizá-los para projetar e desenvolver uma arma cibernética destinada a atacar os interesses dos EUA ou de seus aliados.

Além dos desafios relacionados à questão de sigilo, os aspectos técnicos das operações cibernéticas são difíceis de entender para quem não tenha treinamento técnico. Esse é o caso, especialmente, quando comparadas a sistemas de armas tradicionais. O ciberespaço não é como os domínios físicos tradicionais, onde podemos tocar e ver todos os componentes. Ao contrário, o ciberespaço é, primordialmente, um campo virtual que pode ser manipulado para a obtenção de efeitos no mundo real, nos domínios aéreo, terrestre, marítimo e espacial. É mais fácil visualizar algo como lançar uma bomba contra um alvo do que iniciar um ataque cibernético *multihost* destinado a penetrar uma rede e a enfraquecer ou destruir um sistema crítico[13].

Marginalização por inacessibilidade. Independentemente de ser uma questão de dificuldade em entender, em obter acesso ou em empregar capacidades cibernéticas tecnicamente complexas, a inacessibilidade pode marginalizar as Op Ciber Ofs mais que as defesas de qualquer adversário. Infelizmente, a inacessibilidade pode gerar apatia entre planejadores operacionais com respeito ao emprego das Op Ciber Ofs. Podem considerar "operações cibernéticas" como um jargão que o superior queira apoiar com mera retórica, em vez

de um conjunto de armas e táticas com benefícios tangíveis. Na melhor das hipóteses, as Op Ciber Ofs podem ser marginalizadas, sendo empregadas nas margens das operações, por não serem compreendidas, acessíveis, fáceis de empregar ou consideradas confiáveis.

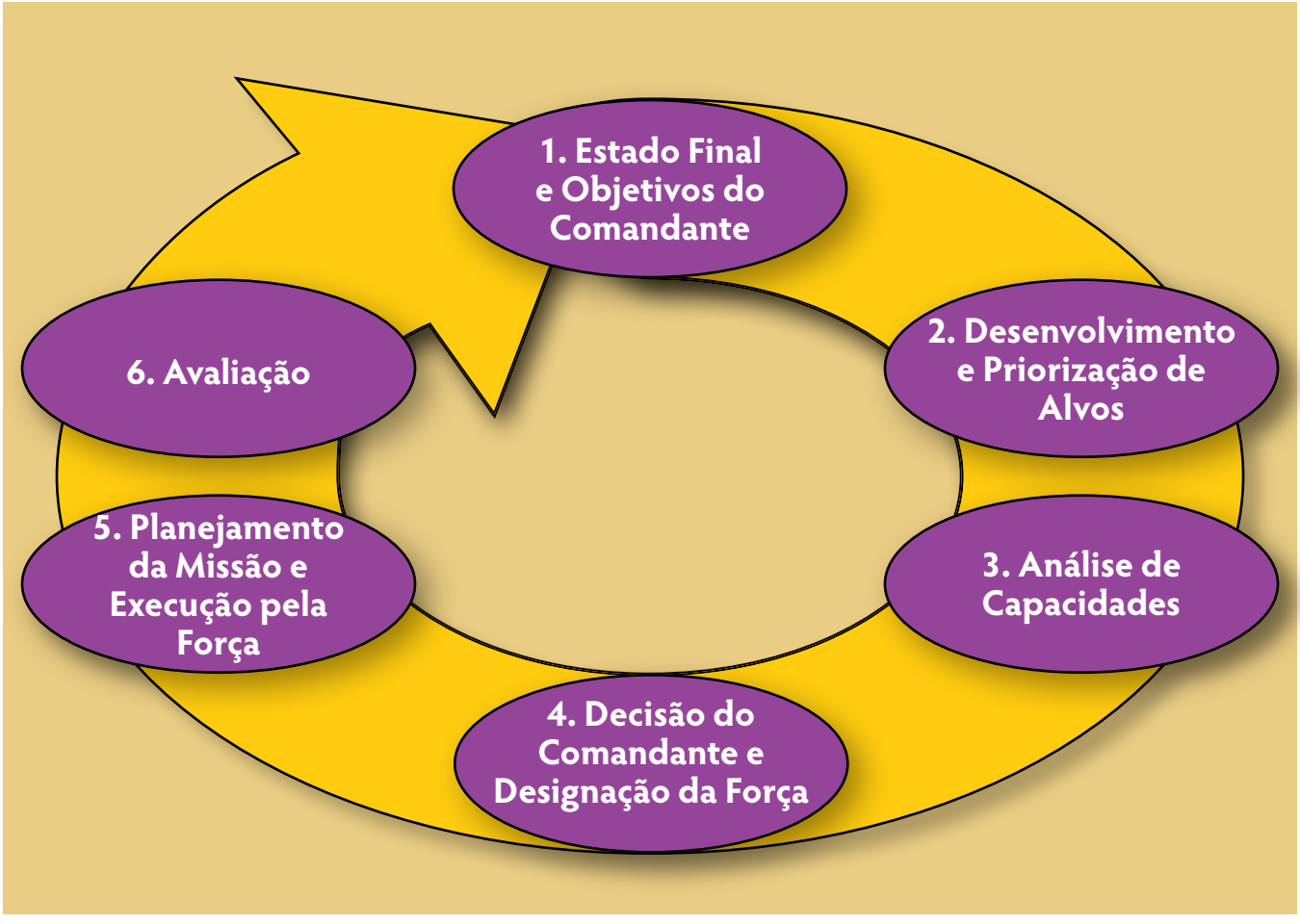
O ciclo conjunto de seleção de alvos. Além dos conceitos errôneos comuns e das questões de inacessibilidade, certos desafios são inerentes à integração das Op Ciber Ofs no ciclo conjunto de seleção de alvos (veja a figura)[14]. Duas fases do ciclo conjunto de seleção de alvos — o desenvolvimento e priorização de alvos e a análise de capacidades — têm o efeito mais significativo nos estágios iniciais do planejamento do emprego operacional das Op Ciber Ofs.

O Comando Cibernético dos EUA (USCYBERCOM) coordena os efeitos cibernéticos desejados contra um alvo, com base nas prioridades do comandante de Comando Combatente Unificado ou comandante da FT Cj. Durante o planejamento de contingência, a fase de análise de capacidades busca fazer a correspondência dos meios e material bélico alocados com o alvo e efeito pretendidos. Após um alvo ser selecionado para ser visado com meios tradicionais, ele é periodicamente considerado durante o ciclo de revisão do planejamento. Não se despendem recursos adicionais para manter acesso ao alvo até que o plano seja executado. Em contrapartida, a seleção de um alvo para as Op Ciber Ofs dá início à alocação e uso imediatos de recursos adicionais. Manter e desenvolver um alvo requer muito tempo. Durante a Operação *Odyssey Dawn* em 2011, as autoridades norte-americanas debateram o uso de Op Ciber Ofs contra a Líbia, mas decidiram não empregá-las por várias razões, principalmente o fator tempo. Analistas do jornal *New York Times* afirmaram que "na realidade, é necessária considerável espionagem digital para identificar possíveis pontos de acesso e nós suscetíveis em uma rede interligada de sistemas de comunicações, radares e mísseis como a operada pelo governo líbio e, em seguida, é preciso escrever e inserir os devidos códigos maliciosos"[15].

Como o ciclo conjunto de seleção de alvos se aplica às Op Ciber Ofs. O primeiro passo para engajar um alvo com as Op Ciber Ofs é obter acesso a ele. Sem acesso físico ou eletrônico, é impossível prosseguir com as Op Ciber Ofs. Um sistema ligado à internet é, em geral, mais acessível, embora possa ser difícil alcançar os componentes visados em função de seu próprio ambiente de segurança de rede. No caso de um sistema fechado, como o programa nuclear iraniano, seria preciso acesso interno à organização, para colher conhecimentos de primeira mão sobre o ambiente computacional na instalação visada[16]. Após adquirirem acesso a um sistema visado, é preciso que as Forças o mantenham enquanto pretenderem atacá-lo. As atualizações de rede ou mudanças no sistema efetuadas durante a manutenção programada do alvo podem fazer com que seja difícil conservar ou recuperar acesso. O risco de se obter acesso a um sistema é que o adversário talvez detecte a invasão por *hackers* muito antes do ataque. O adversário descobriria quais sistemas estariam sendo visados. Além disso, essa descoberta resultaria, sem dúvida, na perda de acesso — e na possibilidade de que o adversário analisasse o ataque para entender as operações cibernéticas norte-americanas e desenvolvesse melhores defesas ou até contra-ataques.

Depois que se ganha acesso, a etapa seguinte é identificar os atributos internos específicos do sistema visado. Os atacantes cibernéticos talvez precisem adquirir o *software* sendo visado a fim de determinar sua natureza e vulnerabilidades. No caso dos sistemas disponíveis comercialmente, isso é algo relativamente fácil de fazer: pode-se comprar o programa. No caso de sistemas raros ou cujo desenvolvimento e uso estejam restritos a um determinado país ou região, as Forças podem precisar adquirir conhecimento interno do ambiente da rede (como pode ter ocorrido com o Stuxnet)[17]. Dependendo do sistema a ser atacado, o código pode não ser discutido em inglês. Qualquer que seja o motivo, se o USCYBERCOM for incapaz de obter conhecimentos técnicos sobre o *software* visado, as Op Ciber Ofs não poderão ter seguimento: seria impossível coordenar o devido efeito. O comandante da FT Cj deve considerar esses atributos das Op Ciber Ofs ao priorizar alvos durante o planejamento deliberado.

Após haver coordenado um meio para manter acesso e obtido conhecimentos sobre o sistema visado, o USCYBERCOM poderá então coordenar a aquisição ou desenvolvimento da arma para atacá-lo. Algumas armas concebidas para atacar sistemas operacionais comuns como o *Windows* estão disponíveis comercialmente. Contudo, os sistemas produzidos e utilizados apenas em determinados países geralmente exigem que as Forças desenvolvam armas da estaca zero. Inicia-se um projeto de aquisição de *software*, nos sentidos



Ciclo Conjunto de Seleção de Alvos

técnico e jurídico. Para fins do processo de aquisições do Departamento de Defesa, os projetos de desenvolvimento de *software* são mais complexos que projetos físicos de engenharia[18]. O desenvolvimento de uma arma cibernética é um desafio complexo por esse motivo e muitos outros. Após uma arma ser desenvolvida, será preciso manter acesso contínuo ao alvo e monitorá-lo. Os atacantes precisarão impedir que procedimentos rotineiros de manutenção do sistema neutralizem seus esforços até que a arma seja empregada ou até que o alvo seja retirado da Lista Integrada e Priorizada de Alvos (LIPA) da Força Conjunta (*joint integrated prioritized target list — JIPTL*)

Desafios da designação de Forças às Op Ciber Ofs. Todas essas ações exigem bastante tempo, meses talvez, antes que algo mais que um ataque rudimentar possa ser iniciado com alguma expectativa de êxito. Além disso, dependendo do alvo e de sua acessibilidade, uma arma talvez precise passar por diversas redes até alcançá-lo. Segundo analistas da ciência forense cibernética, o *Stuxnet* pode ter infectado o ambiente de seu alvo por meio de um dispositivo removível, conectado intencionalmente ou não por um terceiro ou por alguém dentro da própria organização[19]. O *Stuxnet* teria exigido um grande número de programadores trabalhando até seis meses para infectar os computadores visados na rede fechada do programa nuclear iraniano.

Atualmente, o USCYBERCOM coordena todas as Op Ciber Ofs, com a cooperação do devido comando combatente. Isso agrava ainda mais o desafio de fazer a correspondência entre armas e alvos. Não só é preciso que um comando combatente solicite que o USCYBERCOM ataque um alvo, mas cada alvo de sua LIPA conjunta disputa recursos contra os alvos das listas de outros comandos. O USCYBERCOM analisa todas elas, conferindo uma prioridade global aos alvos

individuais e alocando-lhe escassos recursos. Mesmo que o USCYBERCOM considere um alvo como sendo de alta prioridade, o comando pode não contar com os recursos necessários para visá-lo. O USCYBERCOM precisa informar os comandos combatentes e as FT Cj quanto à sua capacidade para atacar os alvos constantes de suas listas.

Análises jurídicas onerosas. Stewart A. Baker, ex-secretário adjunto de Políticas e Tecnologia do Departamento de Segurança Interna sugere que a interpretação jurídica norte-americana das Convenções de Haia reduz a utilidade operacional das Op Ciber Ofs[20]. Afirma que "advogados por todo o governo levantaram tantas questões sobre obstáculos jurídicos relacionados à guerra cibernética que acabaram deixando nossas Forças Armadas incapazes de combater ou de até mesmo planejar para uma guerra no ciberespaço"[21].

Parte dessa complexidade jurídica advém da natureza das Op Ciber Ofs. Conforme observado anteriormente, qualquer ataque cibernético, salvo o mais rudimentar, requer a aquisição, desenvolvimento ou modificação de software para gerar os efeitos pretendidos por um comandante de FT Cj. Isso traz ao processo a Diretriz 5000.01 — O Sistema de Aquisição do Departamento de Defesa (*DODD 5000.01 — The Defense Acquisition System*). Essa diretriz requer que a "aquisição de armas e sistemas de armas do Departamento de Defesa dos EUA esteja em conformidade com toda a legislação nacional, tratados e acordos internacionais relevantes"[22]. No que diz respeito às operações da Força Aérea dos EUA, sua Instrução 51-402 afirma que sua assessoria jurídica conduzirá análises sobre quaisquer novas capacidades cibernéticas (incluindo armas) ou respectivas modificações sendo consideradas para verificar sua legalidade segundo o Direito Internacional dos Conflitos Armados (DICA), a legislação nacional e o direito internacional[23]. Um ataque tradicional com mísseis e bombas contra um objetivo precisa ser submetido a análises jurídicas apenas durante a fase de desenvolvimento e priorização de alvos, já que as armas sendo empregadas já passaram pela avaliação exigida durante a aquisição (em conformidade com a Diretriz 5000.01, do Departamento de Defesa dos EUA). Em contrapartida, como as armas cibernéticas empregadas são diferentes para praticamente cada alvo, as Op Ciber Ofs da Força Aérea dos EUA requerem duas análises jurídicas: uma durante a validação do alvo e outra durante o processo de aquisição. Isso deixa as Op Ciber Ofs à mercê da interpretação mais restrita do DICA por duas equipes diferentes de assessoria jurídica.

Essa limitação, assim como a ambiguidade geral de como o DICA se aplica às operações cibernéticas, criou o que Stewart Baker interpreta como "uma estratégia cibernética que simplesmente omitiu qualquer plano para a condução de operações ofensivas. Aparentemente, estão esperando que todos esses advogados cheguem a um acordo quanto a que tipo de operação ofensiva as Forças Armadas podem organizar"[24].

O ciberespaço, incluindo a consciência sobre as Op Ciber Ofs, deve constar do currículo básico de todo oficial.

Soluções

Esclarecendo a percepção das Op Ciber Ofs. O ensino é a chave para mudar a forma como consideramos, planejamos e empregamos as Op Ciber Ofs. O ciberespaço, incluindo a consciência sobre as Op Ciber Ofs, deve constar do currículo básico de todo oficial. O primeiro nível do ensino profissional militar conjunto (*joint professional military education — JPME*) deve incluir os fundamentos da doutrina e operações cibernéticas para todos os oficiais. Os oficiais intermediários e superiores devem estudar e integrar as operações cibernéticas operacionais e estratégicas no planejamento conjunto durante o segundo nível do JPME. Além disso, os cursos "capstone", ou fundamentais, para novos oficiais-generais, devem incluir instrução sobre as capacidades e limitações das Op Ciber Ofs. O ensino não deve ter como objetivo transformar os oficiais em especialistas cibernéticos, e sim proporcionar-lhes a mesma consciência básica sobre esse domínio que os oficiais em armas combatentes ou de apoio têm em relação a como os que pertençam a outras áreas exercem sua profissão.

Da mesma forma que os detalhes sobre sofisticados sistemas de armas convencionais, as particularidades

das Op Ciber Ofs devem permanecer classificadas em grau de sigilo. Esse é um atributo das operações cibernéticas que deve ser levado em consideração na seleção de alvos: o conhecimento dos processos específicos por meio dos quais são obtidos efeitos cibernéticos devem se restringir aos que necessitem de acesso à informação. A inacessibilidade das capacidades cibernéticas ofensivas — para qualquer um que não trabalhe diretamente em seu desenvolvimento e execução — contribui com um nível de segurança operacional que apoiará a capacidade ao longo do tempo. Além disso, conservar certa inacessibilidade em torno das capacidades cibernéticas ofensivas oferece a opção de disfarçar a intenção operacional. A maioria dos planejadores no âmbito conjunto não conta com os conhecimentos ou com o credenciamento de segurança para saber como fabricar um míssil de cruzeiro Tomahawk da estaca zero. Da mesma forma, não devem poder analisar em detalhe uma capacidade cibernética ofensiva.

Um exemplo desse paradoxo é o vírus de espionagem *Flame*, descoberto em 2012, o qual, acredita-se, circulou pela internet durante cerca de quatro anos antes de ser detectado[25]. Segundo Debra Van Opstal, o *Flame* "explorou o sistema operacional Windows para gravar áudio, imagens de tela, teclas digitadas e informações de navegação na rede dos computadores infectados"[26]. Quem quer que tenha decidido empregar o *Flame* provavelmente não conhecia os detalhes de seu funcionamento, mas entendia o efeito pretendido. O Flame é apenas mais um exemplo de uma ferramenta cibernética ofensiva difícil de detectar, mas sua natureza complexa oferece uma perspectiva única sobre o nível de detalhe necessário para gerar um efeito cibernético disseminado. O desafio para os estados-maiores de comandos combatentes e da FT Cj é aceitar e operar nesse ambiente sem limites definidos, confiando a busca dos efeitos pretendidos e priorizados ao USCYBERCOM sem compreender os detalhes do processo.

Aperfeiçoamento do ciclo conjunto de seleção de alvos. Para melhor utilizar as capacidades de Op Ciber Ofs, as comissões conjuntas de coordenação da seleção de alvos (*joint targeting coordination boards — JTCBs*) devem mudar a forma pela qual elaboram suas LIPA. Devem coordenar a designação de alvos cibernéticos com o USCYBERCOM. Isso as capacitará a melhorar o emprego das Op Ciber Ofs e integrar plenamente as capacidades cibernéticas ao tradicional poder terrestre, aéreo e marítimo.

Análise iterativa de capacidades. Toda comissão conjunta de coordenação da seleção de alvos deve incluir um representante da área cibernética, que deve ter paridade com os representantes dos componentes aéreo, terrestre e marítimo da Força Conjunta. O representante do componente cibernético deve apresentar uma lista de designação de alvos cibernéticos à comissão. Quando esta começar a elaborar a versão preliminar da LIPA conjunta com base nas listas de designação de alvos, o representante do componente cibernético poderá coordená-la junto ao USCYBERCOM. Com esses dados, o USCYBERCOM poderá informar à comissão quais alvos são considerados suscetíveis às Op Ciber Ofs, possibilitando que ela defina melhor a LIPA. Além disso, essa prática permitirá que o USCYBERCOM busque possíveis sinergias com seus esforços em curso, relativos a outros planos. Esse intercâmbio de informações contribuirá para a definição da LIPA conjunta e permitirá que a comissão conjunta de coordenação da seleção de alvos integre as Op Ciber Ofs em sua formulação.

Para obter os melhores resultados das Op Ciber Ofs, a comissão também precisa verificar se seus alvos são de longa duração. Precisa concentrar-se nos efeitos necessários, e não em como eles serão gerados. Os alvos precisam ser de longa duração para que o USCYBERCOM possa coordenar os recursos da forma mais eficiente e evitar perseguir objetivos passageiros. Um alvo de longa duração deve persistir durante vários ciclos de revisão de planejamento. Isso confere ao USCYBERCOM tempo suficiente para desenvolver as armas necessárias para engajá-lo com êxito. Além disso, um foco nos efeitos possibilitará que o USCYBERCOM proponha linhas de ação alternativas à comissão conjunta. Isso permitirá que esta última mantenha seu foco no quadro geral das Op Ciber Ofs, em vez de detalhes. O representante do componente cibernético na comissão deve ser mais do que capaz de resolver conflitos e coordenar as Op Ciber Ofs com o resto da LIPA conjunta.

Coordenação da designação global das Op Ciber Ofs. Toda comissão conjunta de coordenação da lista de alvos deve permanecer flexível quanto à sua LIPA, já que a exigência de que o USCYBERCOM forneça apoio em âmbito global significa a possibilidade de

que recursos sejam realocados. Seja por mudanças de prioridade ou outras razões, nem todos os alvos de todas as LIPA serão visados. O USCYBERCOM precisa informar cada comissão sobre o *status* de seus alvos, especialmente quando houver uma mudança de prioridades, já que isso pode ter um efeito significativo sobre a LIPA conjunta de um comando. Cada comissão deve se preparar para essa possibilidade com o desenvolvimento de listas secundárias, que reflitam a falta de acesso a um alvo cibernético. Isso também requer que a LIPA seja continuamente revista e atualizada, e não praticamente esquecida até uma subsequente revisão de planejamento operacional. A ligação direta proporcionada pelo representante do componente cibernético facilita essa questão, mas será necessário que a comissão conduza pesquisa e planejamento adicionais para alcançar o estado final desejado pelo comandante. A tentação de ignorar ou marginalizar as capacidades cibernéticas persiste, é claro, porque utilizá-las causaria frustração e trabalho adicional. A comissão precisa avaliar a possível recompensa oferecida pelas Op Ciber Ofs em relação à carga de trabalho adicional que elas possam acarretar durante o planejamento deliberado. Contudo, a integração das Op Ciber Ofs pode capacitar uma FT Cj a aumentar seu alcance além do que os tradicionais meios de fogo permitiriam e a combinar tais meios para alvos mais adequados.

Análise jurídica unificada. Os desafios jurídicos diante de uma comissão conjunta de coordenação da seleção de alvos parecem intimidantes, mas ela pode tratá-los de um modo que atenda às exigências do Comando Combatente . Embora os detalhes sobre as regras de engajamento e a legitimidade de alvos estejam no campo do direito, essa é uma área subjetiva, especialmente no que diz respeito a novas tecnologias. O emprego de dois processos jurídicos distintos — no processo de desenvolvimento e priorização de alvos descrito na Publicação Conjunta 3-60 e no processo de aquisição tratado na Diretriz 5000.01, do Departamento de Defesa — para aprovar a criação e emprego de uma arma cibernética é redundante e desperdiça escassos recursos jurídicos.

Em vez disso, o USCYBERCOM deveria conduzir ambas as análise jurídicas. A que é conduzida durante o desenvolvimento e priorização de alvos deveria ser omitida no caso de alvos cibernéticos. O USCYBERCOM deveria conduzir uma análise inicial e uma análise final do DICA em sua coordenação junto à comissão conjunta durante o desenvolvimento da arma cibernética. Além disso, como as armas cibernéticas são projetadas para alvos específicos, a equipe jurídica poderia conduzir tanto as análises exigidas pela Diretriz 5000.01 quanto a validação de alvos. O USCYBERCOM, em coordenação com o representante do componente cibernético, deve dispor dos conhecimentos técnicos especializados para avaliar e ajudar no desenvolvimento da arma. Isso aumentará a efetividade do desenvolvimento e emprego das Op Ciber Ofs. Além disso, como a assessoria jurídica não faz parte do comando combatente, há uma probabilidade menor de que ela se deixe influenciar pelo "pensamento de grupo" ou de que a influência do comando desvirtue o processo.

Conclusão

As Op Ciber Ofs oferecem ferramentas poderosas para um comando combatente ou FT Cj. Contudo, nossos próprios atritos internos — que se manifestam como mal-entendidos, inacessibilidade e processos de evolução lenta — não nos têm deixado tirar pleno proveito dessas capacidades. Nenhuma das soluções descritas é particularmente custosa nem envolvem a compra de equipamentos ou acréscimos à estrutura da força. Ao contrário, têm como foco desenvolver nosso pessoal e nossos processos, a fim de que estejam mais bem preparados para engajar um adversário em todos os domínios. Embora a implementação dessas soluções exija uma ação de longo prazo, postergá-la só agravaria o problema, efetivamente impedindo que os comandantes de FT Cj empreguem Op Ciber Ofs.

Referências

1. Saul David, *The Illustrated Encyclopedia of Warfare: From Ancient Egypt to Iraq* (London: DK Publishing, 2012), p. 95.

2. Sascha-Dominik Bachmann, "Hybrid Threats, Cyber Warfare and NATO's Comprehensive Approach for Countering 21st

Century Threats—Mapping the New Frontier of Global Risk and Security Management", *Amicus Curiae* 88 (Jan. 2012).

3. Mark Landler e John Markoff, "After Computer Siege in Estonia, War Fears Turn to Cyberspace", *New York Times* (29 May 2007).

4. Ibid.

5. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe", Wired.com (21 Aug. 2007). Disponível em: http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

6. James P. Farwell e Rafal Rohozinski, "Stuxnet and the Future of Cyber War", *Survival: Global Politics and Strategy* 53, no. 1 (Jan. 2011): p. 23-40.

7. Stephen W. Korns e Joshua E. Kastenburg, "Georgia's Cyber Left Hook", *Parameters* 38, no. 4 (Winter 2008-2009).

8. Eli Jellenc, apud Iain Thomson, "Georgia Gets Allies in Russian Cyberwar", Vnunet.com (12 Aug. 2008), http://www.v3.co.uk/v3-uk/news/1997915/georgiaallies-russian-cyberwar. Veja, ainda, John Markoff, "Before the Gunfire, Cyberattacks", *New York Times* (12 Aug. 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

9. Mark Clayton, "How Stuxnet Cyber Weapon Targeted Iran Nuclear Plant", *The Christian Science Monitor* (16 Nov. 2010): p. 4.

10. Farwell e Rohozinski, p. 23-40.

11. Ralph Langner, apud Clayton, p. 4.

12. Stephenie Gosnell Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare", Stanford Journal of International Law 48, no. 1 (Winter 2012): p. 209.

13. Anoop Singal e Ximming Ou, *Security Risk Analysis of Enterprise Net*

works Using Probabilistic Attack Graphs (Gaithersburg, MD: NIST Interagency Report 7788, National Institute for Standards and Technology, U.S. Department of Commerce, Aug. 2011).

14. Joint Publication 3-60, *Joint Targeting* (Washington, DC: U.S. Government

Printing Office [GPO], 31 Jan. 2013), Figure II-2.

15. Eric Schmitt e Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya", New York Times (17 Oct. 2011). http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against--libya-was-debated-by-us.html?_r=0.

16. Nicolas Falliere, Liam Murchu, and Eric Chien, W32.Stuxnet Dossier (Cupertino: Symantec Corporation, 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

17. Ibid.

18. Rene G. Rendon e Keith F. Snider, *Management of Defense Acquisition Projects* (Reston, VA: American Institute of Aeronautics and Astronautics, 2008), p. 66.

19. Falliere, Murchu e Chien, p. 3.

20. Stewart A. Baker e Charles Dunlap Jr., "What Is the Role of Lawyers in Cyberwarfare?" *ABA Journal* (1 May 2012). http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare.

21. Ibid.

22. Department of Defense Directive 5000.01, *The Defense Acquisition System* (Washington, DC: GPO, 12 May 2003), p. 7.

23. U.S. Air Force, *Air Force Instruction 51-402: Legal Reviews of Weapons and Cyber Capabilities* (Washington, DC: GPO, 27 July 2011), p. 2.

24. Baker e Dunlap Jr.

25. Debra Van Opstal, ".Aha' Findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience", *Center for Critical Infrastructure Protection and Homeland Security* 11, no. 2 (Aug. 2012).

26. Ibid.