Empregando a competição cibernética estratégica na América Latina

Uma missão de líder cibernético sênior

Coronel James Hamilton, USAF
Capitão Valdir Ruiz, USAF

Introdução

Os Estados Unidos estão mudando rapidamente sua abordagem para a América Latina e o Caribe (ALC), demonstrada diretamente pelo aumento do apoio do Congresso ao Comando Sul dos EUA (USSOUTHCOM). Por extensão, as Forças Aéreas do Sul (AFSOUTH), por meio de sua Direção de Comunicações (A6), estão unindo seus esforços com a divisão de operações cibernéticas do USSOUTHCOM (J38) para afetar as atividades do Departamento de Defesa (DoD) em uma abordagem de todo o governo para o teatro de operações. Assim, a AFSOUTH está buscando melhorar o compartilhamento de informações com os países da ALC a fins de promover o conhecimento e a capacidade cibernética dentro do teatro de operações do sul. Este novo enfoque apresenta oportunidades e desafios no domínio cibernético. Dois destes desafios serão abordados. Em primeiro lugar, à luz da atual falta de conhecimento geral sobre ameaças cibernéticas, o investimento monetário aparentemente vantajoso da China é aceito pelos países da ALC como uma troca justa pelo avanço. No entanto, uma análise de custo-benefício que justaponha a soberania do Estado-nação e o avanço tecnológico é necessária para ajudar as nações da ALC a entender os riscos de segurança cibernética associados a essa troca. Em segundo lugar, uma avaliação cibernética abrangente, baseada no Instituto Nacional de Normas e Tecnologia (NIST, *National Institute for Standards and Technology*), ajudaria diversas agências ou departamentos do governo dos EUA a combater a influência da China e, por fim, apoiando os países parceiros a fazer escolhas bem-informadas como parte de seu cálculo nacional de segurança cibernética. Uma avaliação cibernética abrangente permite que o DoD adapte as ofertas de educação e os objetivos de exercícios da coalizão, combinando as atividades com os níveis de maturidade dos parceiros em todo o Hemisfério Sul, resultando em uma metodologia cibernética sólida que realmente avança as capacidades dos parceiros.

Uma nova abordagem

A comandante do USSOUTHCOM, General Laura J. Richardson, testemunhou recentemente ao Congresso e discutiu a postura do USSOUTHCOM, identificando três linhas principais de esforço, especificamente: "fortalecer alianças e parcerias, combater ameaças e desenvolver nossa equipe."[1] A General Richardson destacou várias áreas de concentração em seu depoimento, mas o foco deste ensaio estará na influência chinesa e russa na região e explicará por que a defesa e a indústria dos Estados Unidos devem ser os parceiros preferidos da ALC para a cooperação em segurança cibernética; além disso, abordará a necessidade de maior aplicação cibernética e treinamento.[2]

Mais recentemente, Matt Ferchen observou que existe um atrito de competição estratégica entre os EUA e a China e que está avançando na região.[3] Por exemplo, Honduras recentemente migrou para a China, longe de Taiwan, a fim de abrir maiores opções comerciais e financeiras com a China.[4] Além disso, Honduras se absteve anteriormente da resolução das Nações Unidas condenando a invasão da Ucrânia pela Rússia.[5] Essas ações correspondem ao avanço da Rússia e da China na região, facilitando à Rússia alavancar seu status de ator na ALC e contribuindo diretamente para a Iniciativa Cinturão e Rota da China (BRI).[6] Parte da influência da China inclui avanços tecnológicos e não está restrita a empréstimos ou projetos de hidrelétricas. Ferchen apresenta a "Rota da Seda Digital" da China, expondo um cabo de fibra ótica que conecta o Brasil à África, financiado principalmente por empresas chinesas. Pode-se inferir que a parceria da ALC com empresas chinesas, possivelmente decorrente de restrições orçamentárias (como visto com Honduras) ou falta de compreensão sobre defesa cibernética, coloca em questão a visão técnica da ALC, como previu o ensaio anterior de Manuel Heitor, *et al*., de 2014, intitulado, "A América Latina pode avançar depois de uma década perdida em mudanças técnicas?"[7]

Embora a ALC tenha progredido constantemente em direção à utilização do domínio cibernético, tornou-se um campo complexo que os governos correm para entender, defender, atualizar e manobrar. Áreas como computação em nuvem, confiança zero (*zero trust*), configuração de serviço de nome de domínio e higiene cibernética são fundamentais para os profissionais cibernéticos. Essas áreas podem ser usadas para desenvolver uma relação de confiança e alternativas confiáveis, levando a um maior esforço dos EUA-ALC para aumentar o envolvimento cibernético e a educação cibernética em todo o hemisfério. O avanço da China não é novo; sua BRI tem aumentado constantemente em poucos anos, mas novos indícios sugerem que a BRI pode estar em declínio ou avançando sob outras alcunha, ou seja, a Iniciativa de Desenvolvimento Global.[8] No entanto, está buscando

vantagens nas operações espaciais e de informação.[9] Estima-se que a competição no teatro da ALC não é apenas resultado da expansão regional da China, mas também reforçada pelo foco dos EUA no Oriente Médio e pela falta de atenção à América do Sul, conforme descrito no ensaio EUA-Afeganistão de Larry P. Goodson de 2015.[10] Aparentemente, os EUA ofereceram menos compromissos e investimentos aos nossos parceiros regionais durante um período prolongado, permitindo assim a entrada da China e da Rússia.[11]

Então, por que os EUA não avançaram ainda mais à luz de seus esforços redirecionados para a educação cibernética e defesa cibernética para a ALC? Um artigo da BNamericas sobre a empresa chinesa de telecomunicações Huawei exemplificou a rapidez com que a China cresceu nos últimos dez anos; a empresa é uma força dentro da ALC e está presente em escolas e universidades (90 apenas no Brasil), redes móveis 5G,[12] computação em nuvem por meio de sua solução CloudCampus 3.0,[13] roteadores, manípulos externos (*switches*) de computador e outros investimentos, dos quais mantém aproximadamente 50-80% de participação de mercado em vários países.[14] Em suma, durante anos houve um atrito progressivo entre os EUA e a ALC, possivelmente decorrente do foco dos EUA no Oriente Médio[15] e de sua interação inconstante com a ALC,[16] combinada com a política de defesa EUA-ALC que se concentrou mais em parceiros com funções de apoio para combater o tráfico de narcóticos e impedir o terrorismo externo e ameaças,[17] todos contribuindo para uma relação descontínua na região que permitiu à China preencher a lacuna.

Recuperando a vantagem

Uma vez que a China têm procurado avançar o comércio, projetos e empréstimos dentro da ALC, o Departamento de Estado agiu para combater as manobras da China com a divulgação, em 18 de dezembro de 2019, do esforço *América Crece* (América Cresce) como uma abordagem de todo o governo para promover o desenvolvimento econômico deliberado no hemisfério.[18] Desde então, outras agências governamentais iniciaram sua própria defesa da parceria com a ALC, como a inclusão do Departamento de Comércio no 51º Conferência Anual de Washington sobre as Américas, onde pediram por maiores laços e cooperação.[19] Da mesma forma, as conferências e atividades da Associação das Câmaras de Comércio Americanas na América Latina e no Caribe contribuíram para o investimento da ALC.[20] Esses esforços prenunciaram a declaração de postura da General Richardson e buscaram a sinergia entre as organizações governamentais e industriais para contribuir para a abordagem de todo o governo como uma alternativa à influência da China e da Rússia.[21]

AFSOUTH como parceira

Em seu ensaio sobre como superar a China, o vice comandante do AFSOUTH, brigadeiro-general Sean Choquette, delineou as linhas de esforço do componente aéreo de apoio ao USSOUTHCOM, nomeando o domínio cibernético como uma área de foco concentrada no teatro da ALC.[22] Como linha de esforço, o domínio cibernético atua como uma Área de Interesse (AOI) dentro da Área de Responsabilidade (AOR) da AFSOUTH. O general Choquette defendeu o compartilhamento de informações e a colaboração na área cibernética, além de chamar os especialistas no assunto (SMEs) da AFSOUTH para educar parceiros no âmbito da segurança cibernética e de infraestrutura.[23] Para tornar esses objetivos estratégicos uma realidade, a AFSOUTH A6 coordenará com o J38 do USSOUTHCOM para se juntar às forças diplomáticas e militares do teatro da ALC para identificar e empregar Medidas de Desempenho (MOP) e Medidas de Eficácia (MOE) por meio de processos de planejamento conjunto deliberados. A AFSOUTH A6 atuará para liderar e apoiar coletivamente as trocas cibernéticas de SMEs (SMEEs) com seus parceiros nacionais, NIST e órgãos acadêmicos para estimular a maturidade cibernética em direção a uma inclinação ascendente para promover o conhecimento e a capacidade cibernética. Para facilitar essa maturidade, existem três áreas específicas de capacidade cibernética a serem desenvolvidas: padronização, educação e emprego, que estão vinculadas às respectivas linhas de esforço do USSOUTHCOM.

Avaliação e padronização do domínio cibernético

O grande treinador de beisebol americano, Yogi Berra, disse certa vez, "Se você não sabe para onde está indo, pode acabar em outro lugar." O secretário de Estado Henry Kissinger afirmou de forma mais estoica, "Se você não sabe para onde está indo, todo caminho o levará a lugar nenhum." Rudimentarmente, os EUA precisam entender as capacidades cibernéticas em todos os 31 países parceiros da AOR. À medida que nossos vizinhos latino-americanos enfrentam sua própria complexidade cibernética, desafios como oscilações políticas, o direito de negociar com exportadores mundiais e/ou diferenças regionais causam distração no domínio cibernético. Uma vez que os 31 parceiros possuem diferentes níveis de maturidade cibernética, que padrão deve ser usado para criar uma capacidade de cibersegurança coesa e resistente em toda a AOR? Ter todos os 31 parceiros praticando no mesmo nível de maturidade cibernética simultaneamente é irrealista; a verdadeira maturidade cibernética leva anos para se desenvolver. Por exemplo, a Organização dos Estados Americanos procurou reunir seus membros para a conscientização cibernética por meio de um relatório conjunto divulgado em 2013 que examinava

as tendências de segurança cibernética,[24] mas houve uma participação coletiva limitada da ALC, o que frustrou o ímpeto. Por isso, a AFSOUTH incentiva e defende a adoção do modelo de estrutura de cibersegurança (CSF) do NIST.[25] O NIST CSF foi concebido para funcionar com todo o governo dos EUA, instituições apoiadas por subvenções federais dos EUA e cadeias de abastecimento de agências federais dos EUA. Heitor, *et al.*, defenderam essa via de segurança ao afirmarem que esse é "[um] programa de extrema importância e relevância que tem ajudado as empresas inovadoras americanas a crescer;"[26] isso vem de uma perspectiva interna da ALC, uma vez que esses pesquisadores eram nativos de Portugal, México, Brasil e Chile.

Notadamente, o NIST CSF usa áreas da norma ISO 27001, mas embora a ISO 27001 seja uma norma internacional, não é um requisito legal para áreas específicas de negócios, ao contrário de estruturas de gestão de risco como NIST CSF, GDPR e HIPAA.[27] A ALC já tem um ponto de partida; a Agência de Governo Eletrônico e Sociedade da Informação do Uruguai já adotou o modelo de 5 níveis do NIST CSF e é membro das nações digitais (uma rede colaborativa dos principais governos digitais do mundo) desde 2018, usando o NIST CSF como roteiro.[28] Representantes do NIST também viajaram para a Colômbia e Brasil para discutir os padrões NIST para indústria, mercados e adoção de governos inteligentes em comércio e defesa.[29] Quando chegarmos a um acordo sobre uma norma comum, podemos começar a trilhar um caminho comum. A maturidade cibernética do parceiro pode ser avaliada, compreendida e desenvolvida por meio de um modelo de avaliação cibernética ubíquo. Usando as operações, atividades e investimentos cibernéticos (OAIs) da AFSOUTH, o A6 sincronizará os esforços para integrar o plano de apoio à campanha de teatro do USSOUTHCOM para conscientização de domínio nos compromissos da OAI para preencher as lacunas de defesa cibernética. MOPs e MOEs desenvolvidos deliberadamente medirão o progresso utilizando uma avaliação de linha de base do NIST CSF como ponto de referência, reutilizando-a iterativamente como um medidor de maturidade e, ao mesmo tempo, atuando como um léxico cibernético comum dentro e em todo o teatro da ALC.[30]

Educação

A educação ocorre em todos os níveis da OAI. Na verdade, as OAIs oferecem abordagens flexíveis para o emprego cibernético durante a interação EUA-ALC; por exemplo, os compromissos dos principais líderes (KLE, *Key Leader Engagements*) trabalham em um nível sênior entre líderes para introduzir e reforçar as melhores práticas, neste caso as práticas cibernéticas. Os líderes militares dos EUA oferecem sua visão sobre como o DoD amadureceu através de sua

capacidade cibernética em um nível estratégico. Da mesma forma, os SMEEs promovem diálogo especializado e estimulante e/ou envolvimento baseado em aplicativos, como o SMEE cibernético e de inteligência realizado no Chile, visto na Figura 1. Os SMEEs permitem que indivíduos dentro do domínio cibernético da AOI possam debater coletivamente problemas e resoluções. Quando os especialistas em cibersegurança trocam ideias, as melhores práticas podem ser utilizadas rapidamente, impedindo a intrusão na rede e os vetores de ameaças em vários níveis. O intercâmbio de ideias deve também abranger domínios como as avaliações cibernéticas, os objetivos dos exercícios, as conferências e o treinamento formal na área de cibersegurança.

Figura 1. Forças Cibernéticas dos EUA / Intel e SMEEs Cibernéticos, representante A6, Capitão Jefferson no Chile

Fonte: Autores

Avaliações

O J38 do USSOUTHCOM e o AFSOUTH A6 fazem parceria para executar Equipes Conjuntas de Assistência Cibernética de Comando de Combate (JCCAT). As JCCATs operam a pedido de um parceiro da ALC, permitindo que especialistas

avaliem políticas, práticas e procedimentos de redes cibernéticas. As JCCAT agem como SME, mas diferem na aplicação imediata da avaliação; essas pequenas equipes usam seu conhecimento tácito para trabalhar com países parceiros para dissecar uma invasão de rede ou ameaça de *malware* do sistema e detectar o impacto dessa ameaça. Idealmente, os JCCATs acontecem antes de uma ameaça, para identificar vulnerabilidades, mas independentemente da necessidade ou do momento, os EUA estão dispostos a colaborar antes e após a avaliação para educar equipes cibernéticas profissionais com ideias semelhantes.

Exercícios

Os exercícios existem para avaliar as forças militares, permitindo que essas forças aprendam com seus erros; e a análise crítica durante os relatórios pós-ação permitem a compreensão do ciclo de tomada de decisão. Assim, para serem efetivas, as ações no campo precisam estar deliberadamente vinculadas em uma metodologia de causa e efeito. Historicamente, não havia uma linha traçada nas fases de planejamento plurianual dos exercícios para determinar as MOEs. A intenção da AFSOUTH A6 agora é usar uma abordagem deliberada, escalonada e mensurável em relação às OAIs que promovem a maturidade cibernética. Em suma, avaliar, ensinar, testar, medir e ajustar são os pontos decisivos para a maturidade cibernética e os exercícios das nações parceiras utilizarão essas habilidades.

Conferências

A ALC organiza algumas das melhores conferências técnicas do mundo. A participação e a interação em conferências não apenas educam em nível acadêmico, como também reforçam as discussões paralelas, para além da apresentação formal de práticas cibernéticas. O COVID-19 acabou com a participação em conferências e agora estamos superando o déficit de troca de ideias. Para liderar neste espaço, a A6 participou de várias conferências da ALC para se envolver com nossos colegas e os resultados são muito promissores. Não obstante, isso significa que os EUA também devem organizar conferências de conscientização cibernética.

A A6 está, portanto, trabalhando para receber os parceiros da ALC, a fim de participar de uma discussão conjunta sobre cibernética e tecnologia da informação da ALC no evento Alamo ACE da Associação de Comunicações e Eletrônica das Forças Armadas (AFCEA) em San Antonio, Texas. A capacidade dos profissionais do setor, bem como Soldados, Marinheiros, Guardas e Aviadores de ouvir desafios e avanços nas capacidades cibernéticas de nossos parceiros da ALC gera compreensão e apoio da comunidade, e pode resolver apenas alguns problemas em

apoio aos interesses compartilhados. A AFSOUTH está muito entusiasmada com o fórum da AFCEA e deseja torná-lo um evento recorrente.

A educação integrada por meio de conferências internacionais também informa os participantes sobre as melhores práticas, padronização e riscos do setor. Um exemplo é a cooperação programática do NIST, onde se discute as cidades seguras/inteligentes. O NIST alerta que esta tecnologia, se implementada de forma deficiente, pode ser uma ameaça à privacidade e segurança pessoal, mas se feita por meio da colaboração da indústria multinacional, pode trazer interoperabilidade de acordo com as normas ISO/IEC do Comitê Técnico Conjunto.[31]

Treinamento Militar Formal

O treinamento formal assume muitas formas. A General Richardson promoveu a Academia Interamericana da Força Aérea (IAAFA) na Estratégia do USSOUTHCOM como um mecanismo para a educação militar profissional e colaboração. Para alavancar este veículo de língua espanhola, a AFSOUTH A6 fez uma parceria com a IAAFA para estabelecer um novo curso de Operações Cibernéticas de Defesa proporcional às habilidades de nossos parceiros nacionais.[32] Este curso visa as nossas forças alistadas; educá-los é fundamental para uma dissuasão eficaz, especialmente quando envolve cibersegurança. Levando esse conceito adiante, a A6 está trabalhando com a IAAFA e a Universidade de Defesa Nacional, para empregar um curso cibernético estratégico para líderes sênior que imbuiria os líderes parceiros de uma compreensão fundamental da defesa cibernética, permitindo-lhes tomar decisões críticas de defesa sobre aquisição, instalação e manutenção de suas redes militares.

Se os EUA e a ALC quiserem avançar em direção a uma interoperabilidade coerente, então o estado final é trabalhar com todos os 31 parceiros em direção à sua própria maturidade por vários meios. A abordagem da AFSOUTH combina o planejamento de operações aéreas e conjuntas com exercícios. Como tal, uma série deliberada é desenhada a partir de uma estrutura padronizada de gestão de riscos cibernéticos, por meio da educação e SMEEs, para a consciência cibernética inerente e capacidade defensiva. Este objetivo é apoiado pela participação em conferências e treinamento formal; o ponto culminante deve então ser o engajamento e o emprego de exercícios utilizando essas experiências. Isso produz melhores parcerias de segurança que atuam para vincular ações cibernéticas e criar uma compreensão robusta da defesa cibernética para que a AFSOUTH possa ajudar a atingir as metas de maturidade do parceiro.[33]

Emprego

Richard L. Manley teorizou em seu artigo no *Joint Force Quarterly* que futuras operações cibernéticas ocorrerão nas sombras, efetivamente na área cinzenta, feitas assim para evitar uma guerra em grande escala ou conflito armado.[34] Ele afirmou também que tanto a China como a Rússia já operam nesta área; a China especificamente navega sem restrições, combinando os elementos do poder nacional, diplomacia, informação, forças armadas e economia (DIME), para ditar sua agenda. Se a ALC não reconhecer que a China tem uma agenda, então os parceiros da ALC renunciam inevitável e sistematicamente à sua soberania nacional através de cada compra ou acordo cibernético.

Para combater as forças chinesas e russas, a utilização da recém-publicada doutrina da Força Aérea dos EUA (USAF) oferece prontamente uma estrutura para defesa e avanço do conhecimento e capacidade cibernéticos. As forças amigáveis podem empregar o princípio da *Persistência*, que "nega a um adversário uma oportunidade de aproveitar a iniciativa ou de realizar diretamente as tarefas atribuídas", e combiná-la com a Flexibilidade e Versatilidade, que permite "ao Poder Aéreo alcançar sinergias através de operações assimétricas e paralelas."[35]

As ações de apoio a estes princípios estimulam a capacidade inerente de superar as barreiras culturais e linguísticas. Um desses exemplos é a alavancagem da relação formal que existe com o Gabinete da Guarda Nacional (NGB, *National Guard Bureau*) enquanto conduz o Programa de Parceria do Estado (SPP), que associa unidades da Guarda Nacional Aérea e do Exército com os países da ALC. A A6 procura aproveitar os intercâmbios que já ocorrem entre as associações NGB-ALC para maximizar as parcerias. Idealmente, se um SPP opera dentro de uma AOI cibernética, como realizar um exercício militar ou liderar um SMEE, então a A6 também estaria nessa equipe. Por exemplo, em 2021, a AFSOUTH A6 liderou e realizou três eventos cibernéticos e apoiou o JCCAT. Em 2022, a A6 liderou três de seus primeiros compromissos cibernéticos presenciais, todos contando com o apoio de provedores de força provenientes da USAF, Força Espacial e NGB.

Para superar a barreira linguística externa, a AFSOUTH A6 entrou em contato com especialistas cibernéticos habilitados para idiomas de várias organizações, incluindo a IAAFA e o Centro de Cultura e Idiomas da USAF (AFCLC), que gerencia o Programa de aviadores habilitados para idiomas (LEAP, *Language Enabled Airmen Program*). O LEAP é um multiplicador de forças, uma vez que o seu papel é desenvolver aviadores multiculturais habilitados para idiomas com proficiência em línguas estrangeiras de nível profissional para apoiar diretamente o poder aéreo, o que fortalece as parcerias e a interoperabilidade.[36] Operando internamente no teatro da ALC, as nações parceiras geralmente têm um Oficial de

Cooperação em Segurança (SCO) designado para identificar e projetar as OAIs e treinamento para seus respectivos países. Os SCOs fornecem dados sobre as OAIs recentemente realizadas que podem incluir uma avaliação resumida do estado atual da capacidade cibernética de seus países.

Notadamente, os SCOs incentivam os componentes do serviço a trabalharem juntos quando realizam eventos cibernéticos conjuntos, em vez de executar eventos específicos de serviço, a fim de reduzir silos ou funis centrados em componentes. Esta defesa está bem colocada, uma vez que alguns Ministérios da Defesa da ALC nomeiam componentes de serviços específicos como líderes operacionais para a condução de operações no ciberespaço, uma vez que podem não estar focados na simetria de componentes conjuntos. Assim, alcançar a paridade com os países parceiros pode representar um desafio, uma vez que a sua estrutura de forças pode não coincidir com a estrutura das forças cibernéticas dos EUA, mas a flexibilidade na cooperação ajuda a superar as diferenças nas diferentes estruturas das forças conjuntas de parceiros. Enquanto os EUA trabalham para simplificar sua própria articulação, também devem incentivar a colaboração conjunta entre os parceiros da ALC para uma defesa cibernética bem-sucedida. Por exemplo, durante duas SMEEs parceiras diferentes em 2022, a AFSOUTH testou planos cibernéticos conjuntos, provando que esses compromissos poderiam ser bem-sucedidos e produtivos quando as barreiras de comunicação fossem retiradas, com os ramos militares participantes conversando abertamente e trocando informações.

Para promover nossa conectividade ALC, devemos seguir o chamado à ação do chefe do Estado-Maior da USAF, general Charles Q. Brown, Jr., e "Acelerar a Mudança ou Perder" para participar da competição estratégica que ele descreveu em seu desafio.[37] Para facilitar esse desafio, a AFSOUTH precisará encontrar novas formas de recrutar especialistas técnicos e habilitados em idiomas para realizar compromissos, avaliações e treinamento. Uma possibilidade é contratar provedores de força de todos os teatros e comandos, utilizando o potencial inexplorado de aviadores para aumentar as OAIs de cooperação em segurança cibernética no USSOUTHCOM.

O caminho a seguir

A AFSOUTH está planejando realizar três SMEEs no Ano Fiscal (AF) de 2023 e está ajustando conceitos para eventos propostos para o Ano Fiscal de 2024 para promover a conscientização e a capacidade cibernética. No ano fiscal de 2024, a AFSOUTH A6 ampliará seu alcance e dobrará seu número de OAIs para aproximadamente 12. A AFSOUTH reconhece que, embora seja importante manter compromissos com parceiros estratégicos maiores, também construirá e manterá relações com países menores na AOR do USSOUTHCOM. Isso nos permitirá

encontrar novas formas de identificar e alocar recursos, financiamento e pessoal, e exigirá criatividade, bem como conhecimento das autoridades de financiamento sob as quais a cooperação dos EUA em matéria de segurança opera. A criação de novos eventos será um desafio, mas proporcionará a vantagem necessária para competir estrategicamente com a China e a Rússia no domínio cibernético.

O caminho a seguir para fortalecer e avançar o conhecimento e a capacidade cibernética é criar cenários táticos que exijam que as forças militares manobrem através dos objetivos do exercício e do atrito que devem criar. Por exemplo, interromper uma rede de rádio, introduzir um efeito de negação de serviço de rede ou simular uma ameaça interna durante um exercício permite que planejadores, líderes e forças militares pensem criticamente de forma conjunta e de coalizão para mitigar a ameaça.

Este caminho já tem precedentes, como a Colômbia se tornar uma nação não pertencente à OTAN como Parceiro Global em 2018. Eles reconheceram a necessidade de sincronizar e padronizar sua postura de defesa com outras nações, assim procuraram se tornar um líder da ALC em treinamento e defesa cibernética.[38] À medida que progridem, a Colômbia exercita e organiza fóruns acadêmicos para treinar e testar a sua capacidade cibernética.

O custo da inação

Invasões, ataques e vulnerabilidades cibernéticas ocorrem repetidamente, como visto no Peru, Chile, México, El Salvador e na última invasão na Colômbia, e continuam impunes.[39] Não surpreendentemente, o ensaio de 2010 de Curtis A. Ward no *Joint Forces Quarterly* discutiu a necessidade do Caribe iniciar ações preventivas para sua segurança nacional e interesses econômicos regionais.[40] Embora tenha havido progresso, também houve avanços da China na região do Caribe,[41] com os chineses chegando ao ponto de criar um roteiro para o avanço durante a Cúpula da Comunidade de Estados Latino-Americanos e Caribenhos (Celac).[42] Uma das áreas identificadas para expansão inclui uma Cúpula de Ciência, Tecnologia e Inovação China-CELAC. Por que isso deveria ser uma preocupação? Uma pesquisa recente da Gartner Inc., destacou que a Huawei possui uma presença significativa no espaço de *firewall* e continua desenvolvendo recursos de IA e aprendizado de máquina, em parte atribuídos por seu atraente modelo de preços.[43] No entanto, isso acelera o entrincheiramento da China na ALC com "empresas de tecnologia que estabelecem padrões como Huawei, ZTE, Dahua e Hikvision – todas sancionadas pelos EUA – em infraestrutura regional, permitindo que Pequim dite as regras do comércio por uma geração."[44]

Esses líderes da indústria de tecnologia chinesa usam efetivamente sua participação no mercado e experiência para extrair dados, de acordo com a lei chinesa,

dos países anfitriões que instalam seus equipamentos.[45] Sem saber, a ALC reforçou a expansão chinesa por meio de contratos de infraestrutura que podem ter resultados negativos na segurança cibernética de um país, uma vez que esses contratos foram considerados "predatórios" quando analisados.[46] Um exemplo é o caso da extração de dados da sede da União Africana que ocorreu ao longo de um período de vários anos, servindo como testemunha dos efeitos dos contratos chineses em ação.[47] Outro exemplo de instalação de tecnologias da informação é a integração de Cidades Seguras, a pretexto da segurança e da redução da criminalidade, que coleta dados biométricos sobre as populações dos países anfitriões[48] enquanto trava a nação anfitriã em contratos de substituição jurídicas.[49] Sincronizar e alavancar a indústria cibernética e de comunicações de corretores honestos para oferecer *software* e *hardware* baseados em valor para a comunidade da ALC, embora muitas vezes de custo mais alto, certamente garantiria uma postura de defesa soberana na região da ALC.

Sinais de alerta de ações cibernéticas chinesas nefastas e invasões russas são abundantes e se ramificam em áreas muitas vezes consideradas benignas. Os hospitais ou laboratórios biomédicos que a China patrocina, ou os testes de vacinas que oferecem, ajudam a extrair o DNA da população anfitriã para coletar diretamente dados que contribuem para o controle de doenças e o marketing farmacêutico da China.[50] Cada passo lento e deliberado da China é um passo à frente dos EUA e seus parceiros da ALC, à medida que a China lentamente coleta dados e ganha poder de influênica para sua posição e manobra na AOR.

Em resumo

O USSOUTHCOM nomeou a AFSOUTH como líder de inovação do comando. Além disso, o General Choquette pediu maior compartilhamento de informações entre as nações da AFSOUTH e da ALC.[51] Como resultado, a A6 está respondendo a esses chamados, a fim de promover o conhecimento e a capacidade cibernética internacional dentro do teatro de operações do sul. Isso será feito através de um método deliberado de padronização, educação e emprego de processos e procedimentos. Facilitar as operações cibernéticas das nações parceiras através da ligação dos objetivos do NIST CSF, treinamento e exercícios militares deve produzir uma tendência positiva em sua jornada cibernética. Além disso, uma abordagem de todo o governo deve ser usada para sincronizar os esforços organizacionais em compromissos de nações parceiras e deve incluir o DoD, o Departamento de Comércio, a Câmara de Comércio e outras comunidades de corretores honestos. A A6 também aproveitará os aviadores faladores de espanhol, através dos programas AFCLC e LEAP, para preencher a lacuna linguística para facilitar a ligação entre os profissionais cibernéticos dos EUA e da ALC. A A6 também

sincronizará a entrada cibernética do KLE, PMEs, JCCATs, participação em conferências, esforços de educação e treinamento para afetar positivamente uma estrutura de segurança cibernética saudável para a maturidade do teatro. A A6 fará isso por meio da interface com a comunidade cibernética da nação parceira para determinar seus respectivos requisitos, de um ponto de vista recíproco, a fim de adaptar os esforços e efeitos cibernéticos.

No entanto, as nações da ALC devem determinar se o avanço tecnológico favorável ao orçamento vale o custo de sua soberania. Os dados de seus cidadãos, bem como os dados de segurança de defesa, estão em jogo com a tecnologia chinesa. Além disso, os hackers russos continuam introduzindo malware e narrativas questionáveis que representam um risco de segurança cibernética em um teatro de operações de defesa cibernética imaturo. A América Latina e o Caribe têm a oportunidade, com base na proximidade dos EUA, de investir fortemente em parcerias da indústria cibernética favoráveis ao crescimento das nações parceiras para impedir a China e a Rússia.[52] De fato, os EUA são palco de uma competição estratégica, mas é à ALC que pertence a escolha decisiva. ❑

Notas

1. Gen. Laura Richardson, USA, Comando Sul dos EUA (USSOUTHCOM), "Declaração do Estado do Exército de 2023 do SOUTHCOM ao Congresso" (8 de março de 2023), https://www.southcom.mil/Media/Special-Coverage/SOUTHCOMs-2023-Posture-Statement-to-Congress//#/?currentVideo=31344.

2. Ted Piccone, "A geopolítica da ascensão da China na América Latina," *Brookings Institution Reports* (Washington, DC: The Brookings Institution, novembro de 2016), https://www.proquest.com/docview/1881432909/abstract/79CBF515D9154B19PQ/1.

3. Schneider, Florian, ed., *Perspetivas Globais sobre a Iniciativa Cinturão e Rota da China: Afirmando a Agência por meio da Conectividade Regional,* Amsterdam University Press, (2021), https://doi.org/10.2307/j.ctv1dc9k7j.

4. "Autoridade hondurenha: EUA 'Respeitam' decisão sobre relações com a China," *Reuters*, (21 de março 2023), https://www.reuters.com/world/honduran-official-us-govt-respects-decision-seek-china-relations-2023-03-21/.

5. Sandra Cuffe, "Por que a América Central alterou os votos da ONU sobre a guerra Rússia-Ucrânia?," *Al Jazeera,* (21 de outubo de 2022), https://www.aljazeera.com/news/2022/10/21/why-did-central-america-shift-un-votes-on-the-russia-ukraine-war.

6. Evan Ellis, "O mais recente retorno da Rússia à América Latina," *Global Americans* (blog), (19 d janeiro de 2022), https://theglobalamericans.org/2022/01/russia-return-latin-america/.

7. Manuel Heitor et al.,, "A América Latina pode avançar após uma década perdida em mudanças técnicas? ... Observando as oportunidades de mudança baseadas no conhecimento em tempos de aumento der incertezas," *Journal of Technology Management & Innovation*, 9, no. 4, (2014), 1–19, https://doi.org/10.4067/S0718-27242014000400001.

8. Andreea Brînză, "O que aconteceu com a iniciativa 'Um Cinturão, uma Rota'?," (6 September 2022), https://thediplomat.com/2022/09/what-happened-to-the-belt-and-road-initiative/.

9. Robert Morgus et al., "A China e Rússia estão na ofensiva cibernética na América Latina e no Caribe? Uma revisão de suas capacidades cibernéticas e as implicações para os EUA e seus parceiros na região," *Security Research Hub Reports*, (1 de Janeiro de 2019), https://digitalcommons.fiu.edu/srhreports/cybersecurity/cybersecurity/14.

10. Larry P. Goodson, "Os EUA e o Afeganistão após 2014," *Asian Survey,* 55, no. 2, (2015), 249–72, https://doi.org/10.1525/as.2015.55.2.249.

11. Lara Seligman, "Biden pressionado para focar na América Latina há muito negligenciada à medida que o caos se instala," *Politico*, (15 de julho de 2021), https://www.politico.com/news/2021/07/15/biden-latin-america-crisis-499752.

12. Juan Delgado, "China, 5G e a ameaça à segurança na América Latina," *Diálogo Américas* (blog), (7 e março de 2023), https://dialogo-americas.com/articles/china-5g-and-the-security-threat-in-latin-america/.

13. Tisha Bhambry, "As principais previsões de segurança cibernética do Gartner para 2023 (APAC)," *Gartner Inc.*, (20 de março de 2023), https://www.gartner.com/en/webinar/462656.

14. BNamericas, "BNamericas - Como a Huawei está redobrando seus esforços na América Latina...," *BNamericas.com*, (23 de dezembro de 2021), https://www.bnamericas.com/en/features/how-huawei-is-doubling-down-on-latin-america-amid-global-headwinds.

15. William M. Leogrande, "Uma pobreza de imaginação: a política de George W. Bush na América Latina," *Journal of Latin American Studies* 39, no. 2, (Maio de 2007), 355–85, https://doi.org/10.1017/S0022216X07002416.

16. Piccone, "A geopolítica da ascensão da China na América Latina;" David Pion-Berlin e Harold Trinkunas, "Déficits de atenção: por que os políticos ignoram a política de defesa na América Latina," *Latin American Research Review* 42, no. 3, (2007), 76–100, https://www.jstor.org/stable/4499390.

17. Pion-Berlin and Trinkunas, "Défices de Atenção."

18. Jeff Abbott, "América Crece: o novo impulso de investimento de Washington na América Latina," *Toward Freedom*, (8 de outubro de 2020), https://towardfreedom.org/story/america-crece-washingtons-new-investment-push-in-latin-america/; Departamento de Estado, "Estados Unidos lançam programa America Crece (Crescimento nas Américas)," Embaixada dos EUA no Panamá, (18 de dezembro de 2019), https://pa.usembassy.gov/united-states-launches-america-crece-program-growth-in-the-americas/.

19. Departamento de Comércio, "Observações da Secretária de Comércio dos EUA, Gina M. Raimondo, 51º Conselho Anual das Américas de Washington (Virtual)," Departamento de Comércio dos EUA, (4 de maio de 2021), https://www.commerce.gov/news/speeches/2021/05/remarks-us-commerce-secretary-gina-m-raimondo-51st-annual-washington-council.

20. Câmara de Comércio, "Associação das Câmaras de Comércio Americanas na América Latina e no Caribe (AACCLA)," (12 de março de 2023), https://www.uschamber.com/program/international-affairs/americas/association-of-american-chambers-of-commerce-in-latin-america-and-the-caribbean-aaccla.

21. Comando Sul dos EUA (USSOUTHCOM), "Declaração do Estado do Exército de 2023 do SOUTHCOM ao Congresso."

22. Sean Choquette e Stephanie Urbano, "Superar a China na América Latina é uma prioridade de segurança nacional: uma perspetiva de líder sênior," *Journal of the Americas,* 4, no. 1, (2022), 173–84, https://www.airuniversity.af.edu/JOTA/Archives/.

23. Choquette and Urbano, "Outcompeting China in Latin America."

24. OAS, "Relatório da OEA examina tendências de segurança cibernética nas Américas," *OAS -Organization of American States*, (3 de maio de 2013), https://www.oas.org/en/media_center /press_release.asp?sCodigo=E-173/13.

25. NIST, "Estrutura de segurança cibernética," *NIST*, (12 de novembro de 2013), https:// www.nist.gov/cyberframework.

26. Heitor et al., "A América Latina pode avançar após uma década perdida em mudanças técnicas?"

27. Secureframe, "ISO 27001 vs NIST," Secureframe, (15 de março de 2023), https://secure frame.com/hub/iso-27001/vs-nist.

28. Mauricio Papaleo e Fabiana Santellán, "Perspectivas sobre a Estrutura," *NIST*, (6 de fevereiro de 2018), https://www.nist.gov/cyberframework/perspectives.

29. Amy Mahn, "NIST International Engagement Updates: Workshop de atualização do CSF 2.0 e muito mais," *NIST*, (30 de setembro de 2022), https://www.nist.gov/blogs/cybersecurity -insights/nist-international-engagement-updates-csf-20-update-workshop-and-more.

30. Mahn, "NIST International Engagement Updates."

31. William Dunway, "Sistemas Ciber-Físicos/Internet das Coisas para Cidades Inteligentes," *NIST*, (9 de abril de 2022), https://www.nist.gov/programs-projects/cyber-physical-systemsinternet-things -smart-cities.

32. IAAFA, "Catálogo de Cursos IAAFA 2023," *IAAFA Main Page*, (15 de março de 2023), https://www.37trw.af.mil/Portals/57/IAAFA%20Page%20photos/2023%20IAAFA%20 Course%20Catalog%20(English)%20(XP%20Edits).pdf.

33. Choquette e Urbano, "Superar a China na América Latina é uma prioridade de segurança nacional: uma perspetiva de líder sênior."

34. Richard L. Manley, "Cyber nas sombras: por que o futuro das operações cibernéticas será secreto," *National Defense University Press*, 3rd qtr, no. 106, (2022), p. 4–10, https://ndupress.ndu .edu/Media/News/.

35. Amy McCullough, "USAF lança nova doutrina de poder aéreo," *Air & Space Forces Magazine* (blog), (22 April 2021), https://www.airandspaceforces.com/usaf-releases-new-airpower -doctrine/; USAF, "Publicação 1 da Doutrina da Força Aérea," *USAF*, (10 de março de 2021), https://www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP%201%20The%20Air%20 Force%20Pocket%20Size%20Booklet.pdf.

36. Mikala McCurry, "AFCLC fornece suporte linguístico para missões DoD," *Air Force News*, (28 de setembro de 2021), https://www.af.mil/News/Article-Display/Article/2791349/afclc -provides-language-support-to-dod-missions/https%3A%2F%2Fwww.af .mil%2FNews%2FArticle-Display%2FArticle%2F2791349%2Fafclc-provides-language -support-to-dod-missions%2F.

37. Air Force News Service, "CSAF divulga ordens de ação para acelerar mudanças em toda a Força Aérea," *Air Force*, (10 de dezembro de 2020), https://www.af.mil/News/Article-Display /Article/2442546/csaf-releases-action-orders-to-accelerate-change-across-air-force /https%3A%2F%2Fwww.af.mil%2FNews%2FArticle-Display%2FArticle%2F2442546%2Fcsaf -releases-action-orders-to-accelerate-change-across-air-force%2F.

38. OTAN, "Relações com a Colômbia," *OTAN*, (17 de junho de 2021), https://www.nato.int/cps/en/natohq/topics_143936.htm.

39. CyberScoop, "Grupo de hackers focado na América Central despeja 10 terabytes de e-mails e arquivos militares," *CyberScoop* (blog), (19 de setembro de 2022), https://cyberscoop.com/central-american-hacking-group-releases-emails/; Fox News Corp., "Hackers 'Black Hat' no Peru têm como alvo ministros do governo, abalando o gabinete", *Fox News*, (28 de dezembro de 2016), https://www.foxnews.com/world/black-hat-hackers-in-peru-target-government-ministers-rattling-the-cabinet.

40. Curtis A. Ward, "Ameaças regionais: imperativos de capacidade de segurança no Baribe," *National Defense University Press*, 3rd qtr, no. 58, (2010), p. 26–31, https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-58.pdf.

41. Kirk Semple, "China amplia alcance no Caribe, perturbando os EUA," *The New York Times*, (8 de novembro de 2020), https://www.nytimes.com/2020/11/08/world/americas/china-caribbean.html.

42. Evan Ellis e Leland Lazarus, "Resoluções de Ano Novo da China para a América Latina e o Caribe," *The Diplomat*, (12 de janeiro de 2022), https://thediplomat.com/2022/01/chinas-new-year-ambitions-for-latin-america-and-the-caribbean/.

43. Tisha Bhambry, "As principais previsões de cibersegurança da Gartner para 2023 (APAC)."

44. Ciara Nugent e Charlie Campell, "Os EUA e a China estão lutando por influência na América Latina, e a pandemia aumentou a complexidade dos desafios," *Time*, (4 de fevereiro de 2021), https://time.com/5936037/us-china-latin-america-influence/.

45. Departamento de Segurança Interna, "DHS alerta empresas americanas sobre serviços e equipamentos de dados de empresas ligadas ao governo chinês | Segurança Interna," *Departamento de Segurança Interna do Governo*, (22 de dezembro de 2020), https://www.dhs.gov/news/2020/12/22/dhs-warns-american-businesses-about-data-services-and-equipment-firms-linked-chinese.

46. Ciara Nugent e Charlie Campell, "Os EUA e a China estão lutando por influência na América Latina, e a pandemia aumentou a complexidade dos desafios," *Time*, (4 de fevereiro de 2021), https://time.com/5936037/us-china-latin-america-influence/.

47. Abdi Latif Dahir, "A China "presenteou" a União Africana com um edifício-sede e depois mandou grampeá-lo," *Quartz*, (30 de janeiro de 2018), https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/; Mailyn Fidler, "União Africana grampeada pela China: Ciberespionagem como prova de mudanças estratégicas," *Council on Foreign Relations*, (7 de março de 2018), https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

48. Evan Ellis, "O avanço digital da China na América Latina," *Diálogo Américas* (blog), (7 de julho de 2022, https://dialogo-americas.com/articles/chinas-digital-advance-in-latin-america/; Greg Myre, "A China quer seus dados — e já pode tê-los," *NPR*, (24 de fevereiro de 2021), sec. Segurança Nacional, https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it.

49. Jonathan E. Hillman e Maesea McCalpin, "Observando as 'Cidades Seguras' da Huawei,'" (4 de novembro de 2019), https://www.csis.org/analysis/watching-huaweis-safe-cities.

50. Myre, "A China quer seus dados — e já pode tê-los;" "Pressão da China para controlar o futuro da saúde dos americanos," *60 Minutes*, (31 de janeiro de 2021), https://www.cbsnews.com/news/biodata-dna-china-collection-60-minutes-2021-01-31/.

51. Choquette e Urbano, "Superar a China na América Latina é uma prioridade de segurança nacional: uma perspetiva de líder sênior."

52. Shannon O'Neil, "Por que a América Latina perdeu com a globalização — e como ela pode vencer agora," *Council on Foreign Relations*, (25 de agosto de 2022), https://www.cfr.org/article/why-latin-america-lost-globalization-and-how-it-can-win-now.

Coronel James Hamilton, USAF

Atualmente serve como Diretor de Ciberespaço e Comunicações da 12ª Força Aérea (AFSOUTH), Davis-Monthan AFB, Arizona. Ele lidera todos os aspectos de comunicações e planejamento cibernético para apoiar diretamente os compromissos do USSOUTHCOM com as nações parceiras como especialista em assuntos cibernéticos do componente aéreo. Ele tem mestrado em Ciências Aeronáuticas pela Embry-Riddle e um doutorado em liderança estratégica pela Liberty University, onde examinou o apoio do líder sênior da Força Aérea dos EUA à comunidade conjunta. Mais recentemente, ele serviu 5 anos na sede da OTAN em Bruxelas, Bélgica, no Estado-Maior Internacional como seu Gerente de Informação e Conhecimento e, em seguida, em Mons, Bélgica, no Estado-Maior do Grupo de Comunicações e Sistemas de Informação como Chefe da Divisão de Operações responsável pelas comunicações e interoperabilidade destacáveis em todo o teatro.

Capitão Valdir Ruiz, USAF

Atualmente serve como Oficial Responsável pela Cooperação em Segurança do Ciberespaço da 12ª Diretoria de Comunicações da Força Aérea (AFSOUTH). Em sua função, ele lidera o planejamento e a execução de operações, atividades e investimentos centrados em Cibersegurança e Defesa Cibernética e coordena os requisitos entre os intervenientes nacionais e internacionais. Ele é um oficial de Operações de Comunicações de Combatentes, e possui bacharelado em Ciências em Cibersegurança e um Mestrado em Tecnologia de Cibersegurança. O capitão Ruiz possui cidadania equatoriana e uruguaia, e viveu no Equador durante a sua educação de primeiro e segundo graus. Ele é um estudioso do *Language Enabled Airmen Program* da USAF.