Empleo de competencia cibernética estratégica en Latinoamérica

Una misión para un líder cibernético superior

Coronel James Hamilton, USAF
Capitán Valdir Ruiz, USAF

Introducción

Los Estados Unidos de América (EUA) están cambiando rápidamente su enfoque para Latinoamérica y el Caribe (LAC), demostrado directamente por el mayor apoyo del congreso al Comando Sur de EUA (USSOUTHCOM, por sus siglas en inglés). Por extensión, las Fuerzas Aéreas del Sur (AFSOUTH, por sus siglas en inglés), a través de su Dirección de Comunicaciones (A6), está aunando esfuerzos con la división de operaciones cibernéticas (J38) de USSOUTHCOM para afectar las actividades del Departamento de Defensa (DoD, por sus siglas en inglés) en un enfoque de todo el gobierno sobre el teatro de operaciones. Así pues, las AFSOUTH están tratando de aumentar el intercambio de información con las naciones de LAC con el fin de hacer avanzar la conciencia y la capacidad cibernéticas dentro del teatro de operaciones del sur. Este nuevo enfoque plantea oportunidades y retos dentro del dominio cibernético. Este artículo tratará con dos de estos retos. En primer lugar, a la luz de una falta real de conocimientos de las amenazas cibernéticas, la supuestamente ventajosa inversión de China está siendo aceptada por los países de LAC como un intercambio justo. Sin embargo, es necesario hacer un análisis de costos y beneficios que yuxtapone la soberanía de la nación-estado y el avance tecnológico para ayudar a las naciones de LAC a entender los riesgos de la seguridad cibernética asociados con dicho intercambio. En segundo lugar, una evaluación cibernética completa, basada en el Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), ayudaría a las diversas agencias o departamentos gubernamentales de EUA a contrarrestar la influencia china, apoyando al final a los países asociados a tomar decisiones bien informadas como parte de su cálculo nacional de seguridad cibernética. Una evaluación cibernética completa permite al DoD adaptar las ofertas de educación y los objetivos de los ejercicios de coalición, haciendo corresponder actividades con niveles de desarrollo de los socios en todo el hemisferio sur, resultando en una buena metodología cibernética que realmente haga progresar las capacidades de los socios.

Un nuevo enfoque

El comandante de USSOUTHCOM, la General Laura J. Richardson, testificó recientemente ante el congreso y habló de la postura del USSOUTHCOM, identificando tres líneas principales de esfuerzo, específicamente: "fortalecer alianzas y asociaciones, contrarrestar amenazas y construir nuestro equipo".[1] La General Richardson resaltó varias áreas de concentración en su testimonio, pero este artículo se concentrará en la influencia china y rusa en la región y explicará por qué la defensa y la industria de EUA deben ser los socios de LAC elegidos para la cooperación en materia de seguridad cibernética; además, tratará la necesidad de una aplicación y un adiestramiento cibernéticos mayores.[2]

Más recientemente, Matt Ferchen observó que existe una fricción de competición estratégica ente EUA y China y que está expandiéndose por la región.[3] Por ejemplo, Honduras pivotó recientemente hacia China, alejándose de Taiwán, para abrirse más a las opciones de comercio y financiación chinas.[4] Además, Honduras se abstuvo previamente de la resolución de las Naciones Unidas que condenaba la invasión rusa de Ucrania.[5] Estas acciones se corresponden con el avance de Rusia y China en la región, facilitando a Rusia el aprovechamiento de su estado provisional en LAC y contribuyendo directamente a la Iniciativa de la Franja y la Ruta (BRI, por sus siglas en inglés) de China.[6] Parte de la influencia de China incluye avance tecnológico y no se limita a préstamos ni proyectos de represas hidroeléctricas. Ferchen habla de la 'Ruta Digital de la Seda', mostrando un cable de fibra óptica que conecta Brasil con África, financiado en su mayor parte por compañías chinas. Se puede inferir que la asociación de LAC con compañías chinas, posiblemente derivada de las restricciones presupuestarias (como en el caso de Honduras) o la falta de entendimiento acerca de la defensa cibernética, pone en cuestión la sagacidad técnica de LAC, como en el ensayo de 2014 de Manuel Heitor y otros, titulado: ¿"Puede Latinoamérica avanzar después de un decenio perdido en cambios técnicos?", pronosticó.[7]

Aunque LAC ha venido progresando constantemente hacia el uso del dominio cibernético, se ha convertido en un campo complejo que los gobiernos se apresuran a entender, defender, actualizar y en los que maniobrar. Áreas como computación en la nube, confianza cero, configuración de servicio de nombre de dominio e higiene cibernética son fundamentales para los profesionales cibernéticos. Estas áreas se pueden usar para desarrollar una relación de confianza y alternativas de confianza, que nos llevan hacia un mayor esfuerzo de EUA-LAC para aumentar la participación y la educación cibernética en el hemisferio. El avance de China no es nuevo; su BRI ha aumentado constantemente en unos años, pero hay nuevas indicaciones que sugieren que la BRI puede estar en declive o avanzando con un

apodo diferente, es decir, la Iniciativa de Desarrollo Global.[8] No obstante, trata de conseguir ventajas en las operaciones del espacio y de la información.[9] Se estima que la competencia en el teatro de operaciones de LAC no es simplemente consecuencia de una expansión regional de China, sino que se ha reforzado también por el enfoque de EUA en el Medio Oriente y la falta de atención en Sudamérica, según lo describió el ensayo EUA-Afganistán de 2015 de Larry P. Goodson.[10] Aparentemente, EUA ofreció menos participaciones e inversiones a nuestros socios regionales durante un tiempo prolongado, permitiendo así que China y Rusia entraran a hurtadillas.[11]

Así pues, ¿por qué no ha avanzado más EUA a la luz de sus esfuerzos reenfocados en educación y defensa cibernéticas para LAC? Un artículo de BNamericas sobre la compañía de telecomunicaciones Huawei constituye un ejemplo de la rapidez con la que creció China en los últimos diez años; la compañía es una fuerza dentro de LAC, y está presente en escuelas y universidades (90 en Brasil solamente), redes móviles 5G,[12] computación en la nube por medio de su solución CloudCampus 3.0,[13] routers, interruptores informáticos y otras inversiones, de las que mantienen aproximadamente un porcentaje del 50%-80% del mercado en varios países.[14] En otra palabras, se produjo una fricción progresiva durante años entre EUA y LAC, derivada posiblemente del enfoque de EUA en el Medio Oriente[15] y su interacción discontinua con LAC,[16] combinada con la política de defensa EUA-LAC que se concentraba más en funciones de operación y apoyo de los socios para combatir el narcotráfico y frustrar el terrorismo y las amenazas externas,[17] contribuyendo todo ello a una relación discontinua en la región que hizo que China rellenara el brecha hueco dejado.

Recuperación de la ventaja

Desde que los chinos han tratado de hacer avanzar el comercio, proyectos y préstamos dentro de LAC, el Departamento de Estado ha actuado para contrarrestar las maniobras de China con la divulgación del 18 de diciembre de 2019 del esfuerzo América Crece, como un enfoque de todo el gobierno para fomentar un desarrollo económico deliberado en el hemisferio.[18] Desde esa época, otras agencias gubernamentales iniciaron su propia defensa hacia la asociación de LAC, como la inclusión del Departamento de Comercio en el 51º Consejo Anual de las Américas de Washington, donde exigieron mayores vínculos y mayor cooperación.[19] Igualmente, los congresos y actividades de la Asociación de Cámaras de Comercio Americanas de Latinoamérica y el Caribe contribuyeron a la inversión en LAC.[20] Estos esfuerzos presagiaron la declaración de la postura de la General Richardson y trataron de combinar las organizaciones gubernamentales e

industriales para contribuir al enfoque de todo el gobierno como una alternativa a la influencia de China y Rusia.[21]

AFSOUTH como socio

En su ensayo sobre cómo superar a China, el subcomandante de las AFSOUTH, el General de Brigada Sean Choquette, describió líneas de esfuerzo de componentes aéreos en apoyo al USSOUTHCOM, nombrando el dominio cibernético como un área de enfoque concentrada en el teatro de operaciones de LAC.[22] Como línea de esfuerzo, el dominio cibernético actúa como un Área de Interés (AOI) dentro del área de responsabilidad (AOR, por sus siglas en inglés) de las AFSOUTH. El General Choquette abogó por el intercambio de información y la colaboración en cibernética así como en llamar a Expertos en el Asunto (SME, por sus siglas en inglés) de las AFSOUTH para educar a los socios que abarcaran seguridad cibernética y de infraestructuras.[23] Para hacer realidad estos objetivos estratégicos, la A6 de las AFSOUTH coordinará con J38 del USSOUTHCOM en la unión de las fuerzas diplomáticas y militares del teatro de operaciones de LAC para identificar y emplear Medidas de Rendimiento (MOP, por sus siglas en inglés) y Medidas de Efectividad (MOE) mediante procesos de planificación conjuntos deliberados. La A6 actuará para liderar y apoyar colectivamente los Intercambios cibernéticos de SME (SMEE, por sus siglas en inglés) con sus socios de países, el NIST y entidades académicas para estimular el desarrollo cibernético hacia una pendiente ascendente para hacer avanzar la conciencia y la capacidad cibernéticas. Para facilitar este desarrollo, hay tres áreas de capacidad cibernética específicas que se deben desarrollar: normalización, educación y empleo, que están vinculadas a líneas de esfuerzo del USSOUTHCOM respectivas.

Evaluación y normalización del dominio cibernético

El gran entrenador de béisbol de EUA, Yogi Berra, dijo una vez: "Si no sabes adónde vas, podrías acabar en otro sitio". El secretario de estado Henry Kissinger declaró de forma más estoica: "Si no sabes a dónde vas, cada camino te llevará a ningún sitio". En términos rudimentarios, EUA necesita entender las capacidades cibernéticas en los 31 países asociados del AOR. A medida que nuestros vecinos latinoamericanos enfrentan su propia complejidad cibernética, retos como los cambios políticos pendulares, el derecho a comerciar con exportadores de todo el mundo y las diferencias regionales causan distracciones en el dominio cibernético. Como los 31 socios poseen varios niveles de desarrollo cibernético, ¿qué norma debe usarse para crear una capacidad de seguridad cibernética cohesiva y robusta en el AOR? Hacer que los 31 socios practiquen al mismo nivel de desarrollo

cibernético al mismo tiempo no es realista; el verdadero desarrollo cibernético tarda años en producirse. Por ejemplo, la Organización de los Estados Americanos trató de reunir a sus miembros para lograr una conciencia cibernética mediante un informe conjunto divulgado en 2013 que examinaba tendencias de seguridad cibernética,[24] pero hubo una participación colectiva limitada de LAC, que frustró el impulso. Por lo tanto, las AFSOUTH animan y abogan por adoptar el modelo de estructura de seguridad cibernética (CSF, por sus siglas en inglés) del NIST.[25] La CSF del NIST está diseñada para funcionar con las instituciones de todo el gobierno de EUA por medio de subvenciones federales de EUA, y cadenas de suministro de agencias federales de EUA. Heitor y otros, abogaban por esta ruta de seguridad al afirmar que, "[e]ste es un programa de la máxima [sic] importancia y relevancia que ha ayudado a crecer a las compañías innovadoras de EUA";[26] esto viene de una perspectiva de LAC interna, ya que estos investigadores eran nativos de Portugal, México, Brasil y Chile.

Cabe destacar que la CSF del NIST usa partes de la norma ISO 27001, pero mientras que ISO 27001 es una norma internacional, no es un requisito legal para áreas de negocios específicas, a diferencia de las estructuras de evaluación de riesgos como la CSF del NIST, la GDPR y la HIPAA.[27] LAC ya tiene un punto inicial; la Agencia para el Gobierno Electrónico y la Sociedad de Información de Uruguay ya ha adoptado el modelo de nivel 5 de la CSF del NIST y es miembro de las *naciones digitales* (una red de colaboración de los gobiernos de liderazgo digital del mundo) desde 2018, usando la CSF del NIST como mapa de ruta.[28] Los representantes del NIST también han viajado a Colombia y Brasil para hablar de las normas del NIST para la industria, los mercados y la adopción de un gobierno inteligente en comercio y defensa.[29] Una vez que estemos de acuerdo en una norma común, podemos empezar a recorrer un camino común. Mediante un modelo de evaluación cibernética ubicuo, se puede evaluar, entender y construir el desarrollo cibernético de los socios. A6, mediante el uso de operaciones, actividades e inversiones (OAI, por sus siglas en inglés) cibernéticas de las AFSOUTH, sincronizará esfuerzos para tejer el plan de apoyo de la campaña del teatro de operaciones del USSOUTHCOM para la conciencia del dominio en participaciones de OAI para rellenar huecos de defensa cibernética. Las MOP y las MOE desarrolladas de forma deliberada medirán después el progreso utilizando una línea de referencia de la CSF del NIST como punto de referencia, reutilizándola de forma iterativa como indicador de desarrollo, además de actuar como un léxico cibernético común dentro y en todo el teatro de operaciones de LAC.[30]

Educación

La educación se produce en todos los niveles de OAI. De hecho, las OAI ofrecen enfoques flexibles de empleo cibernético durante la interacción EUA-LAC; por ejemplo, las Participaciones de Líderes Clave (KLE, por sus siglas en inglés) dan resultado a un nivel entre líderes superiores para introducir y reforzar las mejores prácticas, en este caso las prácticas cibernéticas. Los líderes militares de EUA ofrecen sus puntos de vista sobre cómo el DoD se desarrolló a través de su capacidad cibernética hasta un nivel estratégico. Igualmente, los SMEE fomentan un diálogo experto, que da que pensar y una participación basada en aplicaciones, como la inteligencia y los SMEE cibernéticos llevados a cabo en Chile vistos en la Figura 1. Los SMEE permiten a los individuos dentro del AOI del dominio cibernético aportar ideas colectivamente a problemas y resoluciones. Cuando los expertos cibernéticos intercambian ideas, se pueden emplear las mejores prácticas de forma rápida, frustrando la intrusión en redes y vectores de amenazas múltiples. El intercambio de ideas debe comprender también áreas como evaluaciones cibernéticas, objetivos de ejercicios, congresos y adiestramiento cibernético formal.

Figura 1. EUA Fuerzas Cibernéticas / SMEE de inteligencia y cibernéticos, representante de la A6, Capitán Jefferson en Chile

Fuente: Autores

Evaluaciones

La J38 del USSOUTHCOM y la A6 de las AFSOUTH se asocian para ejecutar Equipos de Asistencia Cibernética Conjunta de Combatientes-Comandos (JCCAT, por sus siglas en inglés). Los JCCAT operan a petición de un socio de LAC, permitiendo a los expertos evaluar las políticas, los procedimientos y las prácticas de las redes cibernéticas. Los JCCAT actúan como los SMEE, pero se diferencian en la aplicación inmediata de la evaluación; estos equipos pequeños usan sus conocimientos tácitos para trabajar con países asociados a fin de analizar un acto de piratería de una red o amenazas de programas malignos de sistemas y detectar el impacto de esa amenaza. Idealmente, los JCCAT se producen antes de una amenaza, para identificar vulnerabilidades, pero sea cual sea la necesidad o el momento, EUA desea colaborar antes y después de la evaluación para educar a equipos profesionales cibernéticos similares.

Ejercicios

Existen ejercicios para probar las fuerzas militares, permitiendo que esas fuerzas aprendan de sus errores; y un análisis crítico durante informes después de acciones permiten entender el ciclo de toma de decisiones. Así, para ser efectivas, las acciones en el campo necesitan estar vinculadas de forma deliberada en una metodología causa y efecto. Históricamente, no se trazó ninguna línea por las fases de planificación de múltiples años de ejercicios para determinar MOE. La intención de la A6 de las AFSOUTH es usar ahora un enfoque deliberado, escalonado y mensurable hacia las OAI que fomenten el desarrollo cibernético. En pocas palabras, la evaluación, la enseñanza, las pruebas, la medición y el ajuste son los puntos decisivos hacia el desarrollo cibernético y los ejercicios de naciones asociadas utilizarán estas destrezas.

Congresos

LAC es anfitrión de algunos de los mejores congresos técnicos del mundo. La asistencia a congresos no solo educa a nivel académico, sino que refuerza conversaciones aparte sobre la presentación formal de prácticas cibernéticas. El COVID-19 hizo añicos la asistencia a congresos y ahora estamos superando el déficit de intercambio de ideas. Para liderar en este espacio, la A6 asistió a varios congresos de LAC para relacionarse con sus homólogos y los resultados son muyprometedores. No obstante, eso significa que EUA debe acoger también congresos de conciencia cibernética.

Por lo tanto, la A6 está trabajando para ser anfitriona de socios de LAC con el fin de participar en una conversación conjunta de tecnología cibernética y de la

información de LAC en el evento ACE de Alamo de la Asociación de Comunicaciones y Electrónica de las Fuerzas Armadas (AFCEA, por sus siglas en inglés) en San Antonio, Tejas. La capacidad de los profesionales de la industria, así como de soldados, fusileros de marina, guardacostas y aerotécnicos para oír cuáles son los retos y avances en capacidades cibernéticas de nuestros socios de LAC fomenta el entendimiento y el apoyo de la comunidad, y simplemente podría resolver algunos problemas en apoyo de intereses compartidos. Las AFSOUTH están muy interesadas en el foro de AFCEA y tratan de hacer que se convierta en un evento recurrente.

La educación integrada a través de congresos internacionales también aclara a los participantes cuáles son las mejores prácticas, la normalización y los riesgos de la industria. El NIST es un ejemplo de cooperación programática donde se habla de ciudades Seguras/Inteligentes. El NIST advierte que esta tecnología, si se implementa mal, podría ser una amenaza contra la privacidad y la seguridad personales, pero si se hace a través de una colaboración industrial de múltiples naciones, podría aportar interoperabilidad según las normas del Comité Técnico Conjunto de ISO/IEC.[31]

Adiestramiento militar formal

El adiestramiento formal puede ser de muchas formas. La General Richardson promovió la Academia de la Fuerza Aérea Interamericana (IAAFA, por sus siglas en inglés) en la estrategia del USSOUTHCOM como un mecanismo para la educación y la colaboración militares profesionales. Para aprovechar este vehículo de habla en español, la A6 de las AFSOUTH se asoció con la IAAFA para establecer un nuevo curso de operaciones de defensa cibernética conmensurable con las capacidades de nuestro país.[32] Este curso tiene como objetivo nuestras fuerzas alistadas; su educación es clave para una disuasión efectiva, especialmente en lo que se relaciona con la cibernética. Para llevar adelante ese concepto, la A6 está trabajando con la IAAFA y la Universidad de Defensa Nacional, para emplear un curso de cibernética estratégica de líderes superiores que infunda a los líderes de las naciones un entendimiento de la defensa cibernética, permitiéndoles tomar decisiones de defensa críticas sobre compras, instalación y mantenimiento de sus redes militares.

Si EUA y LAC se proponen a avanzar hacia una interoperabilidad coherente, entonces el estado final es trabajar con los 31 socios hacia su propio desarrollo mediante diversos medios. El enfoque de las AFSOUTH combina la planificación de operaciones conjuntas y aéreas con ejercicios. Como tal, se pasa de forma deliberada desde una estructura de gestión de riesgos cibernéticos normalizada, mediante educación y SMEE, hasta una conciencia cibernética y una capacidad

defensiva. Este objetivo está respaldado por la asistencia a congresos y un adiestramiento formal; en ese caso la culminación debe ser la participación y el empleo de ejercicios haciendo uso de esas experiencias. Esto mejora las asociaciones de seguridad que actúan para vincular las acciones cibernéticas y crear un entendimiento robusto de defensa cibernética, de modo que las AFSOUTH puedan ayudar a satisfacer los objetivos de desarrollo de los socios.[33]

Empleo

Richard L. Manley, en su artículo de Joint Force Quarterly, propuso que las futuras operaciones cibernéticas se producirán en las sombras, efectivamente en el área gris, para evitar una guerra a gran escala o un conflicto armado.[34] También afirmó que tanto China como Rusia ya operan en esta área; China específicamente navega sin restricciones, combinando los elementos de poder nacional, Diplomacia, Información, Fuerzas Armadas y Economía (DIME, por sus siglas en inglés), para dictar su agenda. Si LAC no reconoce que China tiene una agenda, entonces los socios de LAC inevitable y sistemáticamente renuncian a su soberanía nacional mediante todas las compras y acuerdos cibernéticos.

Para contrarrestar las fuerzas chinas y rusas, la utilización de doctrina publicada recientemente de la Fuerza Aérea de EUA (USAF, por sus siglas en inglés) ofrece de inmediato una estructura para la defensa y el avance de la conciencia y capacidad cibernéticas. Las fuerzas amigas pueden emplear el principio de *Persistencia*, que "niega a un adversario la oportunidad de tomar la iniciativa o lograr directamente las tareas asignadas", y combinar con *Flexibilidad* y *Versatilidad*, lo que permite que el "poder aéreo logre una sinergia mediante operaciones asimétricas y paralelas".[35]

Las acciones que respaldan estos principios estimulan la capacidad inherente para superar barreras culturales y lingüísticas. Uno de esos ejemplos es aprovechar la relación formal que existe con el Buró de la Guardia Nacional (NGB, por sus siglas en inglés) a medida que lleva a cabo el Programa de Asociación de Estados (SPP, por sus siglas en inglés), que empareja unidades aéreas y del ejército de la Guardia Nacional con países de LAC. La A6 trata de sacar ventaja de intercambios que ya ocurren entre asociaciones NGB-LAC para maximizar las asociaciones. Idealmente, si un SPP opera dentro de un AOI cibernética, como llevar a cabo un ejercicio militar o lanzar un SMEE, entonces la A6 estaría también en ese equipo. Por ejemplo, en 2021, la A6 de las AFSOUTH lideró y ejecutó tres eventos cibernéticos y apoyó al JCCAT. Después, en 2022, la A6 lideró tres de sus participaciones cibernéticas por primera vez en persona, todas las cuales se basaban en el apoyo de proveedores de fuerzas conseguidos de la USAF, de la Fuerza Espacial y del NGB.

Para cruzar la barrera lingüística externa, la A6 de AFSOUTH se puso en contacto con expertos cibernéticos con capacidad de idiomas de varias organizaciones, incluida la IAAFA y el Centro de Cultura e Idiomas (AFCLC, por sus siglas en inglés) de la USAF, que gestiona el Programa de Aerotécnicos con Capacidad de Idiomas (LEAP, por sus siglas en inglés). El LEAP es un multiplicador de fuerzas, ya que su función es desarrollar de forma deliberada aerotécnicos con capacidad de idiomas de diversas culturas con conocimiento, a nivel de trabajo, de otras lenguas para apoyar directamente el poder aéreo, lo cual fortalece las asociaciones y la interoperabilidad.[36] Las naciones asociadas, al operar internamente en el teatro de operaciones de LAC, a menudo disponen de un Oficial de Cooperación de Seguridad (SCO, por sus siglas en inglés) asignado para identificar y proyectar las OAI y adiestramiento para su país respectivo. Los SCO proporcionan datos referentes a OAI ejecutados recientemente que pueden incluir una evaluación abreviada del estado de capacidad cibernética actual de sus países.

Cabe destacar que los SCO alientan a los componentes de servicio a trabajar juntos para llevar a cabo eventos de seguridad cibernética, en vez de ejecutar eventos específicos de servicio, para reducir aislamientos o flujos restringidos centrados en componentes. Esta defensa está bien situada, ya que algunos ministros de defensa de LAC nombran componentes de servicio específicos como guías de operación para llevar a cabo operaciones ciberespaciales, ya que es posible que no estén concentradas en la simetría de componentes conjuntos. Así pues, lograr la paridad con países asociados puede ofrecer un reto, ya que es posible que su estructura de fuerza no coincida con la estructura de la fuerza cibernética de EUA, pero la flexibilidad en cooperación ayuda a superar diferencias en construcciones de fuerzas conjuntas asociadas dispares. Mientras que EUA trabaja para optimizar su propia integración en un esfuerzo coordinado, también debe alentar la colaboración conjunta entre socios de LAC para conseguir una defensa cibernética exitosa. Por ejemplo, durante dos diferentes SMEE de socios en 2022, las AFSOUTH probaron planes cibernéticos conjuntos, demostrando que estas participaciones podrían ser satisfactorias y productivas cuando se apartan las barreras de comunicación, con ramas militares participando abiertamente e intercambiando información.

Para fomentar nuestra conectividad de LAC, debemos seguir la llamada a la acción del Jefe de Estado Mayor de la USAF, el General Charles Q. Brown, Jr., y "Acelerar el cambio o perder" para participar en la competencia estratégica que se describe en su reto.[37] Para facilitar este reto, las AFSOUTH necesitarán encontrar nuevas formas de reclutar expertos técnicos con capacidad de idiomas para llevar a cabo participaciones, evaluaciones y adiestramiento. Una posibilidad es buscar proveedores de fuerza de todos los teatros de operaciones y comandos, utilizando

el potencial sin explotar de los aerotécnicos para aumentar las OAI de cooperación de seguridad cibernética en el USSOUTHCOM.

El camino adelante

Las AFSOUTH están planeando ejecutar tres SMEE en el año fiscal 2023 y está refinando conceptos para eventos propuestos para el año fiscal 2024 a fin de hacer avanzar la conciencia y la capacidad cibernéticas. En el año fiscal 2024, la A6 de las AFSOUTH amplificarán su alcance y duplicará su número de OAI a aproximadamente 12. Las AFSOUTH reconocen que mientras que es importante mantener relaciones con socios estratégicos grandes, también formará y mantendrá relaciones con países más chicos en el AOR de las USSOUTHCOM. Esto nos permitirá encontrar nuevas formas de identificar y asignar recursos, financiación y personal, y requerirá creatividad, así como conocimientos de autoridades de financiamiento bajo las que opera la cooperación de seguridad de EUA. La creación de nuevos eventos será difícil, pero suministrará la ventaja necesaria para competir estratégicamente con China y Rusia en el dominio cibernético.

El camino adelante para fortalecer y hacer avanzar la conciencia y la capacidad cibernéticas es crear escenarios basados en táctica que requieran que las fuerzas militares maniobren a través de objetivos de ejercicios y la fricción que tienen la intención de crear. Por ejemplo, alterar una red de radio, introduciendo un efecto de red de rechazo de servicio, o estimular una amenaza interna durante un ejercicio permite a los planificadores, líderes y fuerzas militares pensar de forma crítica en una forma conjunta y de coalición para mitigar la amenaza.

Esta ruta ya tiene precedente, como en el caso de Colombia al convertirse en una nación que no es de OTAN como socio global en 2018. Reconocieron la necesidad de sincronizar y normalizar su postura de defensa con otras naciones, por lo que trataron de convertirse en un líder de LAC en adiestramiento y defensa cibernética.[38] A medida que avanzamos, Colombia ejercita y es anfitriona de foros académicos para adiestrar y probar su capacidad cibernética.

El costo de la falta de acción

Los accesos ilegales, los ataques y las vulnerabilidades cibernéticas se producen repetidamente, según se ha visto en el último ataque informático contra Perú, Chile, México, El Salvador y Colombia, y continúan con impunidad.[39] No es una sorpresa que, en el ensayo de 2010 de Curtis A. Ward en Joint Forces Quarterly, se hablara de la necesidad del Caribe de iniciar una acción preventiva para sus intereses de seguridad nacional y económicos regionales.[40] Aunque se ha progresado, también ha habido un avance de China en la región caribeña,[41] donde China

ha llegado a crear una mapa de ruta para el avance durante el Foro China-Comunidad de Estados Latinoamericanos y del Caribe (CELAC, por sus siglas en inglés).[42] Una de las áreas identificadas para la expansión incluye un foro de ciencia, tecnología e innovación de China-CELAC. ¿Por qué nos debemos preocupar por esto? Investigaciones recientes de Gartner Inc. resaltaron que Huawei poseerá una presencia significativa en el *Espacio de contrafuegos cibernéticos* y sigue desarrollando capacidad de inteligencia artificial (AI, por sus siglas en inglés) y aprendizaje de máquina, atribuida parcialmente por su modelo de precios atractivos.[43] No obstante, eso acelera el atrincheramiento de China en LAC con compañías "tecnológicas de establecimiento de normas como Huawei, ZTE, Dahua y Hikvision–todas ellas sancionadas por EUA-en infraestructura regional, permitiendo a Beijing dictar las reglas de comercios durante una generación".[44]

Estos líderes chinos de la industria tecnológica usan su participación en el mercado y sus conocimientos expertos para exfiltrar datos, según la ley china, de los países anfitriones que instalan sus equipos.[45] LAC ha reforzado, sin saber, la expansión china a través de contratos de infraestructura que puede tener resultados negativos para la seguridad cibernética de una nación, ya que se ha considerado que estos contratos son "depredadores" al ser analizados.[46] Un ejemplo es el caso de exfiltración de datos de la sede de la Unión Africana que se produjo en un período de múltiples años, sirviendo como testigo de los efectos de los contratos chinos en acción.[47] Un ejemplo adicional de instalación de tecnología de la información es la integración de *ciudades seguras*, con el pretexto de la seguridad y la reducción de la delincuencia, que reúne datos biométricos en poblaciones de países anfitriones[48] mientras bloquea a la nación anfitriona en contratos de reemplazo legales.[49] La sincronización y el aprovechamiento de agentes honrados de la industria cibernética y de comunicaciones para ofrecer software y equipos basados en valores para la comunidad de LAC, aunque a menudo a mayores costos, aseguraría ciertamente una postura de defensa soberana en la región de LAC.

Hay indicios abundantes de actividades chinas perversas y de piratas informáticos rusos y se ramifican en áreas que a menudo se consideran que son benignas. Los hospitales o laboratorios biomédicos que patrocina China, o las pruebas de vacunas que ofrecen, ayudan a exfiltrar ADN de la población anfitriona para reunir datos directamente que contribuyen al control de enfermedades y a la mercadotecnia de China.[50] Cada paso adelante lento y deliberado chino es un paso que no pueden dar EUA y sus socios de LAC, ya que China reúne lentamente datos y gana poder blando para asegurarse una posición de AOR y capacidad de maniobra.

En resumen

El USSOUTHCOM nombró a las AFSOUTH como líder de innovación del comando. Además, el General Choquette pidió un mayor intercambio de información entre las acciones de las AFSOUTH y LAC.[51] En consecuencia, la A6 está respondiendo a esas llamadas para hacer avanzar la conciencia y las capacidades cibernéticas internacionales en el teatro sur de operaciones. Esto se hará mediante un enfoque deliberado de normalización, educación y empleo de procesos y procedimientos. La facilitación de operaciones cibernéticas de naciones asociadas mediante el vínculo de la CSF del NIST, el adiestramiento y los objetivos de los ejercicios militares deben producir una pendiente ascendente positiva en su travesía cibernética. Además, se debe usar un enfoque de todo el gobierno para sincronizar esfuerzos de organización en participaciones de naciones asociadas y debe incluir el DoD, el Departamento de Comercio, la Cámara de Comercio y otros agentes honrados de comunidades industriales. La A6 también se aprovechará de aerotécnicos capaces de hablar en español, mediante programas de AFCLC y LEAP, para salvar la distancia del idioma con el fin de facilitar una conexión entre profesionales cibernéticos de EUA y LAC. La A6 también sincronizará la contribución cibernética de KLE, SMEE, JCCAT, asistencia a congresos, esfuerzos de educación y adiestramiento para afectar de manera positiva una estructura robusta de seguridad cibernética para el desarrollo del teatro de operaciones. La A6 hará esto mediante una interfaz con la comunidad cibernética de naciones asociadas para determinar sus requisitos respectivos, desde un punto de vista recíproco, con el fin de adaptar esfuerzos y efectos cibernéticos.

No obstante, las naciones de LAC deben determinar si el avance tecnológico de presupuestos moderados justifica el costo de su soberanía como estado nación. Los datos de sus ciudadanos, así como los datos de seguridad de defensa, están en riesgo con la tecnología china. Además, los piratas informáticos rusos siguen introduciendo software maligno y narrativas cuestionables que plantean un riesgo para la seguridad cibernética en un teatro de operaciones de defensa cibernética sin desarrollar. Latinoamérica y el Caribe tienen la oportunidad, basada en la proximidad de EUA, de hacer grandes inversiones en asociaciones de la industria cibernética favorables al crecimiento de las naciones asociadas para frustrar a China y Rusia.[52] EUA está ciertamente organizada para la competencia estratégica, pero es LAC la que mantiene la opción decisiva. ❑

Notas

1. Gen Laura Richardson, USA "SOUTHCOM's 2023 Posture Statement to Congress," USSOUTHCOM, (8 March 2023), https://www.southcom.mil/Media/Special-Coverage/SOUTHCOMs-2023-Posture-Statement-to-Congress//#/?currentVideo=31344.

2. Ted Piccone, "The Geopolitics of China's Rise in Latin America," *Brookings Institution Reports,* (Washington, DC: The Brookings Institution, November 2016), https://www.proquest.com/docview/1881432909/abstract/79CBF515D9154B19PQ/1.

3. Schneider, Florian, ed., *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity,* Amsterdam University Press, (2021), https://doi.org/10.2307/j.ctv1dc9k7j.most influential investment initiative in recent memory: China's Belt and Road Initiative (BRI).

4. "Honduran Official: US 'Respects' Decision on China Relations," *Reuters*, (21 March 2023), https://www.reuters.com/world/honduran-official-us-govt-respects-decision-seek-china-relations-2023-03-21/.

5. Sandra Cuffe, "Why Did Central America Shift UN Votes on Russia-Ukraine War?," *Al Jazeera*, (21 October 2022), https://www.aljazeera.com/news/2022/10/21/why-did-central-america-shift-un-votes-on-the-russia-ukraine-war.

6. Evan Ellis, "Russia's Latest Return to Latin America," *Global Americans* (blog), (19 January 2022), https://theglobalamericans.org/2022/01/russia-return-latin-america/.

7. Manuel Heitor et al., "Can Latin America Move Forward after a Lost Decade in Technical Change? . . . Looking at Opportunities for Knowledge-based Change in Times of Increasing Uncertainty," *Journal of Technology Management & Innovation* 9, no. 4, (2014), 1–19, https://doi.org/10.4067/S0718-27242014000400001.

8. Andreea Brînză, "What Happened to the Belt and Road Initiative?," The Diplomat, (6 September 2022), https://thediplomat.com/2022/09/what-happened-to-the-belt-and-road-initiative/.

9. Robert Morgus et al., "Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? A Review of Their Cyber Capabilities and the Implications for the U.S. and Its Partners in the Region," *Security Research Hub Reports*, (1 January 2019), https://digitalcommons.fiu.edu/srhreports/cybersecurity/cybersecurity/14.

10. Larry P. Goodson, "The U.S. and Afghanistan after 2014," *Asian Survey,* 55, no. 2, (2015), 249–72, https://doi.org/10.1525/as.2015.55.2.249.

11. Lara Seligman, "Biden Urged to Focus on Long-Neglected Latin America as Chaos Erupts," *Politico*, (15 July 2021), https://www.politico.com/news/2021/07/15/biden-latin-america-crisis-499752.

12. Juan Delgado, "China, 5G, and the Security Threat in Latin America," *Diálogo Américas* (blog), (7 March 2023), https://dialogo-americas.com/articles/china-5g-and-the-security-threat-in-latin-america/.

13. Tisha Bhambry, "The Gartner Top Cybersecurity Predictions for 2023 (APAC)," *Gartner Inc.*, (20 March 2023), https://www.gartner.com/en/webinar/462656.

14. BNamericas, "BNamericas - How Huawei Is Doubling down on Latin America...," *BNamericas.com*, (23 December 2021), https://www.bnamericas.com/en/features/how-huawei-is-doubling-down-on-latin-america-amid-global-headwinds.

15. William M. Leogrande, "A Poverty of Imagination: George W. Bush's Policy in Latin America," *Journal of Latin American Studies* 39, no. 2, (May 2007), 355–85, https://doi.org/10.1017/S0022216X07002416.

16. David Pion-Berlin and Harold Trinkunas, "Attention Deficits: Why Politicians Ignore Defense Policy in Latin America (Falta De Atención: ?Por Qué Los Políticos Ignoran Las Políticas de Defensa En América Latina?)," *Latin American Research Review* 42, no. 3, (2007), 76–100, https://www.jstor.org/stable/4499390.

17. Pion-Berlin and Trinkunas, "Attention Deficits."

18. Jeff Abbott, "América Crece: Washington's New Investment Push in Latin America," *Toward Freedom*, (8 October 2020), https://towardfreedom.org/story/america-crece-washingtons-new-investment-push-in-latin-america/; Dept. of State, "United States Launches America Crece Program (Growth In The Americas)," U.S. Embassy in Panama, (18 December 2019), https://pa.usembassy.gov/united-states-launches-america-crece-program-growth-in-the-americas/.

19. Dept. of Commerce, "Remarks by U.S. Commerce Secretary Gina M. Raimondo, 51st Annual Washington Council of the Americas (Virtual)," U.S. Department of Commerce, (4 May 2021), https://www.commerce.gov/news/speeches/2021/05/remarks-us-commerce-secretary-gina-m-raimondo-51st-annual-washington-council.

20. Chamber of Commerce, "Association of American Chambers of Commerce in Latin America and the Caribbean (AACCLA)," (12 March 2023), https://www.uschamber.com/program/international-affairs/americas/association-of-american-chambers-of-commerce-in-latin-america-and-the-caribbean-aaccla.

21. USSOUTHCOM, "SOUTHCOM's 2023 Posture Statement to Congress."

22. Sean Choquette and Stephanie Urbano, "Outcompeting China in Latin America Is a Top National Security Priority: A Senior Leader Perspective," *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, "OAS Report Examines Cybersecurity Trends in the Americas," *OAS - Organization of American States*, (3 May 2013), https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-173/13.

25. NIST, "Cybersecurity Framework," *NIST*, (12 November 2013), https://www.nist.gov/cyberframework.

26. Heitor et al., "Can Latin America Move Forward after a Lost Decade in Technical Change?"

27. Secureframe, "ISO 27001 vs NIST," Secureframe, (15 March 2023), https://secureframe.com/hub/iso-27001/vs-nist.

28. Mauricio Papaleo and Fabiana Santellán, "Perspectives on the Framework," *NIST*, (6 February 2018), https://www.nist.gov/cyberframework/perspectives.

29. Amy Mahn, "NIST International Engagement Updates: CSF 2.0 Update Workshop and More," *NIST*, (30 September 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, "Cyber-Physical Systems/Internet of Things for Smart Cities," *NIST*, (9 April 2022), https://www.nist.gov/programs-projects/cyber-physical-systemsinternet-things-smart-cities.

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

33. Choquette and Urbano, "Outcompeting China in Latin America Is a Top National Security Priority: A Senior Leader Perspective."

34. Richard L. Manley, "Cyber in the Shadows: Why the Future of Cyber Operations Will Be Covert," *National Defense University Press*, 3rd qtr, no. 106, (2022), 4–10, https://ndupress.ndu.edu/Media/News/.

35. Amy McCullough, "USAF Releases New Airpower Doctrine," *Air & Space Forces Magazine* (blog), (22 April 2021), https://www.airandspaceforces.com/usaf-releases-new-airpower-doctrine/; USAF, "Air Force Doctrine Publication 1," *USAF*, (10 March 2021), https://www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP%201%20The%20Air%20Force%20Pocket%20Size%20Booklet.pdf.

36. Mikala McCurry, "AFCLC Provides Language Support to DoD Missions," *Air Force News*, (28 September 2021), https://www.af.mil/News/Article-Display/Article/2791349/afclc-provides-language-support-to-dod-missions.

37. Air Force News Service, "CSAF Releases Action Orders to Accelerate Change Across Air Force," *Air Force*, (10 December 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. NATO, "Relations with Colombia," *NATO*, (17 June 2021), https://www.nato.int/cps/en/natohq/topics_143936.htm.

39. CyberScoop, "Hacking Group Focused on Central America Dumps 10 Terabytes of Military Emails, Files," *CyberScoop* (blog), (19 September 2022), https://cyberscoop.com/central-american-hacking-group-releases-emails/; Fox News Corp., " 'Black Hat' Hackers In Peru Target Government Ministers, Rattling The Cabinet," *Fox News*, (28 December 2016), https://www.foxnews.com/world/black-hat-hackers-in-peru-target-government-ministers-rattling-the-cabinet.

40. Curtis A. Ward, "Regional Threats: Security Capacity Imperatives in the Caribbean," *National Defense University Press*, 3rd qtr, no. 58, (2010), 26–31, https://ndupress.ndu.edu/portals/68/Documents/jfq/jfq-58.pdf.

41. Kirk Semple, "China Extends Reach in the Caribbean, Unsettling the U.S.," *The New York Times*, (8 November 2020), https://www.nytimes.com/2020/11/08/world/americas/china-caribbean.html.

42. Evan Ellis and Leland Lazarus, "China's New Year Ambitions for Latin America and the Caribbean," *The Diplomat*, (12 January 2022), https://thediplomat.com/2022/01/chinas-new-year-ambitions-for-latin-america-and-the-caribbean/.

43. Tisha Bhambry, "The Gartner Top Cybersecurity Predictions for 2023 (APAC)."

44. Ciara Nugent and Charlie Campell, "The U.S. and China Are Battling for Influence in Latin America, and the Pandemic Has Raised the Stakes," *Time*, (4 February 2021), https://time.com/5936037/us-china-latin-america-influence/.

45. Dept. of Homeland Security, "DHS Warns American Businesses about Data Services and Equipment from Firms Linked to Chinese Government | Homeland Security," *Department of*

Homeland Security Government, (22 December 2020), https://www.dhs.gov/news/2020/12/22/dhs-warns-american-businesses-about-data-services-and-equipment-firms-linked-chinese.

46. Ciara Nugent and Charlie Campell, "The U.S. and China Are Battling for Influence in Latin America, and the Pandemic Has Raised the Stakes," *Time*, (4 de febrero de 2021), https://time.com/5936037/us-china-latin-america-influence/.

47. Abdi Latif Dahir, "China 'Gifted' the African Union a Headquarters Building and Then Allegedly Had It Bugged," *Quartz*, (30 January 2018), https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/; Mailyn Fidler, "African Union Bugged by China: Cyber Espionage as Evidence of Strategic Shifts," *Council on Foreign Relations*, (7 March 2018), https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

48. Evan Ellis, "China's Digital Advance in Latin America," *Diálogo Américas* (blog), (7 July 2022, https://dialogo-americas.com/articles/chinas-digital-advance-in-latin-america/; Greg Myre, "China Wants Your Data — And May Already Have It," *NPR*, (24 February 2021), sec. National Security, https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it.

49. Jonathan E. Hillman and Maesea McCalpin, "Watching Huawei's 'Safe Cities,'"(4 November 2019), https://www.csis.org/analysis/watching-huaweis-safe-cities.

50. Myre, "China Wants Your Data — And May Already Have It;" "China's Push to Control Americans' Health Care Future," *60 Minutes*, (31 January 2021), https://www.cbsnews.com/news/biodata-dna-china-collection-60-minutes-2021-01-31/.

51. Choquette and Urbano, "Outcompeting China in Latin America Is a Top National Security Priority: A Senior Leader Perspective."

52. Shannon O'Neil, "Why Latin America Lost at Globalization—and How It Can Win Now," *Council on Foreign Relations*, (25 August 2022), https://www.cfr.org/article/why-latin-america-lost-globalization-and-how-it-can-win-now.

Coronel James Hamilton, USAF

Sirve actualmente como director de ciberespacio y comunicaciones de la 12ª Fuerza Aérea (AFSOUTH), Base de la Fuerza Aérea Davis--Monthan, Arizona. Lidera todos los aspectos de comunicaciones y planificación cibernética para apoyar directamente las participaciones de las naciones asociadas del USSOUTHCOM como sujeto experto cibernético del componente aéreo. Tiene una maestría de ciencia aeronáutica de Embry-Riddle y un doctorado en liderazgo estratégico de la Universidad Liberty donde examinó el apoyo del líder superior de la Fuerza Aérea de EUA para la comunidad conjunta. Recientemente sirvió 5 años en la OTAN en su sede de Bruselas, Bélgica en el Estado Mayor Militar Internacional tanto como gerente de información y conocimientos y después en Mons, Bélgica en el estado mayor del grupo de sistemas de comunicaciones e información como jefe de división de operaciones responsable de comunicaciones e interoperabilidad desplegables en todo el teatro de operaciones.

Capitán Valdir Ruiz, USAF

Actualmente sirve en la directiva de comunicaciones de la 12ª Fuerza Aérea (AFSOUTH), oficial a cargo de cooperación de seguridad ciberespacial. En su función, lidera la planificación y ejecución de operaciones, actividades e inversiones céntricas de seguridad y defensa cibernéticas y coordina requisitos interesados nacionales e internacionales. Es un oficial de operaciones de comunicaciones de combate, y tiene un título de ciencia en seguridad cibernética y una maestría de ciencia en tecnología de seguridad cibernética. La doble herencia del Capitán Ruiz es ecuatoriana y uruguaya. Vivió en Ecuador durante su educación primaria y secundaria. Es un académico del programa de aerotécnicos con capacidad de idiomas de la USAF.