

USCYBERCOM: "El futuro se trata del dominio de la información"...

La competencia y los conflictos futuros dependerán del "dominio de la información", una misión que se desarrollará en gran medida en el ciberespacio, pero que no puede separarse de las operaciones militares convencionales, dijo recientemente el jefe del UNITED STATES CYBER COMMAND (USCYBERCOM), general Paul Nakasone.

"El futuro se trata de la información, el dominio de la información", dijo el alto oficial durante la conferencia anual WEST del INSTITUTO NAVAL DE ESTADOS UNIDOS y la ASOCIACIÓN DE ELECTRÓNICA Y COMUNICACIONES DE LAS FUERZAS ARMADAS. El general Nakasone hizo sus comentarios sobre el futuro después de reflexionar sobre momentos clave en la existencia de una década de USCYBERCOM, una organización en la que ha estado involucrado desde el principio y de la que asumió el liderazgo en 2018. Nakasone también lidera la NATIONAL SECURITY AGENCY (NSA) y el CENTRAL SECURITY SERVICE (CSS).

"Con demasiada frecuencia pensamos en el ciberespacio como algo distinto de la lucha física. Ese no es siempre el caso", dijo, y agregó que lo virtual y lo físico están cada vez más entrelazados. De esta manera, sostuvo, "los eventos en el campo de batalla virtual informan y reflejan el campo de batalla físico".

El tema del "dominio de la información" parece reflejar visiones más amplias sobre el cambiante entorno competitivo global. Las fuerzas armadas de Estados Unidos, en términos más generales, se están modernizando incluso cuando pasa de un enfoque de dos décadas en combatir el terrorismo a "competir" contra "pares cercanos" tales como China y Rusia. Es en el ciberespacio donde ya se están desarrollando aspectos muy importantes de esta denominada "competencia entre pares".

LOS RIVALES

China también ha destacado su objetivo de controlar el entorno de la información.

Un estudio reciente del INSTITUTO INTERNACIONAL DE ESTUDIOS ESTRATÉGICOS (IISS) descubrió que EE.UU. es la única potencia cibernética global de primer nivel. China, dice el estudio, está lista para desafiar la actual "clara superioridad" de Estados Unidos en el ciberespacio dentro de la próxima década.

El "dominio de la información" también parece, en parte quizá, relacionado con lo que el general de división del US Army Peter Gallagher, que dirige la modernización de la red del Ejército para el COMANDO DE FUTUROS, ha llamado el concepto de "dominio de decisiones". Los comentarios de Gallagher reflejan el objetivo del COMANDO Y CONTROL CONJUNTO DE TODOS LOS DOMINIOS (JADC2), caracterizado como una estrategia de meta-interconexión para coordinar operaciones militares en tierra, mar, aire, espacio y ciberespacio. La información oportuna para los tomadores de decisiones y el control del entorno de información se consideran parte integral del éxito del JADC2.

Al discutir la "imagen de la amenaza", Nakasone detalló tres temas que han sido comunes en discursos recientes y testimonios dados ante el Congreso. El primero es el creciente alcance de lo que Estados Unidos debe defender y proteger en el ciberespacio, debido a una superficie de ataque "mucho más amplia", que incluye sistemas de

armas y un tesoro de datos militares en expansión exponencial. Como se sabe, los datos serán un habilitador clave del JADC2.

El segundo tema es la escala de los actuales ataques cibernéticos, evidenciada recientemente por campañas cibernéticas de alto perfil tales como SOLARWINDS, el hackeo de los servidores de MICROSOFT EXCHANGE, y la llamada COLONIAL PIPELINE. Nakasone observó que los competidores cercanos, China y Rusia, han ejecutado "campañas persistentes y maliciosas" que no deben considerarse "episódicas".

"Ya no estamos en Kansas", dijo, y señaló que los adversarios estadounidenses han invertido y puesto efectivamente en funcionamiento sus capacidades.

El tercer tema es determinar cuán sofisticados son realmente los ciberadversarios de EE.UU., lo que no ha sido obstáculo para que estos, a veces, hayan tenido éxito con técnicas bastante simples. La clave es reconocer cómo se están adaptando los adversarios y actuar en consecuencia.

Nakasone señaló tres tareas que considera importantes en el futuro. En primer lugar, está el arduo trabajo de integrar cibernética en las fuerzas armadas, el gobierno, los aliados y los socios. El segundo es fortalecer las ciberdefensas. El tercero es el desarrollo continuo de un grupo de talentos cibernéticos nacionales mediante la búsqueda de formas de atraer, capacitar y retener a una generación de ciberguerreros de élite.

"No se trata solo del dinero, créame", dijo Nakasone, refiriéndose a la tentación de trabajos mejor pagados en el sector privado. "Pero tampoco se trata solo de la misión. Necesitamos estar abiertos a nuevas ideas sobre el desarrollo profesional".

Hasta este último punto, Nakasone desafió a la audiencia a "pensar de manera diferente".

"Tenemos una tecnología increíble, un oficio increíble, pero lo más importante que tenemos es el talento", dijo. Señaló en este sentido la importancia de las reservas militares y de la Guardia Nacional, a las que se refirió colectivamente como "nuestra profundidad estratégica", así como la importancia de la fuerza laboral civil, que actualmente constituye alrededor del 60% del personal de la sede de CYBERCOM y que proporciona "continuidad, experiencia y tutoría", sostuvo.

Pero no solo CYBERCOM jugará un papel en el futuro cibernético de Estados Unidos. Nakasone promocionó el papel de la NSA, con su doble misión de inteligencia de señales y ciberseguridad. El general señaló la importancia de la criptología en las ciberdefensas, que es una especialidad de la NSA. "El verdadero respaldo es el cifrado", dijo, "para proteger los sistemas de armas y los datos". Cuanto más fuertes sean las capacidades criptográficas de EE.UU., "mejor estaremos", afirmó.

"Cierro con un optimismo", dijo Nakasone, "que debe ser equilibrado con la constatación de que tenemos trabajo por hacer".

