Internacional

Dentro del rango cibernético de la OTAN: cómo se preparan los ejércitos para el ataque y por qué las naciones deben trabajar juntas

Miguel Siurana

Con solo tocar un botón, un soldado que sostiene una computadora portátil envía chispas a una placa de circuito, lo que hace que un generador de energía parpadee en rojo brillante mientras un pitido se hace más fuerte. Esta es la representación de la infraestructura de energía de un país que sufre un ataque cibernético.

Aunque el mapa de placas de circuito representa una isla ficticia, con calles llamadas “Blockchain Street” y “Macintosh Street”, un ataque cibernético de la vida real puede no ser tan visible como este. Aún así, los efectos en la infraestructura pueden ser igual de devastadores, causando que los hogares pierdan energía o agua.

El escenario es solo una simulación, pero sirve como campo de entrenamiento para los soldados que se encuentran en el Cyber Range de la OTAN en la capital de Estonia, Tallin.

En el CR14 NATO Cyber Range, alrededor de 145 comandantes en el sitio de hasta 30 países, la mayoría de ellos países de la OTAN, pero algunos no, se ponen a prueba sobre cómo prevenir un ataque cibernético.

> Dentro del edificio de tres pisos que lo alberga, el primer piso es donde se brindan alimentos y refrigerios y se exhiben algunas de las innovaciones. El segundo piso se usa para entrenamiento y donde no se permiten teléfonos. Y el tercer piso es donde ocurre la verdadera acción, pero está fuera del alcance de los periodistas.

Ucrania y el artículo 5

La operación cibernética de una semana de duración de la OTAN, que tuvo lugar la semana pasada, es un evento anual. Este año ha visto la mayor cantidad de participantes, lo que no sorprende dado **la guerra en ucrania**.

“Lo que hemos visto en Ucrania son ataques cibernéticos realmente continuos desde febrero, incluso desde antes de que comenzara la guerra”, dijo David Cattler, secretario general adjunto de inteligencia y seguridad de la OTAN.

“Operaciones cibernéticas adicionales están en curso… Algunas de estas operaciones han sido vinculadas a la inteligencia militar rusa, al GRU, y están claramente diseñadas para causar efectos psicológicos y agotar los recursos de defensa cibernética, lo que nuevamente destaca el papel que juega la cibernética en una crisis. y se juega en esta guerra”, dijo.

La OTAN se toma tan en serio los ataques cibernéticos que su secretario general, Jens Stoltenberg, dijo este año que los ataques cibernéticos contra un miembro de la OTAN podrían desencadenar el Artículo 5, lo que significa que se considera un ataque contra todos los miembros de la OTAN y la alianza podría reaccionar.

La verdad en la ficción

De vuelta en Cyber Range, las historias inventadas para que los participantes resuelvan involucran la isla ficticia de “Icebergen”, hogar de las naciones del supuesto miembro de la OTAN “Anduaria” y “Harbardus”, un enemigo.

“Eso [the situation in Ukraine] aporta más seriedad en términos de cómo sucede esto realmente. Ya no es tan ficticio. Y esa es la diferencia que trae esta cosa”, dijo a Euronews Next Bernd Hansen, Jefe de la Sección de Ciberespacio en el Comando Aliado de Transformación de la OTAN.

Aunque los participantes y la OTAN mantienen muy en secreto las historias, dicen que pueden incluir ataques a la infraestructura, intrusiones en la red y posibles amenazas internas.

Pero la atención se centra en cómo cada país participante comparte información y puede ayudar al otro en caso de un ataque, en lugar de competir entre sí.

Esto se llama la operación “escudos bloqueados”, un ejercicio de la vida real en el que reaccionarían y ayudarían a otros países.

“Creo que establece el enfoque en la colaboración y nada más, porque si comienzas a competir, tiendes a estar en una situación en la que no compartes tanto porque quieres estar en una buena

situación en escudos cerrados y podrías obtén puntos compartiendo", dijo Tobias Malm, un comandante de las Fuerzas Armadas Suecas en defensa cibernética.

"Por supuesto, siempre habrá un lado competitivo en el sentido de que todos los técnicos quieren resolver los problemas técnicos por sí mismos y ser los primeros en resolverlos. Entonces, en ese sentido, ese es un ingrediente competitivo en el ejercicio", dijo a Euronews Next.

Aunque actualmente no es miembro de la OTAN, es posible que Suecia pronto lo sea después de que los miembros de la OTAN acogieran rápidamente su solicitud para unirse a la alianza junto con la vecina Finlandia luego de la invasión de Ucrania por parte de Rusia.

Pero no es la primera vez que Suecia participa en los programas de formación de la OTAN.

"Hemos estado en este ejercicio creo que durante 10 o 12 años. Así que no es nada nuevo", dijo Malm.

"Pero para nosotros trabajar juntos en materia de ciberdefensa es bueno, aprendemos mucho y creo que podemos aportar algo nuevo a la OTAN con respecto a cómo trabajamos y también con respecto a cómo trabajamos".

Aunque tanto Suecia como Finlandia han estado aquí antes, este año ha sido importante para los países.

"Este año hemos mejorado la capacidad y el intercambio de información", dijo Markus Riihonen, Comandante Mayor de Defensa de las Fuerzas de Defensa de Finlandia.

"Me he sentido muy, muy orgullosa de ser tratada con mucho cariño. Y parte de esto es porque hay gente con la que ando por aquí y me tratan como a un aliado", dijo a Euronews Next.

"Espero tener dos países de seguridad cibernética de muy alto nivel [Finland and Sweden]que es muy beneficioso para ellos. [NATO]. esto es lo que ellos [NATO] me han hecho saber que esperan con ansias la adhesión y la integración en el futuro".

Innovaciones tecnológicas

Con las numerosas empresas emergentes de seguridad cibernética en Finlandia y Suecia, la OTAN tiene todas las razones para estar entusiasmada con la incorporación de los países.

"Estamos ansiosos por poder dar la bienvenida a Finlandia y Suecia a nuestro ecosistema de innovación para mantener nuestra ventaja tecnológica. Quiero decir, ahora son sus socios o invitados de clase mundial, y también habrá trabajo como verdaderos aliados cercanos", dijo David van Weel, Secretario General Adjunto de la OTAN para Desafíos de Seguridad Emergentes.

"Estos son dos países muy capaces, especialmente cuando se trata del campo de la innovación. Tienen un historial de fuerte compromiso con sus sectores privados. Tienen ecosistemas de innovación florecientes", dijo.

Van Weel dijo que trabajar con el sector privado y la academia resultará crucial para la ciberdefensa, lo que se puede ver en la forma en que empresas como Starlink y Microsoft han ayudado a Ucrania.

"La OTAN está comprometida a mantener su ventaja tecnológica y ejercicios como la coalición cibernética, ayúdanos a probar y poner en práctica estas nuevas tecnologías", dijo.

“La amenaza del ciberespacio es real y está creciendo y necesitamos hacer más inversiones para mejorar nuestras defensas cibernéticas, más experiencia, más cooperación, también con el sector privado”.

En el edificio NATO Cyber Range, la innovación se muestra en forma de los primeros scooters 5G del mundo que zumban por los largos pasillos. Aunque solo está ahí como inspiración, muestra cómo el transporte que opera con 5G podría ser atacado.

Del mismo modo, también hay un simulador de acorazado, que podría sufrir un ataque cibernético si el mapa digital que usa el barco fuera pirateado y desaparecieran países o islas.

Pero la prueba más grande para los países participantes está en la infraestructura, como el alumbrado público, el suministro de agua y la calefacción, que están bajo ataque cibernético.

Esto, en el mundo real, es una amenaza grave, que Ucrania ha experimentado desde octubre después de que Rusia comenzó a atacar su infraestructura energética, dejando alrededor del 30 por ciento de las centrales eléctricas en todo el país destruidas y muchas sin calefacción ni luz en el invierno.

Georgia, que también limita con Rusia, también está preocupada por los ataques cibernéticos. El país postsoviético, que no es miembro de la OTAN, fue atacado por Rusia hace 13 años en una guerra de cinco días.

Gran parte de la infraestructura de Georgia también es soviética en diseño e instalación.

“Para el Ministerio de Defensa, la seguridad cibernética es una de las principales prioridades porque enfrentamos muchos desafíos”, dijo Nika Gogindze del Ministerio de Defensa de Georgia sobre ciberseguridad.

Dijo que la semana de seguridad cibernética de la OTAN le ha permitido mejorar la cooperación cibernética de Georgia con otros países.

“Nuestro objetivo era mejorar la coordinación con nuestros aliados y su naturaleza y disminuir el tiempo para encontrar nuevas formas de comunicarnos con ellos durante la crisis de ciberataques.

“Así que se logró el objetivo y estoy muy feliz con eso”.

A medida que termina la semana, también lo hace, por supuesto, cualquier rastro cibernético de las operaciones que ocurrieron. Todos los inicios de sesión de correo electrónico se borran del edificio y comienza una nueva semana para nuevas operaciones de capacitación cibernética.

El origen : www.euronews.com