Ciberataques contra Rusia: Occidente cría cuervos

PABLO JOFRÉ LEAL :: 17/02/2023

Uno de los países más corruptos del mundo, Ucrania, desarrollará toda una industria de hackeo

Los países occidentales liderados por EEUU y donde destaca el papel de testaferro cumplido por la Organización del Tratado del Atlántico norte - OTAN - se han impuesto, como objetivo, llevar adelante una guerra donde destacan dos líneas de acción, peligrosísimas para Europa en particular y el mundo en general.

Estas dos líneas se ejemplifican por: las órdenes dadas al gobierno títere de Ucrania presidido por Volodimir Zelensky, para ser quien instigará un enfrentamiento militar directo bajo la constante provocación de atacar a la población del Donbás y luego del inicio de la operación militar de desnazificación y desmilitarización presentarse ante el mundo como la víctima de afanes expansionistas de Moscú, que se impone como narrativa de los medios occidentales. En segundo lugar los padrinos de Ucrania, principalmente Washington y su brazo militar europeo han decidido ocupar el proceso de operaciones adscritos a la denominada guerra híbrida - que se sitúa fuera de ellos márgenes clásicos de un ejército contra grupos insurgentes - con el uso de diversos métodos de creación más reciente y aquellos más convencionales, que se dan en el campo de la economía, sicología, el uso desinformador y manipulador de los medios de comunicación, las telecomunicaciones, ataques informáticos, hackeo de sistemas de defensa e incluso de servicios básicos.

Es así, que en esta guerra híbrida contra Rusia, EEUU y los suyos, no sólo han generado la destrucción de un tramo del gasoducto Nord Stream II, sino también la censura de gran parte de los medios de comunicación ruso en una acción que muestra la hipocresía de ese tipo de llamados que suele hacer occidente respecto a la libertad de expresión, como elemento central del mundo democrático. Se suma a lo señalado los ataques cibernéticos para tratar de parar el funcionamiento del sistema energético de la Federación rusa, que les permita generar un caos social de proporciones y provocar la reacción de protesta del pueblo ruso, como lo intentaron contra Irán tras la muerte de la joven Mahsa Amini.

La idea de los ataques cibernéticos contra la red energética rusa, está encaminada a desequilibrar la entrega de servicios básicos para la población rusa. El generar un caos en el sistema eléctrico significa afectar, no sólo la vida cotidiana sino también aspectos básicos de defensa, puertos, aeropuertos, estaciones de ferrocarriles. El sistema bancario, el tránsito de calles y carreteras. En fin…un caos masivo. En diciembre del año 2022 la OTAN organizó, en varias bases militares un entrenamiento en la esfera de la Ciber-Seguridad. La más importante de ella "Cyber Coalition 2022" se efectuó en Estonia, país báltico fronterizo con Rusia. Tomaron parte en ella un verdadero ejército de técnicos, programadores civiles y militares. Además de mil militares miembros de la OTAN, se hicieron presente especialistas de Finlandia, Suecia, Japón, Irlanda y Georgia. El jefe de este entrenamiento fue Charles Elliott, comandante en jefe y director del ejercicio Cyber Coalition 2022, miembro de la marina de los EEUU quien destacó, que el blanco de todo este tipo de ejercicios es Rusia.

Cyber Coalition 2022 representa, según la información entregada por los organizadores de este tipo de eventos de preparación para las guerras híbridas "un lugar perfecto para experimentar, impulsar la guerra en el ciberespacio y el desarrollo de capacidades. Se utiliza, entre otras cosas, para probar y validar conceptos, capturar requisitos o explorar tecnologías emergentes y disruptivas, en apoyo de los operadores y comandantes militares. La campaña de experimentación de Cyber Coalition 2022 incluyó experimentos sobre el uso de la inteligencia artificial para ayudar a contrarrestar las amenazas cibernéticas, sobre la estandarización de los mensajes cibernéticos para fomentar el intercambio de información y sobre la explotación de la inteligencia sobre amenazas cibernéticas, para informar la conciencia situacional del ciberespacio"

Este tipo de ejercicios, que es parte ya de las actividades cotidianas de los países occidentales, se han aplicado contra Rusia, China, Irán, Venezuela, entre otros. Para el comandante supremo aliado de Transformación de la OTAN, general Phillippe Lavigne, de la Fuerza Aérea Francesa "Los actores malignos buscan degradar nuestra infraestructura crítica, interferir con nuestros servicios gubernamentales, extraer inteligencia, robar propiedad intelectual e impedir nuestras actividades militares. Los aliados se comprometen a proteger su infraestructura crítica, desarrollar resiliencia y reforzar sus defensas cibernéticas. Continuaremos elevando nuestra guardia contra este tipo de actividades cibernéticas maliciosas en el futuro y nos apoyaremos mutuamente para disuadir, defender y contrarrestar todo el espectro de amenazas cibernéticas, incluso considerando posibles respuestas colectivas"(1)

Las actividades agresivas y destructivas de EEUU contra Rusia, en materia de realizar ciberataques contra la infraestructura digital de la federación rusa, está causando una nueva etapa en la escala de intensidad del conflicto entre las dos potencias nucleares. En junio del año 2022, a pocos meses del inicio de la operación de desnazificación y desmilitarización de Ucrania - advertida por Rusia tras ocho años de ataques de Kiev contra la población del Donbás - El General Pablo Nakasone, Comandante del Comando cibernético de EE.UU., Director de la Agencia de Seguridad Nacional y Jefe del Servicio Central de Seguridad, dio a conocer que su país estaba realizando una serie de operaciones digitales de carácter ofensivo, para apoyar y proteger a Ucrania.

El mencionado general subrayó, como excusa, que toda la operación se realizó bajo supervisión civil, de tal manera de no generar acciones encaminadas a investigar este tipo de operaciones, absolutamente al margen de la ley.Recordemos, que durante su audiencia de confirmación el año 2018, Nakasone dijo que "no creía que Rusia, China y otros países hubieran visto una respuesta estadounidense suficiente a los ciberataques como para cambiar su comportamiento" (2). El mismo Nakasone, en junio del año 2022, admitió que sus subordinados fueron desplegados en Ucrania antes del conflicto y que han realizado varias operaciones contra Rusia después del 24 de febrero del 2022, cuando comenzó el operativo militar ruso, aunque no estuvieran sobre el terreno. «Hemos realizado una serie de operaciones en todo el espectro: operaciones ofensivas, defensivas y de información», declaró el general estadounidense a la cadena Sky News. Precisó que las acciones del USCC han sido legales y supervisadas por las autoridades superiores militares y civiles de EEUU.

El presupuesto de la secretaría de guerra estadounidense, para el año 2023, establece 11

mil millones de dólares para efectuar ciberataques contra lo que consideran estados enemigos y ello se está ocupando, sin freno alguno,conscientes que una reacción de la federación rusa en el campo de la ciber-esfera puede provocar el derrumbe de infraestructura vital estadounidense y ocasionar daños al sector civil, tal como Washington lo ha ocasionado a Rusia. Los ciberataques ejecutados por EEUU han afectado no sólo a Rusia, sino también a China y la República Islámica de Irán, lo que se ha constituido en graves violaciones al derecho internacional, sin que ello tenga consecuencias contra EEUU y dan muestra del doble estándar de occidente en materia de seguridad.

Una esfera de acción que muestra toda la ambición de Joe Biden, quien en octubre del año 2022 dio a conocer en sus documentos doctrinales , que todo el mundo y el espacio global de información y acción, eran parte de la esfera de interés de EEUU. En enero pasado los gobiernos de EEUU y Japón dieron a conocer que ampliarían su esfera de seguridad al espacio japonés con el fin de salvaguardar los satélites esenciales para las actividades de vigilancia militar y ejecución de acciones en el campo de las guerras híbridas. La alianza de Washington y Japón ha tenido resultados acusados por China, quien en septiembre del año 2022 acusó abiertamente a la Casa Blanca de realizar un ciberataque masivo dirigido ante todo el sistema educativo chino (3)

A su vez, en octubre del año 2022 la República Islámica de Irán atribuyó la responsabilidad a EEUU y el régimen sionista por ciberataques que intentaron violar la seguridad de las centrales nucleares de la nación persa al igual que una ola de ataques cibernéticos contra el Banco Central de Irán y dos plataformas de mensajería. Irán denunció, en aquella ocasión, que el número de ataques cibernéticos se acercó al centenar, sin que los organismos internacionales se pronunciaran Irán ha refutado en un sinnúmero de ocasiones el ejecutar ataques cibernéticos y cuestiona el doble rasero de la comunidad internacional cuando pasa lo mismo en contra del país persa. Tras cuestionar la competencia y la legitimidad de occidente, para formular tales acusaciones, la representación iraní criticó "el silencio y el apoyo directo o indirecto frente a los numerosos ataques cibernéticos contra la infraestructura, e incluso las instalaciones nucleares de Irán" (4)

Según la ciber-doctrina estadounidense en materia civil y militar, Rusia es el enemigo principal de Washington en el espacio de información y ello implica ejecutar todo tipo de acciones, para que su acciones ofensivas, sobre todo en la red de Internet, tengan resultados que signifiquen daño a Rusia. Para efectuar los ataques al sector bancario y la esfera de servicio financiera, por ejemplo, los estadounidenses usan un proyecto especial del ciber-comando de EEUU llamado "IT Army of Ucrania" en el marco de cierta similitud al que utilizan las unidades especiales de las Fuerzas Armadas Ucranianas. Rusia acusó directamente a EEUU de entrenar al ejército de TI ucraniano, reclutar piratas informáticos para ataques cibernéticos.

A fines de enero de este año 2023, el viceministro de Relaciones Exteriores de Rusia, Oleg Syromolotov, al hablar con la agencia de noticias rusa TASS, sostuvo que su país, está al tanto de las operaciones que lleva a cabo EEUU contra ellos en el espacio de la información al reclutar piratas informáticos y brindar capacitación al ejército de TI de Ucrania. "Es revelador que EEUU esté poniendo en práctica sus políticas agresivas. No intentaron ocultar el hecho de que su comando cibernético está realizando operaciones contra nuestro

país. Somos muy conscientes de que Washington está reclutando agresivamente a piratas informáticos, entrenando a los llamado Ejército de TI de Ucrania, y utilizando tecnologías de información y comunicación de sus socios y empresas privadas controladas para llevar a cabo ataques cibernéticos contra la infraestructura de información de Rusia» (5)

Al ejercer ciber-influencia del territorio ucraniano en la infraestructura rusa, los países occidentales pueden causar procesos incontrolables en el ciberespacio ocasionado gravísimos daños no sólo al país enemigo, sino también a los que suelen denominarlos "daños colaterales". Una transferencia d programas con códigos maliciosos por parte de Washington a Kiev ocasiona, inevitablemente, su fuga al mercado negro por al carácter intrínsecamente corrupto de la casta política-militar ucraniana y su uso por parte de hackers en su utilización criminal como ya ha ido denunciado pero acallado por lo medios de desinformación y manipulación occidentales, en cuyos países reventará, más temprano que tarde estas organizaciones criminales.

Que recuerden los estadounidenses a la agrupación "Shadow Broker" (6) quienes robaron los códigos fuente - 'source code' - del sistema operativo Windows. Robados a la Agencia de Seguridad Nacional de EEUU, que fueron utilizados, posteriormente para crear el virus "WanaCry" que en el año 2017 bloqueó el funcionamiento de muchísimas empresas y organizaciones en el mundo. Hackearon cientos de miles de tarjetas de créditos. El uso indiscriminado de hackers lo que ocasiona es un descontrol que más temprano que tarde repercute en aquellos que han propiciado su florecimiento. Hoy se anima a uno de los países más corruptos del mundo, Ucrania, a desarrollar toda una industria de creación de códigos maliciosos, de hackeo, se anima a cometer crímenes, impunemente.Occidente suele criar cuervos que después comen sus ojos sin asumir nunca sus responsabilidades.

Notas

1. https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia
2. https://www.forbes.com.mx/eu-tiene-nuevo-jefe-de-seguridad-cibernetica/
3. Un informe publicado el lunes por el Centro Nacional de Respuesta a la Emergencia de Virus Informáticos (CVERC) de China acusa a la NSA, la agencia de inteligencia militar estadounidense, de haber «realizado decenas de miles de ciberataques maliciosos» en China «en los últimos años». El informe acusa a una rama de la NSA, la Tailored Access Operations (TAO), de haberse infiltrado en la Universidad Politécnica del Noroeste, con sede en Xi'an (norte de China). Esta institución de enseñanza superior, financiada por el Ministerio de Industria y Tecnología de la Información, está especializada en la investigación aeronáutica y espacial.https://www.diariolibre.com/planeta/tecnologia/2022/09/05/china-acusa-a-agencia-militar-de-eeuu-de-ciberataques/2045888
4. https://www.hispantv.com/noticias/politica/551137/iran-condena-ciberataque-albania
5. https://www.wionews.com/world/russia-alleges-us-of-training-ukrainian-it-army-recruiting-hackers-556807
6. Los Shadow Brokers son conocidos por haber divulgado el exploit Eternal Blue que fue lo que derivó en el masivo ataque de WannaCry que en 2017 afectó a más de 230 mil

computadoras en 150 países.https://www.xataka.com/seguridad/the-shadow-brokers-su-historia-desde-el-hackeo-a-la-nsa-hasta-la-venta-de-exploits-por-suscripcion-mensual

Hispantv.com

---

https://www.lahaine.org/mm_ss_mundo.php/ciberataques-contra-rusia-occidente-cria