Publicado en la página web del CEEEP
Fecha: 26 de enero de 2021

Ciberespacio: ¿El Salvaje Oeste?

Adolfo Arreola García, graduado del Colegio del Aire de la Fuerza Aérea Mexicana. Egresado de la Universidad Nacional Autónoma de México (UNAM) en la licenciatura de Relaciones Internacionales y la Maestría en Estudios México-Estados Unidos (graduado con mención honorífica); doctorado en Seguridad Internacional en Universidad Anáhuac. Profesor investigador en la Facultad de Estudios Globales de la Universidad Anáhuac México Norte y profesor en la Facultad de Estudios Superiores Acatlán, UNAM. Coordinador del Diplomado "Ciberseguridad y Estrategia el poder de la información" en la Universidad Anáhuac México Norte. Diseñó la materia de ciberseguridad.

Resumen

En este artículo, el autor analiza las dificultades que existen en el ciberespacio, debido a sus propias características y a la falta de una regulación internacional integral para la atribución de ciberataques, así como para responder adecuadamente a los intentos por dañar o destruir los sistemas de comunicación, mando y control por parte de actores perversos.

Introducción

En el presente siglo, el ciberespacio es considerado como un elemento esencial en la vida de millones de personas alrededor del mundo. A través y dentro del ciberespacio se realizan operaciones esenciales para el desarrollo económico, la actividad político-social, la seguridad, la producción industrial, la práctica democrática y la protección de las infraestructuras críticas de un Estado.

Sin embargo, al ser un espacio de dominio y competencia, el ciberespacio se ha convertido en una herramienta y medio para realizar actividades ilegales, con cierto nivel de impunidad, debido a la falta de una regulación de los actos violentos y de guerra cometidos por medio del ciberespacio.

A fin de exponer lo anterior, el análisis integra cuatro secciones que detallan los pormenores del ciberespacio, identifican los elementos que clasifican a un evento adverso como ciberataque, la dificultad de responderlo, y exponen la necesidad de un marco legal para la preservación de la paz y seguridad en el ciberespacio.

Características del ciberespacio

El ciberespacio es un ámbito de la guerra, en el cual los Estados del mundo buscan hacerse con la supremacía, diferenciándose de los otros ámbitos bélicos por su alcance global, velocidad e impacto. El ciberespacio se caracteriza por ser un espacio creado por el hombre, tener un carácter global, tener al internet como elemento central, ser una tecnología de doble uso, ser un medio para realizar ataques de forma anónima, tener importancia geopolítica, no respetar conductas internacionalmente aceptadas y, dificultar la atribución de las acciones.

El ciberespacio es un lugar creado por el hombre y para el hombre, ya que es donde, de manera colectiva, confluyen las actividades diversas de la sociedad, arropando las transacciones, relaciones y pensamiento de todos aquellos usuarios que se conectan. El ciberespacio no tiene fronteras al ser una abstracción de la mente humana, el cual tiene un alcance global y elementos tangibles e intangibles que permiten la representación del mundo material en un espacio virtual.

El ciberespacio no está regulado por el Derecho Internacional Humanitario debido a su aparición reciente. Sin embargo, el impacto negativo de los ciberataques y la capacidad destructiva de las ciberarmas han ido en aumento; por lo tanto, los Estados que los utilicen como medios de defensa y ataque deben hacerlo con plena consideración de los Convenios de Ginebra.

La atribución de las acciones violentas es una tarea lenta y difícil en el ciberespacio debido a las características técnicas y organizacionales, la naturaleza del ciberataque, la configuración del internet y los avances tecnológicos. A pesar de ello, existen esfuerzos internacionales para garantizar la atribución precisa de los actos y demostrar la ilegalidad del acto.

El ciberespacio es considerado como un Global Common. En 1996, John Perry Barlow redactó la Declaración de Independencia del Internet para convencer a los gobiernos de no asumir soberanía alguna sobre el ciberespacio. Poco después, el ciberespacio se convirtió en el último de los Global Commons, justo por ser un espacio virtual creado por el hombre con utilidad común en donde la información es el principal activo.

El ciberespacio tiene una importancia geopolítica. Bajo las condiciones de hiperconectividad y competencia internacional por dominar el ciberespacio, controlarlo es vital para la obtención, preservación e incremento del poder que ostenta un Estado. Hoy, el ciberespacio, junto con las tecnologías de la información,

son activos estratégicos para los gobiernos del mundo ya que, quien controle el ciberespacio, se hará con el control del mundo. Esto ha generado cambios en las políticas de seguridad nacional, doctrinas militares e investigaciones académicas que buscan establecer modelos de ciber soberanía.

El ciberespacio es una herramienta de doble uso. Al ser un ámbito en donde se busca un dominio y se enfatiza la competencia, el ciberespacio no solamente sirve para realizar actividades no lesivas, sino también se ha convertido en una herramienta y medio para causar daño, robar, estafar, atacar, interrumpir, sorprender, manipular, mentir y asesinar. Irónicamente, el ciberespacio sirve tanto para lograr la conciliación, el desarrollo y la paz, como para motivar el conflicto, el atraso y la guerra.

En resumen, las características del ciberespacio lo convierten en un espacio único, con potencial para generar daño por medio de un ciberataque. La no atribución abre la puerta a que los actores utilicen el ciberespacio con impunidad en beneficio de sus objetivos geopolíticos. Por consiguiente, regular las actividades u operaciones y establecer penas en caso de hacer mal uso de sus capacidades en perjuicio de terceros es una acción impostergable.

En qué condiciones se sufre un ciberataque

A pesar de que la palabra "ciberataque" es utilizada para referirse a eventos adversos que atentan contra los sistemas computarizados de mando, control y comunicaciones, no todos deben ser considerados como un ciberataque. El objetivo final y los actores de un hackeo de gran envergadura serán los elementos que definan la clasificación del evento adverso como un ciberdelito o un ciberataque. Diferenciar con eficacia, permitirá avanzar en la construcción de un marco legal internacional que regule los ciberataques y el uso de la fuerza para responder en dicha situación.

En otras palabras, si el hackeo, realizado por un delincuente o grupo delictivo, tiene como objetivo principal tomar ventaja de las vulnerabilidades del sistema financiero y robar dinero de cuentas bancarias, ha de ser tipificado como fraude o robo, a menos que el marco legal de los Estados determine algo diferente, o se identifique con precisión que un Estado es el actor o patrocinador de dicho acto. Si un grupo terrorista logra tomar el control de instalaciones estratégicas o infraestructura crítica provocando un sabotaje, dicho evento debe ser catalogado/castigado, ya sea

como acto terrorista o sabotaje; sin embargo, si un Estado realiza una ciberoperación con pleno conocimiento de causa y un objetivo político-estratégico en contra de los sistemas computarizados de otro Estado, debe de considerarse como un ciberataque, acto de guerra o acto de agresión.

Siendo la agresión la manifestación más evidente del uso de la fuerza entre Estados y la principal amenaza para la seguridad internacional, es aceptable una respuesta armada, en legal y legítima defensa. Es en el caso de agresión entre Estados, que se puede hablar de un ciberataque y justificar el uso de la fuerza como medio de defensa. Lo anterior se fundamenta en el Derecho Internacional Humanitario, el cual establece que los Estados son los únicos actores que hacen uso de la fuerza en defensa de sus intereses cuando la soberanía, supervivencia, permanencia e integridad del Estado se encuentran en riesgo.

Limitar el derecho a hacer la guerra y lanzar ciberataques es algo que permite distinguir entre "aquello que atenta contra la seguridad pública" y "un ataque a la seguridad nacional", para dar debida y legítima respuesta. Sin embargo, en el contexto actual de operaciones clandestinas, enfrentamientos indirectos, uso de apoderados (proxies) para hacer la guerra, contratos con empresas de seguridad militar privada, mayor participación de la iniciativa privada en operaciones militares, empleo del ciberespacio como campo de batalla, uso intensivo de tecnología en la guerra y dependencia en sistemas computarizados, se evidencia que existe una zona gris en donde se superponen ambas seguridades, se dificulta la atribución de los ataques, se diluye la diferencia entre paz/guerra, se recurre a actores no estatales, y se justifican medidas no convencionales para realización y la solución de conflictos.

Esta zona gris es particularmente útil en el ciberespacio ya que, por las características de los ciberataques, es difícil atribuirlos con precisión. Los ciberataques son un fenómeno relativamente nuevo y una amenaza para la seguridad nacional e internacional que deja poco espacio de maniobra legal a los Estados que los sufren. Nadie sabe cómo será el próximo ciberataque, pero se prevé que será más complejo, persistente, automatizado, dirigido, personalizado, adaptable, evasivo, furtivo, disruptivo y peligroso.

La dificultad para responder a un ciberataque: Caso SolarWinds

El hackeo sufrido por SolarWinds Inc. ha revivido el debate existente sobre cómo responder a un ciberataque. Debido a la magnitud y alcance del hackeo contra SolarWinds la sociedad estadounidense -con toda lógica, pero escasa reflexión-, pide que se contraataque con toda la fuerza del Estado. En un sentido, la respuesta demanda que todo aquel que ose atacar a los Estados Unidos (EE. UU.) reciba la fuerza de sus armas en respuesta, implementado la "Ley del Talión". De esta forma, se obtendría una defensa inicial basada en la disuasión y el miedo. Sin embargo, la reacción del gobierno estadounidense requiere consideraciones precisas y meditadas. Si bien EE. UU. destaca por su diverso, letal y completo ciberarsenal, también es evidente que su vulnerabilidad más importante es la combinación de la hiperconectividad y la dependencia digital que experimenta. Estratégicamente, el gobierno de EE. UU. reconoce que debe atender la fragilidad de la ciberdefensa si desea salir victorioso de un ciberconflicto. EE. UU. no puede utilizar su ciberpoder sin garantizar que la escalada de violencia virtual y cibernética cause un mayor daño a su enemigo. Eso requiere una defensa infalible que, en el contexto actual, no es viable.

De hecho, el presidente electo Joe Biden tiene claro que "una buena defensa no es suficiente", y declaró que es preciso interrumpir y disuadir a los potenciales adversarios de atreverse siquiera a lanzar un ciberataque, insinuando que tomará acciones ante dichos ciberasaltos. Las palabras de Biden, de alguna forma, sugieren la ofensiva como la mejor defensa.

Regulación de las operaciones en el ciberespacio

La necesidad de una regulación clara, concisa y precisa de las actividades de los diferentes actores en el ciberespacio ha sido evidenciada con la ocurrencia de eventos adversos y dañinos para algunos actores estatales y no estatales, que se han visto maniatados para responder eficazmente. Los eventos adversos incluyen actos de ciberespionaje, filtraciones de información, ciberataques personalizados y actos de revancha o demostración de fuerza. A continuación, se muestran ejemplos representativos de actos que transgreden la ley utilizando el ciberespacio:

- El hackeo contra la compañía SolarWinds, supuestamente por hackers rusos, ha reavivado el debate sobre la falta de regulación y, por ende, certeza de las

operaciones en el ciberespacio. Esto vuelve a ser un tema de debate, después de 24 años del ciberataque del grupo conocido como Moonlight Maze en contra de agencias gubernamentales y universidades de renombre. Dicho evento es considerado como "el primer ciberataque de espionaje coordinado con alcance mundial", logrando robar información clasificada y quedar, sin embargo, impune.

- En el terreno de las filtraciones de información sensible, Edward Snowden es el ejemplo más evidente de las amenazas internas existentes para las compañías. Aunque Snowden reveló información sobre los programas de espionaje e intervención estadounidenses, no dio mayores detalles sobre las herramientas o métodos que utilizan para su implementación y/u operación. En tal sentido, no hubo repercusiones contra el gobierno de EE. UU., pero sí contra Snowden.
- Los casos de Stuxnet y Saudi Aramco. En el primero, EE. UU. e Israel utilizaron al Stuxnet –troyano considerado como la primera ciberarma– para interrumpir o detener el programa nuclear iraní. Fue el ciberataque que rompió el Rubicón Digital, inició con la carrera de ciberarmamentos, y cambió la forma de hacer la guerra. De hecho, en respuesta al ciberataque con Stuxnet, Irán borró la información de miles de computadoras de la Compañía Saudi Aramco interrumpiendo todas sus actividades. Ambos eventos quedaron sin castigo a pesar de los daños e inconvenientes causados.

Las lecciones aprendidas del ciberespionaje contra SolarWinds, de ciberataques como el Stuxnet y de filtraciones de información como la de Edward Snowden, dejan en claro que las operaciones en el ciberespacio funcionan con pocas reglas de conducta aceptadas internacionalmente. El ciberespacio, como alguna vez lo dijo el presidente Obama, es "el salvaje Oeste" o un territorio sin ley, donde convergen las acciones de gobiernos, terroristas y compañías de tecnología, poniendo a prueba las fronteras de la legalidad con pocas o nulas repercusiones.

Conclusiones

Bajo las condiciones de hiperconectividad y dependencia en el ciberespacio, existen múltiples detalles de operación y funcionamiento que requieren la urgente atención por parte de los gobiernos si se quiere evitar que el libre acceso al ciberespacio y la dificultad de atribución de actos violentos e ilegales, permitan

creer que no existe diferencia entre actos de ciberseguridad pública y de ciberguerra, ni un control sobre la adquisición de las ciberarmas.

El ciberespacio es el quinto ámbito de la guerra y, en consecuencia, se debe modificar el marco jurídico internacional vigente para incluir la reglamentación de las ciberoperaciones y ciberataques. El ciberespacio no puede ni debe ser un territorio sin regulación sobre su empleo como medio para causar daño o realizar actos de guerra, ya que la impunidad resultante motivaría que nuevos actores se incorporen al cibercrimen, la violencia escale y los actos de uso ilegítimo de la fuerza queden sin castigo. ¿Hasta cuándo la comunidad internacional lo seguirá permitiendo?

Referencias:

1. Es el fundador de la Electronic Frontier Foundation, organización creada como contraparte de la aprobación de la Telecommunictions Act de 1996 en EE.UU.
2. La Declaración está disponible en: https://revistas.uca.es/index.php/periferica/article/view/943
3. Algunos reportes mencionan que se vieron afectadas más de 18000 de los clientes de las firmas, lo cual ha generado pánico entre los gobiernos por el impacto económico, político, social y tecnológico que pudiera tener. El 17 de diciembre, Microsoft había identificado 40 compañías, agencias de gobierno y think thanks que pudieron haber sido infiltrados por los hackers.
4. Para más información consultar: Sanger, D, y Perloth, N. (17 de diciembre de 2020). More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government. The New York Times. nytimes.com [Edición digital]. Consultado el 25 de diciembre de 2020, en https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html
5. En 1996, había dos grupos de ciberespionaje dominando el ciberespacio: Moonlight Maze (Rusia) y Equation Group (EE.UU.). El grupo Moonlight Maze es considerado como la primera Advanced Persistent Threat o APT, y se presume es patrocinado u organizado por el gobierno ruso. Recientemente se le ha conectado con la APT conocida como Turla.

Bibliografía:

1. Barlow, J. P. (2011). Declaración de independencia del ciberespacio. Periférica Internacional. Revista Para El análisis De La Cultura Y El Territorio, 1(10), 241-242. Recuperado el 22 de diciembre de 2020, de https://revistas.uca.es/index.php/periferica/article/view/943

2. Sanger, D, y Perloth, N. (17 de diciembre de 2020). More Hacking Attacks Found as Officials Warn of 'Grave Risk' to U.S. Government. The New York Times. nytimes.com [Edición digital]. Consultado el 25 de diciembre de 2020, en https://www.nytimes.com/2020/12/17/us/politics/russia-cyber-hack-trump.html