DERECHO INTERNACIONAL Y SEGURIDAD CIBERNÉTICA

Desde el derecho internacional resulta importante abordar un tema de actualidad como es la seguridad cibernética

En estos últimos tiempos han crecido los ataques cibernéticos, lo que hace peligrar la paz internacional, objetivo éste del derecho Internacional.

Con las revoluciones tecnológicas surge un nuevo medio o ámbito donde puede desarrollarse la guerra: el "Ciberespacio".

PALABRAS CLAVE: **CIBERESPACIO / DERECHO INTERNACIONAL / ATAQUE CIBERNÉTICO / CIBERGUERRA / DERECHO INTERNACIONAL HUMANITARIO / DERECHO DE LA GUERRA**

Por **Matilde Beatriz Grispo**

¿CÓMO SE DEFINE AL CIBERESPACIO?

"El conjunto de dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicaciones" (Kuehl, en 2009)

En ese ciberespacio, que configura un nuevo escenario estratégico, operacional y táctico, es donde la guerra ha encontrado un nuevo medio de desarrollo, es un espacio que cambia en forma constante conforme la innovación tecnológica. Es en este nuevo ámbito donde los estados deben también ejercer su soberanía.

Es un ámbito que no está sujeto a límites naturales ni geopolíticos, dado que la información va sin fronteras. Esto ha permitido adquirir un importante grado de sofisticación, pero también la incidencia de nuevos riesgos fruto de este nuevo esquema y la falta de límites ha llevado a que al ciberespacio puedan acceder en igual forma tanto los estados como los actores no estatales.

El ciberespacio admite un flujo de información en forma rápida y hacia cualquier parte del mundo en un tiempo relativamente corto, Los sistemas tradicionales precisan sistemas de armas para hacer sentir el poder territorial, naval o aéreo. En el ciberespacio, las armas no son cinéticas (motor, motriz).

En el ciberespacio también existen las armas tanto defensivas como ofensivas pero son totalmente diferentes.

Esto alude a un nuevo paradigma: la ciberguerra.

Es importante señalar que las armas defensivas están compuestas por hardware y software de seguridad, dispositivos de análisis y control de tráfico de red y son de acceso a todos los actores de la red, lo que obviamente quiebra el monopolio estatal sobre la violencia.

Estas nuevas armas poseen un gran potencial para producir grandes daños a las naciones y hasta ahora no existe un

La ciberguerra se da en el ciberespacio, un escenario nuevo que no está regulado internacionalmente, porque no se puede definir el ámbito territorial.

marco jurídico en el Derecho Internacional Público que regule la ciberguerra.

Aquí se puede afirmar que surge el primer planteo entre la ciberguerra y el Derecho Internacional Público.

Se debe analizar el tema de la ciberguerra, entenderla como un fenómeno diferente, con características totalmente distintas y ver cuál es la posibilidad que tiene el Derecho Internacional Público para darle un marco legal, teniendo en cuenta que este regula las relaciones entre los estados y las de estos con organismos internacionales, entre otros. En otras palabras, se trata de resolver desde lo jurídico los alcances del ciberespacio y con ello las implicancias de la ciberguerra.

¿Por qué es necesario que exista un marco legal que contemple la Ciberguerra? Simplemente porque hay un cierto acuerdo para limitar el concepto de ciberguerra a las actividades realizadas por los estados en el ámbito de las redes digitales y no estarían incluidas las actividades realizadas por actores no estatales en estas.

En los sistemas tradicionales, estos precisan sistemas de armas para hacer sentir el poder territorial, naval o aéreo, pero esto no es así en el ciberespacio.

Hoy no existe una definición de ciberguerra única; sin embargo se puede hacer referencia a una que tiene una aceptación general: "ciberguerra es el conjunto de actividades ofensivas y defensivas, simétricas o asimétricas, realizadas en redes digitales por estados o actores con igual status abarcando peligros potenciales para la estructura crítica nacional y los sistemas militares" (Coughlan, Shane. 2009)

Se dijo que la ciberguerra se da en el ciberespacio, un escenario nuevo que no está regulado internacionalmente, porque no se puede definir el ámbito territorial.

Por otro lado, se debe definir de dónde surgen los ataques para saber si se aplica el *Jus ad Bellum*.

Las características de Ciberguerra son las siguientes:

- la inminencia de la amenaza o la posibilidad de un ataque cibernético (se cree que la ciberguerra es algo del futuro, ya que está interrelacionado con el aumento de la interconexión de los sistemas de infraestructuras civiles y militares). Por lo tanto, resulta que los países que tienen sistemas de información precarios tienen menos posibilidades de sufrir un ataque cibernético.
- el anonimato es una de las características que ofrece ventajas y desventajas, ya que están en juego la libertad y privacidad y además se dificulta la atribución de responsabilidades. La falta de normas genera impunidad para aquellos que a través de los sistemas informáticos e infraestructuras cibernéticas del estado, los utilicen sin el consentimiento del estado y ocasionen hostilidad hacia otro estado, generando un conflicto armado.
- Falta de regulación y falta de control del ciberespacio: El problema que se plantea es que no habrá responsabilidad a nivel internacional si no se puede determinar el responsable del acto, lo mismo ocurre cuando tampoco se puede identificar el autor de una operación determinada ni el vínculo que guarda esa operación con el conflicto armado, lo que hace difícil determinar si el Derecho Internacional Humanitario es aplicable a la operación.

Es importante señalar que uno de los principios del Derecho Internacional Humanitario consiste en distinguir las partes del conflicto armado, es decir, entre combatientes y objetivos militares, civiles y bienes de carácter civil y atacar sólo a los objetivos militares o legítimos.

El problema que se plantea en el ciberespacio es que esta distinción resulta complicada ya que tanto uno como los otros, utilizan los mismos métodos para circular en la red. Por ejemplo, resulta difícil determinar la participación directa de los civiles en las hostilidades cuando operan en red de la misma forma que el combatiente aunque sus objetivos sean diferentes.

El Derecho Internacional impuso ciertas restricciones al ciberespacio. En la última década, cuando se referían al ciberespacio hablaban de falta de normas que lo regularan y permitía un avance vertiginoso ya que no había límites materiales.

Sin embargo esta posición fue cambiando cuando observaron que existían ciertas reglas de Derecho Internacional, universales y de *ius cogens* (Normas Imperativas "No admite acuerdo en contrario" Estado comete acto contrario al "*ius cogens*", acto nulo Objetivo proteger el interés colectivo de la comunidad internacional y lograr el oren público internacional), a las cuales no podían renunciar y que también eran aplicables en este ámbito y entre las que se encontraba el Derecho Internacional Humanitario.

Hoy resulta difícil admitir la existencia de un derecho consuetudinario que pueda aplicarse al ciberespacio por lo que su regulación jurídica proviene de normas convencionales.

DERECHO INTERNACIONAL HUMANITARIO

Es un conjunto de normas internacionales de origen convencional y consuetudinario, específicamente destinado a ser aplicado en los conflictos armados, internacionales o no, que limita por razones humanitarias, el derecho de las partes en conflicto a elegir libremente los métodos o modos y medios (armas) para hacer la guerra y que protege a las personas y los bienes afectados o que puedan resultar afectados por ella.

Se pueden plantear los siguientes interrogantes:

1. ¿Hasta qué punto las ciberoperaciones se encuentran bajo la protección del Derecho Internacional Humanitario?

2. ¿Van a ser determinantes en la consecución de la guerra o como mecanismo autónomo cuando éstas generen hostilidad?
3. ¿Van a ser las ciberoperaciones una amenaza para la paz y la seguridad internacional o un uso de la fuerza?
4. ¿Puede el Consejo de Seguridad tomar medidas que incluyan Fuerzas Militares para mantener y restablecer la paz?

Es necesario definir qué son las ciberoperaciones, cuáles son sus objetivos y sus efectos y si están contempladas en el Derecho Internacional Humanitario.

Las ciberoperaciones son aquellas operaciones realizadas contra un ordenador, mediante un ordenador o un sistema informático, utilizando para ello el flujo de datos.

Pueden tener distintos objetivos: infiltrar un sistema informático y recopilar, destruir o encriptar datos, entre otros, es decir, la tecnología puede utilizarse en la guerra y estas operaciones pueden constituir ataques contemplados en el Derecho Internacional Humanitario.

Las Ciberoperaciones en sí mismas no tienen por qué producir un conflicto armado entre las partes o una hostilidad, pero en cambio los ciberataques pueden dar lugar a un conflicto armado entre dos partes organizadas.

Es necesario distinguir cuidadosamente la terminología que se utiliza para las operaciones desarrolladas en el ciberespacio de la terminología técnica que se utiliza en el Derecho Internacional, como fuerza, ataque armado o ataque.

El Derecho Internacional Humanitario sólo entra en juego cuando las operaciones cibernéticas se cometen en el marco de un conflicto armado, sea entre estados, entre estados y grupos armados organizados, o entre grupos armados organizados.

Las ciberoperaciones pueden originar un conflicto armado, cuando estas originan una hostilidad entre varias partes con intereses contrapuestos y pueden derivar en un ciberataque, cuando la ciberoperación lleva implícita el uso de la fuerza.

CIBERATAQUES Y CONFLICTO ARMADO

¿Cuáles son los problemas que se presentan con estos nuevos escenarios y los conceptos jurídicos que ya existen y que conforman el Derecho Internacional Humanitario?

En primer lugar, cuando se habla de Conflicto Armado, este no fue definido en forma expresa, ya que no surge de ninguno de los convenios de Ginebra (1949) ni tampoco de sus Protocolos Adicionales (1977). Sólo cabe señalar que en el marco del Protocolo Adicional a los Convenios de Ginebra relativo a la protección de las víctimas de los conflictos armados sin carácter internacional (Protocolo Adicional II), se señalan los requisitos de aplicación de dicho tratado, pero no lo define.

Resulta difícil determinar la participación directa de los civiles en las hostilidades cuando operan en red de la misma forma que el combatiente aunque sus objetivos sean diferentes.

«Se recurre a la fuerza entre estados o hay una situación de violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre estos grupos dentro de un Estado»

Pero se ha considerado, para darle un concepto o una interpretación, lo que la doctrina, la práctica de los propios estados y la jurisprudencia internacional consideraron relevante para definir el conflicto armado.

Se puede citar:

La postura que surgió de la posición adoptada por el Tribunal Penal para la ex Yugoslavia, en el caso de Dusko Tadic:

«Se recurre a la fuerza entre estados o hay una situación de violencia armada prolongada entre autoridades gubernamentales y grupos armados organizados o entre estos grupos dentro de un Estado»

También el Tribunal Penal para Ruanda ha señalado en los casos Akayesu y Musema que el término ***"Conflicto Armado" en sí mismo sugiere la existencia de hostilidades entre las Fuerzas Armadas organizadas en mayor o menor medida".***

Así caracterizado el Conflicto Armado surgen al menos cuatro elementos:

- La fuerza o violencia armada
- La prolongación en el tiempo
- La organización del grupo que participa en el conflicto
- La inclusión del conflicto armado entre grupos junto al de las tradicionales nociones de conflicto armado internacional o no internacional entre la autoridad estatal y un grupo armado

Resulta difícil definir el tema con relación a las ciberoperaciones, porque operan de diferentes formas, no siguen un patrón fijo de actuación, por lo cual se necesita para cada caso realizar un análisis para determinar si dichas ciberoperaciones constituyen un conflicto armado y qué principios del Derecho Humanitario le son aplicables.

Otro punto importante es considerar si el término "fuerza", tal como es entendido en el Derecho Internacional Humanitario, es aplicable a las ciberoperaciones, cuando estas no causan muertes, ni heridas, ni destrucción. ¿Por qué es importante? Porque permite determinar la legitimidad del uso de ***la Legítima Defensa***, dado que si no hay fuerza, no

pueden emplearse las medidas de la legítima defensa. Quizás hay que buscar las medidas proporcionales.

Si se interpreta en forma literal el Derecho Internacional, se puede concluir que no se puede considerar a las ciberoperaciones como un ataque armado y, por lo tanto, no sería de aplicación de ninguna manera la legítima defensa. Ello no quita la posibilidad de que genere un conflicto armado.

Las ciberoperaicones pueden dar lugar a un conflicto armado, es por ello que hoy la comunidad internacional se ha visto en la necesidad de fijar unos requisitos que nos permitan distinguir, a la luz de los hechos ocurridos, si se está o no ante un supuesto en el que los actores involucrados se ven obligados al desarrollo de hostilidades conforme los principios del Derecho Internacional Humanitario.

En todo este tiempo se ha incrementado la cantidad e incidencia práctica de las ciberoperaciones.

- En 2007, la aviación israelí bombardeó una instalación nuclear secreta en Siria. El ataque aéreo fue precedido por un ciberataque que engañó a los sistemas de defensa aérea y, por lo tanto, impidió detectar la incursión de los aviones en el territorio sirio.
- El 27 de abril de 2007, en medio de los roces existentes entre nacionalistas estonios y rusos, el sector público y privado del estado fueron víctimas de una campaña de Ciberguerra que afectó las estructuras críticas del país durante varias semanas, entre las cuales había sitios del gobierno, periódicos y entidades bancarias. Estonia no fue el primer país pero sí lo fue en gran escala, y el arma utilizada para el ataque fue la "negación de servicio distribuida" que persigue la caída de los sitios elegidos como blancos que bombardean con falsos pedidos de información. Los ataques tuvieron origen en varios países como ser Egipto, Perú y Rusia, pero Estonia denunció a Rusia diciendo que tenía pruebas que jamás presentó. Un mes después de los ataques, se concluyó que posiblemente los atacantes fueron bandas de hackers con motivación política y no agencias del gobierno ruso, pero un famoso hacker ruso reconoció que los ataques no podrían haber sido posibles sin la colaboración de las autoridades rusas.

  En consecuencia, nada pasó porque no hubo posibilidad de determinar de manera fehaciente quién había sido el atacante. Sin embargo, sirvió para alertar a la OTAN por su falta de prevención y de poder para detener ese nuevo tipo de enfrentamiento.
- El 8 de agosto de 2008, en medio de acciones separatistas por parte de provincias pro rusas, La Federación Rusa lanzó un asalto militar contra Georgia. Un día después el foro Stopgeorgia.ru Project fue creado y contaba con 30 miembros. Este foro tenía un grupo de hackers experimentados y ofrecía una lista de 37 blancos informáticos de alto valor que podían ser alcanzados desde direcciones IP de Rusia o Lituania. También proveía las guías necesarias para atacar la infraestructura informática de Georgia. Según Rusia, Georgia fue el primero en efectuar un ciberataque contra Rusia y lo presentó como un ataque estatal y no como un ataque civil. Sin embargo, no pasó nada.
- En enero de 2009, aviones de combate franceses no pudieron despegar de sus portaviones ya que su sistema electrónico fue desactivado por un virus informático.

Muchos autores han considerado que siempre que haya una guerra, un conflicto armado, deben ser aplicadas las normas del derecho de la guerra, independientemente de cómo se desarrolla.

CONCLUSIONES:

El desarrollo tecnológico ha determinado nuevos conflictos con características propias, que generan nuevos escenarios, por lo que es necesario la adaptación de las normas a esta nueva realidad.

La ciberguerra se da en un ámbito, el ciberespacio, que goza de sus propias características, que no contempla el Derecho Internacional.

Muchos autores han considerado que siempre que haya una guerra, un conflicto armado, deben ser aplicadas las normas del derecho de la guerra (Derecho Internacional Humanitario), independientemente de cómo se desarrolla dado que existen reglas universales, que tienen que regir en todos los ámbitos. ¿Se puede considerar que la ciberguerra constituye un conflicto armado conforme el Derecho Internacional Humanitario?

La ciberguerra requiere un tratamiento normativo propio que se adapte a sus características.

Matilde Beatriz Grispo
Abogada, Mediadora, Especialista en Derecho Penal (Criminologia) - Universidad de Buenos Aires. Especialización en Docencia Universitaria en Ciencias Empresariales y Sociales UCES. Magister en Políticas Públicas EPOCA - USAL y UNIVERSIDAD CARLOS III DE MADRID – Docente del Instituto de Inteligencia de las FFAA, docente de Gendarmería Nacional. Dicta la materia de Derechos Internacional y Ciberguerra en el Curso de Ciberguerra que se dicta en el Instituto de Inteligencia de las FFAA, entre otras. Secretaria de la Comisión del Derecho del Mar del Colegio Público de Abogados y Secretaria de la Comisión de Mediación del Colegio de Abogados de la Ciudad de Buenos Aires.

〉 ARTÍCULO CON REFERATO