# GEOPOLITICA Y CIBERSEGURIDAD

**Por María Celsa Rodríguez Mercado ***

**Resumen:**

En un principio la geopolítica tuvo como objeto causas geográficas, con el tiempo se fueron desarrollando otras cuestiones que atañen a un tema de agenda política que se atiende con importancia. Hoy la ciberseguridad forma parte de la problemática. Hay nuevas cuestiones que influyen en la relación con los vecinos y con el mundo.

Porque la integración territorial del Estado hoy va más allá de su territorio cuando hablamos del ciberespacio. Los límites de la estrategia ya es un eslabón determinante que los líderes del mundo lo han entendido. El teatro de operaciones ya no tiene límites ni fronteras. Por ello el compromiso de la OTAN en 2010 fue de "disuadir y defenderse de cualquier amenaza de agresión y de los desafíos de la seguridad emergente, cuando estas supongan una amenaza a la seguridad fundamental de los aliados individualmente o de la alianza en su conjunto".

El cibercrimen juega un papel importante en los sistemas financieros y el ciber terrorismo que atentan contra los sistemas electrónicos destruyendo las comunicaciones y las computadoras por medio de virus, es de vital interés protegerlos y darle un mecanismo de defensa más sofisticados al estar en constante evolución no solo sus atacantes sino también sus herramientas de prevención y defensa.

## Introducción:

Los límites de la estrategia ya es un eslabón determinante que los líderes del mundo lo han entendido. Mientras los países latinoamericanos empujados por las ideas que fueron vitaminizadas desde el Foro de Sao Paulo, -un centro castrista, chavista y comunista-, ha considerado a la seguridad interna como externa, una amenaza, impulsando su debilitamiento, y dejando en estado agónico la defensa de los países que se escudaron en las ideas del Socialismo del Siglo XXI mientras el campo de batalla se concentra en las guerrillas, el narcotráfico, el Hezbollah, Isis y Hamas.

Raymon Aron dice acerca de la guerra asimétrica que "este tipo de amenazas ha proliferado como consecuencia del desplome del sistema bipolar de la guerra fría y el ingreso de una

nueva etapa de la civilización. Los combatientes de antiguas bandas revolucionarias han devenido en bandos criminales equipados con elementos de tecnología satelital que les permiten constituirse en modo de una red mayor, en la que circulan las diversas actividades del nihilismo pos moderno: guerrilla, narcotráfico, tráfico de armas, guerras en la infosfera, contrabando, tráfico de órganos, tráfico de niños, esclavismo, tráfico de piedras preciosas, terrorismo islámico, etnocidio, genocidio, etc.

Hoy se debe estructurar un sistema que regule un diseño de estrategia desde la defensa ante los ciberataques donde somos más vulnerables a los hackers que con tecnología superior y conocimientos elevados, explotan tácticas de rastreo y espionaje violando toda seguridad digital.

El teatro de operaciones ya no tiene límites ni fronteras. Por ello el compromiso de la OTAN en 2010 fue de "disuadir y defenderse de cualquier amenaza de agresión y de los desafíos de la seguridad emergente, cuando estas supongan una amenaza a la seguridad fundamental de los aliados individualmente o de la alianza en su conjunto".

Cabe aclarar que cuando se dice "cualquier amenaza" esto se dirige: al terrorismo incendiario, los lobos solitarios, el terrorismo de armas biológicas, los ataques cibernéticos, las amenazas cibernéticas, amenazas tecnológicas y ambientales, o robo de información clasificadas.

**Cuestión de Defensa:**

La Planificación de la Defensa se centra por ello no solo en armas  sino también en los equipos de comunicación altamente calificada donde los drones y equipos de vuelo no tripulados utilizan las tácticas  de defensas y espionaje para operaciones especiales

Según la Unión Internacional de Telecomunicaciones, organismo especializado de las Naciones Unidas  para las tecnologías de la Información y de la Comunicación:

“La ciberseguridad es el conjunto de herramientas políticas, concepto de seguridad, salvaguarda de seguridad, directrices, métodos de gestión de riesgos, acciones, prácticas idóneas, signos y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en los ciber entornos.

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios o aplicaciones, los sistemas de comunicación en la comunicación multimedio y la totalidad de la información transmitida y/ o almacenada en el ciber entorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad contra los riesgos de seguridad correspondiente en el ciber entorno. (Unión Internacional de Telecomunicaciones 2008)

Asimismo “la agencia de la Unión Europea para la Seguridad en la Red y de la Información ENISA dice que la elaboración de inteligencia sobre amenazas de origen cibernética constituye un desafió esencial para los responsables de la seguridad”.

Analizando, “las ciberamenzas apuntan a diferentes objetivos: La sociedad civil, el individuo, las empresas, los interés económicos y los Estados”. Dentro de los Estados las causas pueden ser motivo de ataques terroristas, crear conflictos, ser un núcleo criminal, un sabotaje técnico y producir efectos en los servicios del Estado”. [1]

Para mantener una confianza perdurable en el área tecnológica en materia de operaciones militares se requiere que se generen un aumento considerado en el valor que tiene la ciberseguridad para armar las infraestructuras de información militar con una adecuada cadena de mando y un manejo del control y riesgos en los sistemas de armas que está bajo el control de la red de línea del ciberespacio, el llamado C41.

“Al respecto el Mayor Orón Mincha de la División de Telecomunicaciones del Ejército israelí y miembro del Directorio C41 dijo: “En el ciberespacio hay una amplia variedad de herramientas para cometer ataques y nuestra labor es siempre estar dos pasos por delante”. Miles de ataques diarios ocurren en el ciber espacio porque como dice Mincha “la ciberseguridad no es el futuro sino el presente… somos los que prevenimos en esa nube

para que puedan comunicarse con todos, puedan hablar con todos y enviarse información… El ciberataque está cambiando la forma y apariencia que tendrá la guerra del futuro y puede que mate o no a la gente o que lo haga a posteriori - por ejemplo si el ataque neutraliza la electricidad en un hospital- por lo que no hay duda que se trataría (de una agresión) que abra el camino hacia una anarquía dentro de un país".

Hay que tener en cuenta que el ciberdelito es un arma que también atenta contra la economía de un país pero que es muy redituable para los atacantes que tienen un objetivo dinerario. Es más redituable que el narcotráfico porque los hackers venden datos personales que son usados diariamente en internet por millones de personas, datos de tarjetas de crédito y débito en las transacciones personales donde se cruzan millones por día. Cada dato personal se cobra 3 dólares. Pero los datos gubernamentales son los más cotizados.

El Ransomware es un programa que tiene la particularidad de encriptar archivos y terminan por bloquear el ingreso de esos datos, y luego para poder acceder a los archivos piden rescates para habilitar esos archivos, lo hacen también con los celulares.

**¿Cuáles son los ataques que utilizan los hackers, donde los mecanismos de seguridad deben poner la atención?**

La Red Eléctrica;

Las Plantas Nucleares;

La Red de Comunicaciones;

Aeropuertos Internacionales;

Sistemas de Seguridad Nacional;

Bancos;

Estaciones de trenes,

Software mal intencionado: - Other;

- Adware Spyware;

- Worms;

- Virus;

- Troyanos.

En 2012, la Armada de Chile aprobó el proyecto DIPRIDA que renueva material, C41 de mando, control, computación e Inteligencia. Trabaja en la conformación de un sistema de defensa misilístico para alcanzar blancos en tierra como los misiles híbridos LORA (Long Range Artillerg) de la Israelí MALAM de IAI.

Sabemos que las Fuerzas armadas ven al ciberespacio como una unidad de ciberdefensa militar en el cuál convergen los sistemas de información y comunicación (CIS) y la guerra electrónica (EW). Esto es un dominio en expansión constante.

En el libro "Seguridad y defensa nuevos medios para nuevos escenario" Podemos encontrar por ejemplo ciertos hechos que nos revelan cómo funcionan los ciberataques y los instrumentos de defensa:

"En el año 2007 en Estonia cuando las páginas oficiales de varios departamentos del Gobierno, Bancos y Prensas quedaron bloqueados totalmente por ciberataques del exterior, con posible origen en Rusia, consistente en ataques distribuidos de desviación de servicios, DDos. El detonante del ciberataques se debió a que la estatua conmemorativa de la historia rusa en la segunda guerra mundial colocada en el centro de Tallin durante la ocupación soviética fue traslada a un cementerio militar. Aunque Estonia solicitó a la OTAN incluso la aplicación del art 5º finalmente no se ejecutó si bien experto en Ciberdefensa de la organización acudieron en su ayuda. A raíz de los anteriores y ante los nuevos temores de una agresión rusa a los países bálticos, surgieron varios debates acerca de los compromisos exigibles a la OTAN sobre la garantía de protección basada en dicho artículo que establece la defensa mutua entre los aliados".

De mayor importancia desde el punto de vista de las operaciones militar fue el conflicto armado entre Georgia y Rusia en el verano de 2008. Las ciber operaciones militares evolucionaban acorde con el planeamiento de las maniobras de los combates armados de las Fuerzas Terrestres y para ello necesitaban adquirir continuamente inteligencia. Las ciberoperaciones cuya atribución tampoco ha sido reconocida por Rusia hasta ahora fueron conducidas en coordinación con las operaciones armadas y sirvieron para debilitar eficientemente la capacidad de respeto militar y política de Georgia.

Otro ejemplo de actividad de ataque físico y al mismo tiempo de influencia, es el del soldado analista de inteligencia de Estados Unidos acusado de filtrar a Wikileaks material clasificado. Entre ese material se encontró un vídeo en el que se ve como un helicóptero estadounidense mató a un grupo de civiles en Irak donde se encontraba 2 periodistas de la agencia Reuters. Es sospechoso además de haber filtrado otros documentos clasificados acerca de las guerras de Afganistán y de Iraq así como unos cables diplomáticos de los embajadores estadounidenses.

Por ello fue acusado oficialmente de “ayudar al enemigo”.

Otro caso relacionado con lo anterior y muy significativo es el de confidencialidad y “lealtad debida” en este nuevo dominio que constituye el Ciberespacio. Nos referimos en particular al ex técnico de la CIA y ex Consultor de la Agencia Nacional de Inteligencia de Estados Unidos.

Este ingeniero que trabajó durante cuatro años en la NSA admitió ser el origen de la información revelada por los diarios The Guardían y The Washington Post, sobre programas de espionajes secretos de llamada en Estados Unidos y probablemente en el resto del mundo.

La actualidad informátiva se centra en las revelaciones sobre escuchas de telefonía móvil e interceptación de correos electrónicos en Europa no solo a organismos oficiales también a dirigentes y responsables políticos”.

La ubicación de Chile en Ciberseguridad -lo dice el NCSI-, coloca al país andino como "el primer país latinoamericano en ciberseguridad al estar en el lugar 33º de la lista".

Esto hace que Chile está más preparado para prever amenazas en su ciberespacio y poder resolver y gestionar los incidentes sin efectos mayores. Los puntos sensibles en que Chile lidera es la lucha contra el ciberdelito, la rapidez en la identificación electrónica y la protección de datos.

Por ello la inversión en Chile en esta materia es de casi 160 millones de dólares invertidos en ciberseguridad donde el punto de mayor interés se concentra en identificar el perfil de riesgo corporativo y el protocolo de respuesta a incidentes.

Las llaves de defensa y estrategias son importante para acentuar la seguridad.

"'En el prólogo de *Cypherpunks: La libertad y el futuro de internet*, Enrique Dans esboza se forma precisa lo que hace bastantes años sucede en la red: "**El ciberespacio, en todos los sentidos, se ha militarizado**. El equivalente de lo que está ocurriendo en la red situado en la calle, fuera de la red, sería directamente la ley marcial. La red y el libre intercambio de información podrían estar posibilitando un período histórico que supusiese el mayor y más vibrante progreso a todos los niveles, pero están en su lugar alumbrando la época más oscura, autocrática y totalitaria que el ser humano ha vivido jamás'"

"...El documento denominado "Estrategia Nacional Cibernética" fue anunciado en un tono intimidante por el mismo consejero de seguridad nacional, [de los Estados Unidos] John Bolton. En una rueda de prensa dijo a periodistas lo siguiente:

Vamos a hacer muchas cosas ofensivamente y creo que nuestros adversarios deben saberlo (…) Identificaremos, contrarrestaremos y disuadiremos el comportamiento en el ciberespacio que es desestabilizador y contrario a los intereses nacionales (…) América

inventó Internet. Ha traído prosperidad y productividad a las vidas estadounidenses y a las de todo el mundo. En el futuro debemos hacer más para garantizar que sea seguro y siga siendo un motor del crecimiento estadounidense… Depende de si son hostiles actuando contra nosotros, básicamente (…) Las personas que deben preocuparse por esto son las que se han tomado o se están preparando para tomar acciones hostiles en el ciberespacio contra nosotros, ya sean estados extranjeros, organizaciones terroristas, organizaciones delictivas o lo que sea"

Esto sonó como una amenaza, más allá de las estrategias diplomáticas.

El gobierno de los Estados Unidos acordó un acuerdo con el gobierno de Chile en que "ambos países se comprometen a trabajar juntos en promover y desarrollar el creciente consenso internacional en el marco de un comportamiento responsable del estado en el ciberespacio, e impulsar esfuerzos en las Américas para construir alianzas confiables entre los países de ideas afines. Ambos países además afirman la importancia de la cooperación entre estados de ideas afines para disuadir las actividades informáticas maliciosas contrarias a dicho marco.

Estados Unidos y Chile se comprometen a continuar desarrollando una estrecha colaboración en torno a la **ciberseguridad, la protección de la infraestructura crítica, de respuesta ante incidentes, la protección de datos, la provisión de tecnologías informáticas y de comunicación, la seguridad informática internacional, y la cooperación militar y entre instituciones** de aplicación de la ley a través del establecimiento de canales sólidos para la comunicación abierta en torno a los asuntos informáticos de cuidado.

El acuerdo fue contraído con delegaciones de ambos países, las cuales fueron encabezadas por dos representantes. Por su parte, Robert Strayer, subsecretario adjunto para Seguridad Informática y Comunicaciones Internacionales y Política de Información, del Departamento de Estado, encabezó a la delegación que integró a diversas agencias del gobierno de los

Estados Unidos; en tanto, el subsecretario de Defensa Cristián de la Maza encabezó a la delegación chilena".[3]

**Conclusión:**

La ciberseguridad es una materia de profunda importancia para los gobiernos del mundo. Y comprende un tema de agenda en función de la seguridad interna y externa donde la ciberguerra que busca recopilar información con entornos políticos, el cibercrimen en que juegan un papel importante los sistemas financieros y el ciber terrorismo que atentan contra los sistemas electrónicos destruyendo las comunicaciones y las computadoras por medio de virus, es de vital interés protegerlos y darle un mecanismo de defensa más sofisticados al estar en constante evolución no solo sus atacantes sino también sus herramientas de prevención y defensa.

**Referencias:**

[1] Seguridad Nacional, amenazas y respuestas de Luis la Corte Ibañez

[2] https://www.fayerwayer.com/2018/09/politica-trump-ciberataques-extranjeros/

[3] https://www.fayerwayer.com/2018/09/chile-ee-uu-acuerdo-ciberseguridad

** María Celsa Rodríguez Mercado es abogada, bloguera, escritora, analista política, columnista en distintos medios internacionales, analista del Circulo Acton Chile, y Vicepresidente de la Fundación Internacional Latinoamérica Libre.*