Seguridad Multidimensional y las Nuevas Amenazas: Cibercrimen, ciberespionaje y ciberguerra como nuevas amenazas en la seguridad

Por Olga Ramírez Poggi (*)

Actualmente, el Hemisferio enfrenta tanto amenazas tradicionales a la seguridad como nuevas amenazas, por esas razones la seguridad debe tener un carácter multidimensional. Tenemos como base fundamental la Carta de Naciones Unidas y la Carta de la OEA.

Bajo este concepto de seguridad con alcance multidimensional tenemos desafíos que son prioridades para todo Estado en el Hemisferio por ejemplo: la consolidación de la paz que es un valor en el cual se basa la democracia, la justicia, el respeto a los derechos humanos, la solidaridad, la seguridad y el respeto al derecho internacional.

Asimismo, se necesitan mecanismos de cooperación entre estados para enfrentar las amenazas tradicionales como las nuevas amenazas y otros desafios que enfrenta el Hemsiferio.

Cada Estado, va a determinar cuáles son sus prioridades nacionales de seguridad y según eso definirá sus estrategias, planes y acciones.

Tenemos que mencionar algunas condiciones vitales para la estabilidad y paz en el hemisferio por ejemplo: la democracia representativa, las libertades fundamentales, la buena gestión gubernamental, la promoción del desarrollo económico, social y humano, la inclusion social, la educación, la lucha contra la pobreza, la hambruna y las enfermedades.

Las amenazas tanto tradicionales como nuevas amenazas de alcance multidimensional incluyen aspectos, económicos, politicos, sociales, ambientales y de salud. Y muchas de éstas amenazas son de naturaleza transnacional por lo que la cooperación es indispensable para combatirla. Por ejemplo entre estos nuevos desafíos de diversa naturaleza tenemos: el terrorismo y el terrorismo biológico, la delincuencia organizada transnacional, la corrupción, narcotráfico, lavado de activos, tráfico de armas, la pobreza extrema y exclusión social, los desastres naturales y los de origen humano como las pandemias, la trata de personas, el riesgo del transporte marítimo de materiales, la posesión y uso de armas de destrucción masiva, migraciones no controladas, la delincuencia cibernética y las amenazas a la infraestructura crítica, seguridad para el transporte y seguridad portuaria, etc.

Definitivamente cada Estado tiene tanto problemas internos como externos que afectan al resto de países como por ejemplo: el crimen organizado. Pero para esto, los Estados establecen sus prioridades por lo que es indispensable basarnos en el análisis de la magnitud de la amenaza y darle la dimension adecuada, identificar claramente los problemas que enfrentamos y darle la verdadera prioridad a los problemas que merecen tenerla. Los intereses circunstanciales de cada Estado no deben dejar de admitir los problemas que atraviesa el país.

Los Estados estamos llamados al diálogo para la solución pacífica de situaciones de conflictos tanto internos como externos con pleno respeto a la integridad territorial y a la soberania de los Estados, no olvidemos que la transparencia en las políticas de defensa y seguridad son la base de la confianza y la seguridad en el hemisferio.

Una forma de lograr la paz y seguridad en el hemisferio es el fortalecimiento de los acuerdos y mecanismos bilaterales y subregionales de cooperación en material de seguridad y defensa. Asimismo, existe un tratado para la proscripción de las Armas Nucleares en América Latina y el Caribe (Tratado de Tlatelolco) y sus protocolos. También debe haber un compromiso de parte de los Estados con el control de armamentos, el desarme y la no proliferación de todas las armas de destrucción en masa y la aplicación de los Estados de la Convención sobre la Prohibición de Desarrollo, la Producción y el Almacenamiento de Armas Bacteriológicas (biológicas) y Toxínicas y sobre su destrucción y el tratado de no Proliferación de Armas nucleares. Por lo que muchos Estados deberían limitar sus gastos militares e invertirlos en sus problemas prioritarios.

En el Perú enfrentamos diferentes tipos de amenazas la primera que quiero mencionar es la delincuencia organizada transnacional que atenta contra las instituciones de los Estados y contra nuestra sociedad, se necesita fortalecer las leyes y tener una cooperación multilateral mas activa con los Países vecinos por ejemplo a través del intercambio de información, la asistencia juridica y la extradición de forma rápida. Asimismo, no quiero dejar de mencionar de las obligaciones contraidas por los Estados en la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional y sus tres protocolos, sobre el lavado de dinero, el secuestro, el tráfico ilícito

de personas, la corrupción y crímenes relacionados a los mencionados. En el Perú, se está trabajando para tener transparencia en las insttuciones financieras, públicas y privadas y poder disminuir el lavado de activos en nuestro país.

Asimismo, enfrentamos problemas de años anteriores que se han ido transformando como el terrorismo que fue terrible entre los años 1980 y 1997 (Sendero Luminoso y El MRTA) que dentro de mi punto de vista se ha convertido en narcoterrorismo.

Asimismo, el abuso del medio ambiente y de los recursos naturales que son fundamentales para nuestra subsistencia y no podemos dejar de mencionar los desastres naturales causados por el cambio climático ya que somos un país que ha sufrido variaciones climáticas extremas que se han ido evidenciando a lo largo de los años. Existen diferentes estudios e informes que encierran, desde el retroceso de los Glaciares hasta los efectos del Fenómeno, El Niño. Asimismo, y por último quisiera mencionar la inseguridad ciudadana producto de la pobreza extrema, la falta de educación y la alta tasa de desempleo en el país.

Para enfrentar tales males necesitamos fortalecer la ley y mejorar la cooperación con nuestros vecinos a través del intercambio de información, asistencia jurídica y extradiciones rápidas.

Ante cada amenaza, los Estados deben reconocer primero su dimensión exacta e identificar claramente el problema para darle la prioridad que le corresponda. Y una forma de lograr la paz es fortaleciendo y apoyándose en los acuerdos y mecanismos bilaterales y multilaterales de cooperación. Por ejemplo, para encarar con éxito el problema de la inseguridad ciudadana, el Perú bien puede apoyarse en la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos complementarios. Dicho tratado se complemente además con tres protocolos dirigidos a combatir el lavado de dinero, el secuestro, el tráfico ilícito de personas, la corrupción y otros crímenes relacionados.

Por ejemplo: El Comando conjunto de las fuerzas armadas tienen la misión de la Conducción de las Operaciones y Acciones Militares de las Fuerzas Armadas, enmarcadas en el respecto al Derecho Internacional Humanitario.

En la Labor internacional: El Perú, en su calidad de miembro fundador de la Organización de las Naciones Unidas, ha tenido un alto nivel de participación en las misiones de paz, colaborando con tropas para los Cascos Azules. El Perú ha enviado tropas del Ejército, la Marina y la Fuerza Aérea. En la actualidad participa con personal militar que se desempeña como Observadores Militares, miembros de Estado Mayor e integrantes del Contingente Militar denominado; "Compañía de Infantería Perú. Asimismo, el Perú ha colaborado con tropas para los Cascos Azules, desde Junio de 1958, cuando los primeros militares peruanos viajaron al Líbano para participar en la Misión de Observadores de las Naciones Unidas en Líbano (UNOGIL). Allí permanecieron hasta diciembre de ese año. Posteriormente en noviembre de 1973, un numeroso grupo de oficiales y suboficiales llegó al Medio Oriente para tomar parte en la Fuerza de Emergencia de las Naciones Unidas II (UNEF II) que había sido establecida por el Consejo de Seguridad un mes antes, a raíz del conflicto que estalló entre Egipto e Israel, los militares peruanos – parte de un contingente internacional de siete mil hombres - integraron el reconocido "Batallón Perú.

En la Defensa Nacional: Las fuerzas armadas también enfrentan el problema del Valle de los ríos Apurímac, Ene y Mantaro (VRAEM) el cual se expresa en la presencia de tres elementos interrelacionados que lo convierten en una realidad muy complicada:

- **Pobreza y Pobreza Extrema:** La mayoría de la población del VRAEM (76.1%), se encuentra en situación de pobreza, porcentaje que duplica el promedio nacional. La pobreza extrema, alcanza a la mitad (50,1%) de los pobladores del valle, en tanto que, a nivel nacional al 13,7% de los peruanos.

- **Tráfico ilícito de drogas:** La presencia del narcotráfico se expresa en el creciente incremento del número de hectáreas de producción ilegal de hoja de coca. Existían 16,019 has de hoja de coca en el 2007 (8,100 has en 1999), con una producción de alrededor de 51,000 TM de hoja de coca, con un desvío de 11,000 TM de insumos químicos y con una capacidad potencial de producir 137 TM de cocaína.

- **Terrorismo:** Los remanentes de "Sendero Luminoso", mantienen su accionar violento en el marco de un limitado discurso político-terrorista y valiéndose de su conocimiento de la zona y experiencia en asesinatos, se han involucrado en el tráfico ilícito de drogas, para brindar seguridad en su traslado así como en el de insumos; e inclusive, cultivan hoja de coca, procesan y comercializan clorhidrato de cocaína, lo que les permite disponer de una importante fuente de financiamiento y mayor influencia sobre la población. Asimismo, existe una ley que establece beneficios por colaboración eficaz en el ámbito de la

criminalidad organizada ley nº 27378 y beneficios por colaboración eficaz asimismo medidas de protección para aquellos ciudadanos que deseen acogerse a esta ley.

La participación de las FFAA también se circunscribe en apoyo a la PNP cuando se sobrepase la capacidad operativa de esta, el accionar de FFAA estará dirigido a garantizar el funcionamiento de Entidades, Servicios Públicos Esenciales y resguardar Puntos Críticos Vitales. De la misma manera también apoya a la PNP en temas de tráfico ilícito de drogas, terrorismo, protección de instalaciones estratégicas para el funcionamiento del país y servicios públicos esenciales y en otros casos constitucionalmente justificados en que la capacidad de la Policía sea sobrepasada en el control del orden interno; sea previsible o existiera el peligro de que esto ocurriera.

De la misma manera, el Comando conjunto de las fuerzas armadas tiene la misión de la erradicación de la minería ilegal e informal, así como participar en las acciones de apoyo a la zona de desastres naturales y acciones cívicas humanitarias.[1]

En mi opinión, los riesgos que enfrentan las fuerzas armadas dependen de las funciones que se les asignen. Si estas no están claramente definidas y reguladas siempre hay riesgo de:

- Exceder el mandato y generar una contingencia de Derechos Humanos o legal en general
- Emplear los recursos fuera de los fines presupuestales aprobados,
- Exponer al establecimiento militar a circunstancias políticamente comprometedoras o a tareas para las que no son idóneos (apoyo directo al desarrollo económico, funciones policiales directas o asistencialismo social)

El surgimiento de nuevas franquicias criminales y terroristas híbridas en América Latina presenta una amenaza de seguridad de primer nivel. En muchos casos estas organizaciones operan bajo amplia protección estatal y contraminan la gobernanza democrática, la soberanía, el crecimiento económico, el comercio y la estabilidad de los países. Con el fin de la Guerra Fría se dió el fin negociado de varios conflictos armados y el desmoronamiento del marxismo, la mayoría de grupos armados se insertaron en el proceso democrático. Sin embargo, no fue así para todos los grupos, y actualmente se ve una vez más el patrocinio de grupos armados no estatales en América Latina bajo el estandarte de la "Revolución Bolivariana."

Durante las dos últimas décadas ha existido interacción entre grupos del COT[2] a través de varios continentes y se evidenciado el flujo de cocaína sudamericana, a través de Venezuela, hacia el África Occidental pasando por Mali, Guinea Bissau, y otros estados frágiles, con posibilidades de beneficiar no sólo a las estructuras tradicionales del COT de la región, sino también a entidades terroristas. Las situaciones anteriormente descritas indican la existencia de múltiples grupos, tanto terroristas como criminales y también algunos estados extra-regionales, que están ampliando y profundizando sus relaciones, lo cual sugiere que la tendencia podría extenderse más allá de Latinoamérica. Asimismo, podemos afirmar que existe una profundización de la penetración de los estados por el COT.

De la misma manera, el COT es capaz de producir daños considerables al sistema financiero mundial al subvertir los mercados legítimos. Asmimo, los grupos terroristas e insurgentes buscan cada vez más financiamiento y apoyo logístico por medio del crimen y las redes criminales. Por lo tanto, podemos afirmar que los Estados criminalizados usan frecuentemente al COT como especie de estrategia de gobernanza.

A medida que se van consolidando las relaciones estatales, los conductos criminales-terroristas recombinantes se arraigan más y por ende son más peligrosos. Dentro de éste ambiente, se abren una cantidad de opciones, desde la venta de armas, el uso de aviones del estado, hasta el fácil acceso a las estructuras bancarias por lo que los gobiernos no pueden controlar el tráfico de drogas, armas, etc.

Estos mercados ilegales están dominados por redes ágiles, multinacionales y con abundantes recursos que vienen potenciados por la globalización por lo que hay que considerer que no hay límites geográficos, los gobiernos están limitados por su soberanía, los incentivos para superar las barreras puestas por los gobiernos son gigantescos y las redes prescinden de la burocracia. Ante este fenómeno lo importante son conceptos de soberanía más flexibles, fortalecimiento del multilateralismo, establecimiento de nuevos mecanismos e instituciones y mejorar la regulación.

El control de grandes extensiones de territorio en América Latina por los grupos no-estatales, facilita el movimiento de productos ilegales por medio de redes de conductos transcontinentales y a su vez contramina la estabilidad de

[1] http://www.ccffaa.mil.pe/menuDESARROLLO/accivicas.hml

[2] COT: Crimen Organizado Transnacional

una región. La amenaza crece cuando los grupos criminales/terroristas anidan dentro de los gobiernos que se alinean ideológicamente, como es el caso de Irán y los estados bolivarianos de América Latina, que han sido identificados como patrocinadores de grupos designados como terroristas y narcotraficantes.

Las Amenazas del COT constituyen sólo una parte de las amenazas geoestratégicas que están surgiendo para EE.UU. Los Estados criminalizados actualmente están extendiendo su asimiento sobre el poder a medida que van fortaleciendo sus alianzas con estados externos hostiles y actores cuasi-estatales como son Irán y Hezbollah. Actualmente, se han dado claras declaraciones de intensión por los estados bolivarianos de ayudar a Irán en sus esfuerzos por esquivar el régimen de sanciones establecidas por mandato internacional.

Los Actores armados no-estatales se definen en: grupos terroristas, organizaciones criminales transnacionales, milicias, insurgencias (En Colombia y Perú han sido denominadas grupos terroristas por Estados Unidos) y cada grupo tiene características operativas distintas que deben ser comprendidas para poder apreciar el desafío que presentan. Los diferentes actores no necesariamente son aliados, y de hecho a veces son enemigos, con frecuencia forman alianzas de conveniencia.

Aún los violentos carteles de droga, que con frecuencia libran batallas territoriales, también con frecuencia acuerdan treguas, aunque la mayoría termina cuando ya no son de beneficio mutuo. Apesar que los actores no estatales conforman la mayor parte de los agentes criminales involucrados en actividades ilícitas, los actores estatales juegan un papel cada vez más importante. Dicho Papel se relaciona en parte a la disponibilidad de territorio para los conductos.

Los Grupos del COT pueden explotar las vulnerabilidades de estados débiles, pero también prosperan de servicios provistos por estados más fuertes. En tanto, la ausencia del estado puede ser producto de un intento exitoso de grupos del COT por ganar dominio local, pero puede ser también resultado de una percepción entre la población local de que el estado representa una amenaza hacia sus comunidades, su sustento, o sus intereses. Tales percepciones podrían resultar no tanto de estados débiles, como de estados fuertes o en recuperación que tratan de erradicar la corrupción. Los estados débiles y capturados son los cuales la autoridad gubernamental ha sido tomada por grupos del COT, quienes a su vez son los principales beneficiarios de los ingresos de la actividad criminal. Un ejemplo de lo mencionado es el siguiente: los dirigentes militares y políticos de Venezuela han permitido que las FARC transporte cocaína a través de Venezuela hacia el África Occidental y luego comparten las ganancias.

El apoyo más activo que brindó Venezuela a las FARC a través de Chávez y se dió cuando dicha organización se había convertido principalmente en una organización narcotraficante, dejando en segundo lugar su función de insurgencia política. Actualmente, existe evidencia de que el gobierno venezolano, bajo el mando de Chávez, está promocionando activamente a los narcotraficantes y grupos del COT/terroristas, en particular, las FARC y Hezbollah. Aunque el Brasil y el Perú no apoyan activamente a las FARC, tienen sus propios problemas con el narcotráfico, y ejercen poco control sobre sus regiones fronterizas. A Pesar de esta realidad geográfica y geopolítica, Colombia se ha propuesto un costoso esfuerzo por restablecer el control estatal en muchas regiones dentro de su propio territorio nacional. El costo sube cuando los grupos criminal/terroristas como las FARC se convierten en instrumentos de la estrategia política regional de un estado.

América Latina, no es vista generalmente como parte del fenómeno de regiones apátridas, presenta múltiples amenazas centradas en estados criminalizados, su alianza híbrida con patrocinadores extra-regionales del terrorismo y actores no-estatales del COT. En zonas fuera del control gubernamental, el estado es ineficaz, lo que contribuye al problema de la gobernanza debido a corrupción y negligencia. Hoy en día existe evidencia contundente de que los estados del eje bolivariano, bajo el liderazgo de Venezuela, toleran el incremento de actividad criminal en sus territorios y auspician a grupos armados no-estatales.

Es imperativo que la comunidad de inteligencia, las fuerzas armadas, y las agencias de orden público desarrollen un entendimiento mucho más profundo y matizado de la manera cómo los estados criminalizados/grupos del COT/terroristas y los estados hostiles y los actores extranjeros no-estatales explotan los espacios no gobernados. Por lo tanto, una estrategia eficaz para combatir el COT debe basarse en una fundación sólida de inteligencia regional, la cual, aunque conocedor de los vínculos regionales primordiales. Actualmente existe una nueva prioridad de primer nivel para la seguridad nacional, debido a los nuevos actores regionales.

Asimismo, el fenómeno del terrorismo es como mencionabamos, un asunto actual. Los especialistas en la materia califican como actos terroristas hechos de la historia que van desde la rebelión de Espartaco (año 75 D.C.) hasta algunas prácticas realizadas en las Cruzadas (1095 - 1291), pasando por manifestaciones durante la llamada revolución industrial. Y es que parece ser que la dominación ejerciendo el miedo ha sido y siempre será una tentación ejercida frente al poder o desde el poder mismo. Es por ello que el Departamento de Estado de los EEUU

definió al terrorismo como ¨el uso calculado de violencia ilícita para inculcar miedo con la intención de coercionar o intimidar gobiernos y sociedades en la búsqueda de objetivos que por lo general son políticos, religiosos o económicos¨.

Lo que podemos afirmar es que el terrorismo ha acompañando al hombre prácticamente desde la formación de las naciones y no puede negarse que su afianzamiento evidenció un notable impulso a partir del siglo XX. Así, los llamados ¨movimientos de liberación nacional¨ organizados fudamentalmente en África, fueron caldo de cultivo de actividades terroristas ejm: Argelia, Angola, Mozambique y el Congo estuvieron plagadas de terrorismo de todo nivel. En el Perú del siglo pasado, existen antecedentes de violencia política y de enfrentamiento al poder del Estado con las guerrillas de inspiración cubana de los años sesenta.

El surgimiento de Sendero Luminoso iría incubándose fundamentalmente desde el seno de la Universidad de Huamanga hasta lograr las dimensiones apocalípticas al que pudo llegar. Hoy en día, si bien Sendero Luminoso ha dejado de ser una amenaza para la gobernabilidad del país y ya es en la práctica imposible que obtenga la captura del poder como estuvo muy cerca de hacerlo, es necesario tener en cuenta que su desafío a la democracia se mantiene vigente y, lamentablemente con posibilidades de expresión a partir de su ya mencionada innegable alianza con el narcotráfico y la minería ilegal. El movimiento terrorista más letal del mundo es, sin duda el ISIS[3]. Y tal dimensionamiento es debido a su gran capacidad de emplear métodos heterodoxos–pragmáticos para desarrollarse mediante acuerdos estratégicos con el narcotráfico, bandas de falsificadores, lavadores de dinero e incluso con el fenómeno de las pandillas como la llamada ¨maras salvatruchas¨.

Esto nos lanza una voz de alerta que no debe desconocerse para no repetir el pasado. Sendero Luminoso está cambiando de piel y si no se le hace frente en forma decidida mediante el uso de las modernas técnicas de inteligencia y la tecnología necesaria, mas temprano que tarde estaremos volviendo a lamentar una nueva negación de la realidad que, como antaño, en que se llamó ¨abigeos¨ a los terroristas, tiñó de sangre al país y carcomió la esperanza de millones de peruanos. Hay autores que encuentran diferencias entre insurgencia, subversión y terrorismo. La insurgencia es un levantamiento popular . La subversión hace alusión a un movimiento que hace uso de la fuerza para cambiar el régimen, las reglas de juego. Sin embargo, hasta ese punto, aún no se puede hablar de terrorismo, ya que el calificativo de terrorista se aplica a las acciones, a los métodos criminales y sanguinarios, a las matanzas de inocentes para alcanzar un fin político.

En este sentido, una organización terrorista es aquella que utiliza estrategias que implican la matanza de inocentes. Ese fue el caso de Sendero Luminoso que asesinaba a todo aquel que considere como opositor, a todos aquellos que no pensarán como ellos. Sendero Luminoso fue una organización fundamentalista, terrorista, sanguinaria e irracional. La mejor forma de hacer una reconciliación nacional es acercando al Estado a la Sociedad, que la presencia estatal se haga sentir en los pueblos antes olvidados, que los excluidos sean tomados en cuenta, que se tenga como prioridad al campesinado y las poblaciones selváticas.

Existen otros autores que definen hacen una diferencia analítica entre terrorista y guerrilla por la formas de empleo de violencia organizada contra el Estado por ejemplo:

Terrorismo(Función de violencia) :	Principalmente simbólico-comunicativa
Terrorismo (apoyo social):	Limitado a pequeños grupos de intelectuales pertenecientes a la clase media
Terrorismo (Factor territorial):	Sin base territorial
Terrorismo (Dinámica):	Sin posibilidades de asumir el poder político-militar, más bien contraproducente

---

Guerrilla (Función de violencia):	La aplicación de la violencia sirve a fines instrumentales
Guerrilla (apoyo social):	Incluye capas sociales más amplias, en particular la de la población rural
Guerrilla (Factor territorial):	Con base territorial
Guerrilla (Dinámica):	Con posibilidad eventual de asumir el poder político-militar

Ambas formas de comportamiento insurgente se aplican preferentemente cuando un grupo más débil se levanta contra un adversario militar mente superior. La guerrilla se basa en la idea de compensar la inferioridad militar mediante una manera irregular de luchar, ganando así tiempo para poder movilizar las fuerzas propias hasta igualar las del enemigo o superarlas. En cambio, el terrorista renuncia de antemano a poder competir con el Estado a nivel

[3] El **Estado Islámico** (**EI**; en árabe: الدولة الإسلامية, *al-Dawla al-Islāmīya*) o **Dáesh** es un grupo terrorista insurgente de naturaleza yihadista suní, autoproclamado califato, asentado en un amplio territorio de Irak y Siria.El grupo es controlado por radicales fieles a Abu Bakr al-Baghdadi, autoproclamado «califa de todos los musulmanes».Técnicamente el grupo se organiza como un Estado no reconocido, ya que controla de facto varias ciudades como Mosul, Faluya o Al Raqa, siendo esta última considerada su capital

militar, en lugar de ello confía en el efecto psíquico de sus acciones violentas. Citando a Wordemann, "la guerrilla procura ocupar él espacio, mientras que el terrorismo se esfuerza por ocupar el pensamiento"[4].

Cibercrimen, ciberespionaje y ciberguerra como nuevas amenazas en la seguridad:

El cibercrimen usa el ciberespacio para realizar sus delitos a fin de obtener beneficios económicos, apoyándose para ello en las redes de comunicaciones y sistemas de información electrónicos.

¿Qué tienen en común el cibercrimen, ciberespionaje y ciberguerra? ¿Qué acciones se han tomado a nivel internacional para responder a estos retos? El fenómeno de Internet ha conllevado también a la aparición de nuevos problemas: el cibercrimen y el ciberterrorismo. El cibercrimen usa el ciberespacio para realizar sus delitos a fin de obtener beneficios económicos, apoyándose para ello en las redes de comunicaciones y sistemas de información electrónicos. Éste abarca desde el delito económico, como el fraude informático, la falsificación, espionaje informático, computer hacking, la piratería comercial y otros crímenes contra la propiedad industrial y el crimen organizado.

Los ciberdelincuentes y cibercriminales usan la red para:

(i) Obtener dinero de forma fraudulenta.
(ii) Bloquear páginas web de instituciones, organizaciones, empresas o gobiernos
(iii) Propagar malware, tal como un virus, una backdoor, un spyware o un gusano, y
(iv) Blanquear dinero a fin de recibir el dinero procedente del fraude en su cuenta corriente y remitirlo a un tercer destinatario.

El ciberterrorismo excede al cibercrimen. Se define como la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos y religiosos. Se considera que el ciberterrorismo ha realizado un uso pasivo de Internet, puesto que los ataques informáticos se han limitado a colapsar servicios de sitio web de instituciones o empresas, robar información, inutilizar sistemas de comunicación o contrainformar, por lo que se puede decir que no se ha producido un ataque cibernético que cause grandes pérdidas y conlleve a hablar de ataques ciberterroristas.

El uso de Internet por parte de los grupos terroristas se centra, principalmente, en:

(i) Obtener financiamiento para sus causas.
(ii) Llevar a cabo una guerra psicológica, mediante la propagación de información equívoca, amenazas, divulgación de imágenes de sus atentados y videos de torturas.
(iii) Efectuar reclutamiento de miembros.
(iv) Mantener comunicación con sus organizaciones.
(v) Coordinar y ejecutar acciones.
(vi) Encontrar información para sus posibles objetivos, y adoctrinar ideológicamente y promocionar sus organizaciones.

La ciberguerra es en todo similar a los paradigmas de la guerra asimétrica y de la guerra total, el fundamento es el siguiente:

(i) Los efectos pueden alcanzar a todos los ciudadanos, administraciones, instituciones y empresas del Estado aunque no estén conectados al ciberespacio.
(ii) Involucra, voluntaria o involuntariamente, a todos los ciudadanos, administraciones, instituciones y empresas del Estado.
(iii) La relación entre eficacia y coste es muy alta, posiblemente la más alta, ya que puede inutilizar sistemas básicos y críticos de un país con un coste para el atacante extraordinariamente bajo.
(iv) No necesita de una infraestructura grande y costosa como la industria de armamento clásico – terrestre, naval, aéreo. Solo necesitan personas con muy buena formación en ingeniería informática y en psicología.
(v) En la ciberdefensa pasiva, deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su nivel y con sus medios.
(vi) Es muy difícil probar fehacientemente la autoría de un ataque, lo que proporciona un anonimato muy grande y convierte a la ciberguerra en una guerra pérfida.

---

4 Terrorismo y Guerrilla. La violencia organizadacontra el Estado en Europa y América Latina. Un análisis comparativo. *Peter Waldmann*

Como se ha visto, el paradigma de la ciberguerra es una mezcla de los paradigmas de la guerra total y de la guerra asimétrica que convierten a la ciberguerra en muy peligrosa por sus posibles efectos y por su perfidia. Además, crea un marco conceptual nuevo, la ciberseguridad, para el cual es necesario crear conciencia en todos los ciudadanos como individuos y como Estado.

Los efectos de la cibernética pueden ser empleados como el arma pérfida del siglo XXI ya que las amenazas son reales pero se perciben por el común de los mortales de manera difusa, por lo que no hay un conocimiento adecuado de los daños que puede producir un ataque informático. Los usuarios de sistemas informáticos tienen grandes dificultades para percibir claramente la amenaza cibernética, lo que dificulta mucho la concienciación.

El Ciberespionaje: Según el director de Inteligencia Nacional de los EE. UU.. James R. Clapper se define las ciberamenazas en términos de «ciberataques» y «ciberespionaje»: un «ciberataque» es una operación ofensiva no cinética con la intención de crear efectos físicos o manipular, alterar o suprimir datos. Puede ir desde una operación de denegación de servicio que impide temporalmente el acceso a un sitio «web» a un ataque contra una turbina de generación de energía que causó un daño físico y un apagón que duró varios días.

El «ciberespionaje» se refiere a intrusiones en las redes de acceso a información sensible diplomática, militar o económica. Una solución es la ciberinteligencia, identificar las vulnerabilidades e individualizar los peligros existentes y potenciales, ello resulta muy difícil de realizar, debido a la carencia de fronteras del ciberespacio, el acceso a redes bajo anonimato, por ello, el uso de medios de seguridad resulta más factible, aunque existe también la posibilidad de que sean vulnerados. Otra solución posible es el establecimiento de organismos gubernamentales destinados exclusivamente a la lucha contra los ataques cibernéticos. Existen maneras que podrían emplearse como líneas de acción estratégicas a la seguridad cibernética: el incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas, con apoyo de un marco jurídico operativo y eficaz. Otra manera sería la garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Asimismo, la mejora de la seguridad de las tecnologías de la información y la comunicación (TIC).

Por otro lado, la capacitación de profesionales en ciberseguridad. Asimismo, la implantación de una cultura de ciberseguridad sólida por lo que se deberá concientizar a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento y por último se deberán intensificar la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional que persigan un entorno seguro.

El Convenio de Budapest sobre el Cibercrimen es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Su principal objetivo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

A pesar de un marco jurídico común, la eliminación de obstáculos jurisdiccionales para facilitar la aplicación de la ley de delitos informáticos sin fronteras, no puede ser posible dentro de este marco. La transposición de las disposiciones del Convenio en la legislación nacional es difícil, especialmente si se requiere la incorporación de las expansiones sustanciales que van en contra de los principios constitucionales. Se está trabajando con otros países para combatir la delincuencia transnacional, incluido el de ayudar a otras naciones a construir sus capacidades de aplicación de la ley. Se sigue con la lucha contra el terrorismo internacional y en frustrar los ataques terroristas que se han planeado y puesto en marcha en Internet. No hay duda de que cada nación debe proteger a sus ciudadanos contra la delincuencia y los ataques en línea, y fuera de línea.

Conclusiones:

El Hemisferio enfrenta hoy amenazas tradicionales y nuevas que demandan innovar un enfoque multidimensional de la seguridad hemisférica que, en mi opinión, debería tener como base jurídica la Carta de las Naciones Unidas y la Carta de la OEA. El desafío prioritario es consolidar la paz, que es el valor fundamental que sustenta la democracia, la justicia, y el respeto a los derechos humanos y al derecho internacional. Para ello existen mecanismos de cooperación entre estados contra las amenazas. Cada Estado determina sus prioridades nacionales en seguridad y según eso define sus estrategias, planes y acciones a nivel hemisférico.

Entre los nuevos desafíos tenemos: el terrorismo, la delincuencia organizada transnacional, la corrupción, narcotráfico, lavado de activos, tráfico de armas, pobreza extrema, desastres naturales, pandemias, trata de personas, riesgos del transporte marítimo de materiales, posesión y uso de armas de destrucción masiva, migraciones no controladas, delincuencia cibernética, amenazas a la infraestructura crítica, seguridad para el transporte y seguridad portuaria, etc.

Es necesario que la comunidad de inteligencia, las fuerzas armadas, y las agencias de orden público desarrollen un entendimiento mucho más profundo de la manera cómo los estados criminalizados/grupos del COT/terroristas y los estados hostiles y los actores extranjeros no-estatales explotan los espacios no gobernados. Asi, una estrategia eficaz para combatir el COT debe basarse en una fundación sólida de inteligencia regional.

El Perú enfrenta diferentes amenazas, la primera es la delincuencia organizada –principalmente el narcotráfico- que atenta contra la seguridad de las instituciones y de los ciudadanos. De hecho la inseguridad ciudadana, el problema que más afecta hoy a los peruanos, es producto en buena medida del accionar del narcotráfico nacional e internacional, además de la pobreza, la falta de educación y las deficiencias estructurales del estado. También arrastramos problemas de años anteriores como el terrorismo.

El cibercrimen usa el ciberespacio para realizar sus delitos. El ciberterrorismo excede al cibercrimen. Asimismo, el Ciberterrorismo solo ha hecho un uso pasivo del internet a la actualidad. La ciberguerra es en todo similar a los paradigmas de la guerra asimétrica y de la guerra total por lo que se puede considerar una mezcla de los dos, lo que la convierten a la ciberguerra en muy peligrosa por sus posibles efectos. Asi nace la ciberseguridad como instrumento de concientización de los individuos. Ante el ciberespionaje, nace la ciberinteligencia y la implantación de una cultura de ciberseguridad sólida así como la intensificación de la colaboración internacional.

Qué tienen en común el cibercrimen, ciberespionaje y ciberguerra y en qué son diferentes?

El cibercrimen usa el ciberespacio para realizar sus delitos a fin de obtener beneficios económicos, apoyándose para ello en las redes de comunicaciones y sistemas de información electrónicos.

¿Qué tienen en común el cibercrimen, ciberespionaje y ciberguerra y en qué son diferentes. ¿Qué acciones se han tomado a nivel internacional para responder a estos retos? El fenómeno de Internet ha conllevado también a la aparición de nuevos problemas: el cibercrimen y el ciberterrorismo. El cibercrimen usa el ciberespacio para realizar sus delitos a fin de obtener beneficios económicos, apoyándose para ello en las redes de comunicaciones y sistemas de información electrónicos. Éste abarca desde el delito económico, como el fraude informático, la falsificación, espionaje informático, computer hacking, la piratería comercial y otros crímenes contra la propiedad industrial y el crimen organizado. Los ciberdelincuentes y cibercriminales usan la red para: (i) obtener dinero de forma fraudulenta, (ii) bloquear páginas web de instituciones, organizaciones, empresas o gobiernos (iii) propagar malware, tal como un virus, una backdoor, un spyware o un gusano, y (iv) blanquear dinero a fin de recibir el dinero procedente del fraude en su cuenta corriente y remitirlo a un tercer destinatario. El ciberterrorismo excede al cibercrimen. Se define como la forma en la que el terrorismo utiliza las tecnologías de la información para intimidar, coaccionar o causar daños a grupos sociales con fines políticos y religiosos. Se considera que el ciberterrorismo ha realizado un uso pasivo de Internet, puesto que los ataques informáticos se han limitado a colapsar servicios de sitio web de instituciones o empresas, robar información, inutilizar sistemas de comunicación o contrainformar, por lo que se puede decir que no se ha producido un ataque cibernético que cause grandes pérdidas y conlleve a hablar de ataques ciberterroristas. El uso de Internet por parte de los grupos terroristas se centra, principalmente, en: (i) obtener financiamiento para sus causas (ii) llevar a cabo una guerra psicológica, mediante la propagación de información equívoca, amenazas, divulgación de imágenes de sus atentados y videos de torturas, (iii) efectuar reclutamiento de miembros, (iv) mantener comunicación con sus organizaciones (v) coordinar y ejecutar acciones (vi) encontrar información para sus posibles objetivos, y adoctrinar ideológicamente y promocionar sus organizaciones. La ciberguerra es en todo similar a los paradigmas de la guerra asimétrica y de la guerra total, el fundamento es el siguiente: (i)Los efectos pueden alcanzar a todos los ciudadanos, administraciones, instituciones y empresas del Estado aunque no estén conectados al ciberespacio. (ii) Involucra, voluntaria o involuntariamente, a todos los ciudadanos, administraciones, instituciones y empresas del Estado. (iii) La relación entre eficacia y coste es muy alta, posiblemente la más alta, ya que puede inutilizar sistemas básicos y críticos de un país con un coste para el atacante extraordinariamente bajo (iv) No necesita de una infraestructura grande y costosa como la industria de armamento clásico – terrestre, naval, aéreo. Solo necesita personas con muy buena formación en ingeniería informática y en psicología. (v) En la ciberdefensa pasiva deben participar todos los ciudadanos, administraciones, instituciones y empresas del Estado, cada uno a su nivel y con sus medios. (vi) Es muy difícil probar fehacientemente la autoría de un ataque, lo que proporciona un anonimato muy grande y convierte a la

ciberguerra en una guerra pérfida. Como se ha visto, el paradigma de la ciberguerra es una mezcla de los paradigmas de la guerra total y de la guerra asimétrica que convierten a la ciberguerra en muy peligrosa por sus posibles efectos y por su perfidia. Además, crea un marco conceptual nuevo, la ciberseguridad, para el cual es necesario crear conciencia en todos los ciudadanos como individuos y como Estado. Los efectos de que la cibernética pueda ser empleada como el arma pérfida del siglo XXI son que las amenazas son reales pero se perciben por el común de los mortales de manera difusa, como no hay un conocimiento adecuado de los daños que puede producir un ataque informático, los usuarios de sistemas informáticos tienen grandes dificultades para percibir claramente la amenaza cibernética, lo que dificulta mucho la concienciación. El Ciberespionaje: Según el director de Inteligencia Nacional de los EE. UU., James R. Clapper se define las ciberamenazas en términos de «ciberataques» y «ciberespionaje»: un «ciberataque» es una operación ofensiva no cinética con la intención de crear efectos físicos o manipular, alterar o suprimir datos. Puede ir desde una operación de denegación de servicio que impide temporalmente el acceso a un sitio «web» a un ataque contra una turbina de generación de energía que causó un daño físico y un apagón que duró varios días. El «ciberespionaje» se refiere a intrusiones en las redes de acceso a información sensible diplomática, militar o económica. Una solución es la ciberinteligencia, identificar las vulnerabilidades e individualizar los peligros existentes y potenciales, ello resulta muy difícil de realizar, debido a la carencia de fronteras del ciberespacio, el acceso a redes bajo anonimato, por ello, el uso de medios de seguridad resulta más factible, aunque existe también la posibilidad de que sean vulnerados. Otra solución posible es el establecimiento de organismos gubernamentales destinados exclusivamente a la lucha contra los ataques cibernéticos. Existen maneras que podrían emplearse como líneas de acción estratégicas a la seguridad cibernética: el incremento de la capacidad de prevención, detección, investigación y respuesta ante las ciberamenazas, con apoyo de un marco jurídico operativo y eficaz. Otra manera sería la garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas. Asimismo, la mejora de la seguridad de las tecnologías de la información y la comunicación (TIC). Por otro lado, la capacitación de profesionales en ciberseguridad. Asimismo, la implantación de una cultura de ciberseguridad sólida por lo que se deberá concientizar a los ciudadanos, profesionales y empresas de la importancia de la seguridad de la información y del uso responsable de las nuevas tecnologías y de los servicios de la sociedad del conocimiento y por último se deberán Intensificar la colaboración internacional. Se promoverán los esfuerzos tendentes a conseguir un ciberespacio internacional que persigan un entorno seguro. El Convenio de Budapest sobre el Cibercrimen es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Su principal objetivo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. Conclusión: A pesar de un marco jurídico común, la eliminación de obstáculos jurisdiccionales para facilitar la aplicación de la ley de delitos informáticos sin fronteras, no puede ser posible dentro de este marco. La transposición de las disposiciones del Convenio en la legislación nacional es difícil, especialmente si se requiere la incorporación de las expansiones sustanciales que van en contra de los principios constitucionales. Se está trabajando con otros países para combatir la delincuencia transnacional, incluido el de ayudar a otras naciones a construir sus capacidades de aplicación de la ley. Se sigue con la lucha contra el terrorismo internacional y en frustrar los ataques terroristas que se han planeado y puesto en marcha en Internet. No hay duda de que cada nación debe proteger a sus ciudadanos contra la delincuencia y los ataques en línea, y fuera de línea.

(*)Abogada en derecho internacional y catedrática de Política Internacional