CAPÍTULO II

LA SEGURIDAD DIGITAL EN EL ENTORNO DE LA FUERZA PÚBLICA DIAGNÓSTICOS Y AMENAZAS DESDE LA GESTIÓN DEL RIESGO*

Jairo Becerra
Ivonne Patricia León

Capítulo de libro resultado del proyecto de investigación titulado "Gestión de Riesgos en seguridad Digital" de la Maestría en Ciberseguridad y Ciberdefensa de la Escuela Superior de Guerra, que a su vez hace parte de la línea de investigación "Seguridad Digital" del grupo de investigación "Masa Crítica", reconocido y categorizado en (B) por Colciencias. Registrado con el código COL0123247, está adscrito a la Escuela Superior de Guerra "General Rafael Reyes Prieto"de la República de Colombia.

Introducción

La aparición de nuevas tecnologías de la información y la comunicación introdujo en el escenario internacional la posibilidad de *virtualizar* la guerra y con ella, una serie de transformaciones en la estructura del Estado cuyo propósito fundamental es reaccionar ante nuevas amenazas. La revolución tecnológica ha enfrentado al planeta entero con la posibilidad de un ciberataque en diversos niveles que podrían comprometer lo militar, político, económico y social.

La cuarta revolución tecnológica amplió el espectro de amenazas a las cuales deben responder los Estados. Un ejemplo de ello lo representan los ataques terroristas cuya intensidad se magnifica por la percepción de inseguridad que se genera en la opinión pública. De esta manera, el ciberterrorismo se ha convertido en un arma de alcance mundial que amenaza al Estado, emporios empresariales e individuos indiscriminadamente.

Este fenómeno, ha planteado la necesidad de contar con medios seguros para la transmisión de datos (redes seguras). No obstante, la posibilidad de responder efectivamente ante las amenazas que vienen dadas por la guerra virtual se encuentra con la imposibilidad de delimitar fronteras claras para combatirlas, y con ello, la conciencia de que se trata de una problemática de carácter global ante la cual no es posible la cobertura total de los riesgos.

Estas preocupaciones son recogidas por la Asamblea General de la Organización de las Naciones Unidas en 1999, cuando plantea la posibilidad de que las nuevas tecnologías de información y comunicación se

utilicen con fines en contra de la estabilidad y la seguridad internacionales. Para el año 2004, la Comunidad Andina plantea entre sus objetivos, prevenir, combatir y erradicar las nuevas amenazas a la seguridad. Mientras la Organización de Estados Americanos crea una red hemisférica para la respuesta a incidentes de seguridad de computadores.

A dos años de que se cumpla la segunda década del siglo XXI las hipótesis sobre la batalla por la primacía digital se extienden rápidamente. En el escenario internacional Estados Unidos y China ocupan las principales noticias en revistas como *The Economist* en su carrera por la fabricación de tecnologías de información y comunicación que podrían impactar de manera decisiva en redes y sistemas armamentísticos de avanzada.

En Colombia, la cuarta revolución industrial y la aparición de nuevas tecnologías comporta un nuevo espectro de retos de cara a la modernización del país. Los procesos de producción industrial cada vez más automatizados y los sistemas de inteligencia artificial, conllevan un alto grado de independencia en la toma de decisiones que termina por afectar ejes tan importantes para el Estado, como son la seguridad y la defensa de una parte, así como nuevas demandas sociales derivadas de presiones laborales.

Para avanzar de cara a la revolución tecnológica, Colombia tendrá que enfrentar los aspectos relacionados con la política y la administración del Estado, el ambiente y la conectividad misma que implican las nuevas tecnologías. De esta forma, será necesario trabajar en torno a la gobernanza digital que implica aspectos como el gobierno electrónico, la participación a través de nuevas redes de información y la transparencia política. Asimismo, es necesario considerar la infraestructura inteligente relacionada con las redes de interconexión y posibilidades para generar una ciudad inteligente y la transversalidad en las TIC (Portafolio, 2017).

En este orden de ideas, este documento presentará una conceptualización general a partir de la cual se pretenden evidenciar las problemáticas, amenazas y riesgos que enfrenta la sociedad contemporánea en el marco de la cuarta revolución tecnológica. En el segundo apartado, se

profundizará en los riesgos tecnológicos y los avances logrados en este campo. Finalmente, en el tercer acápite se presentan las estrategias en perspectiva de futuro frente a la gestión del riesgo y la seguridad Digital.

1. Nuevas tecnologías, un nuevo mundo

Las tecnologías de información y comunicación han representado una nueva dimensión de posibilidades y amenazas en el mundo contemporáneo. Los sectores público y privado han incorporado dentro de sus procesos el uso de herramientas tecnológicas que disminuyen costos y hacen posible ofrecer respuestas ágiles frente a problemas cotidianos. La cuarta revolución industrial ha significado de esta forma, una trasformación profunda en las actividades cotidianas y una disminución significativa en el tiempo requerido para actuar, generando también un marco para la transparencia y el acceso oportuno a la información.

En este apartado se presentan las características de la revolución de la información y la comunicación, evidenciando sus alcances y las principales transformaciones que esta produjo en el marco de la globalización. En el segundo apartado se presentan las nuevas tecnologías haciendo énfasis en la aparición de los sistemas ciberfísicos y el Internet de las cosas. Finalmente, el tercer punto volverá sobre los actores en el contexto de la cuarta revolución tecnológica y la globalización que comparten el nuevo escenario internacional con el Estado.

1.1. La revolución de la información

Las últimas décadas del siglo XX y las primeras del siglo XXI estuvieron marcadas por la globalización y la intensificación de la interconexión de redes económicas, políticas, culturales y militares. La cuarta revolución tecnológica profundizó las consecuencias de la globalización a partir de los avances en computación, tecnología digital, robótica, inteligencia artificial, impresión 3D, nanotecnología y computación cuántica, entre otras.

El concepto de Revolución 4.0 fue presentado por primera vez como una directriz del gobierno alemán en la Feria de Hannover realizada en 2011. Allí se planteó la necesidad de una Estrategia de Alta Tecnología como parte del programa marco *Horizonte 2020*. Las características de la propuesta recogían la estandarización, la posibilidad de que los dispositivos se configuren automáticamente (*plug and play*) y una producción interconectada digitalmente.

El eje principal de la Tecnología 4.0 es la información y su integración en procesos en los que no es posible distinguir entre elementos, ámbitos y niveles de producción. Estas nuevas tecnologías actúan como una extensa Red Neuronal de procesadores sociales de información y de conocimiento cuya lógica de interconexión es altamente compleja. La industria que surge a partir de estas nuevas tecnologías requiere para su funcionamiento de estructuras altamente flexibles que pueden ser rápidamente modificadas o reordenadas (Minsky, 1988, pp. 17-19; Castells, 2006, pp. 87-90).

Los cuatro rasgos predominantes de estas redes son instantaneidad o comunicación en tiempo real, interactividad o comunicación bidireccional, virtualidad o amplitud comunicacional, y unicidad o integración comunicacional. Todo esto se encuentra asociado a la posibilidad de generar nuevos mecanismos de organización tanto en el ámbito político como en el económico y nuevas formas de relacionamiento que no dependen de una infraestructura física ni de una territorialidad determinada.

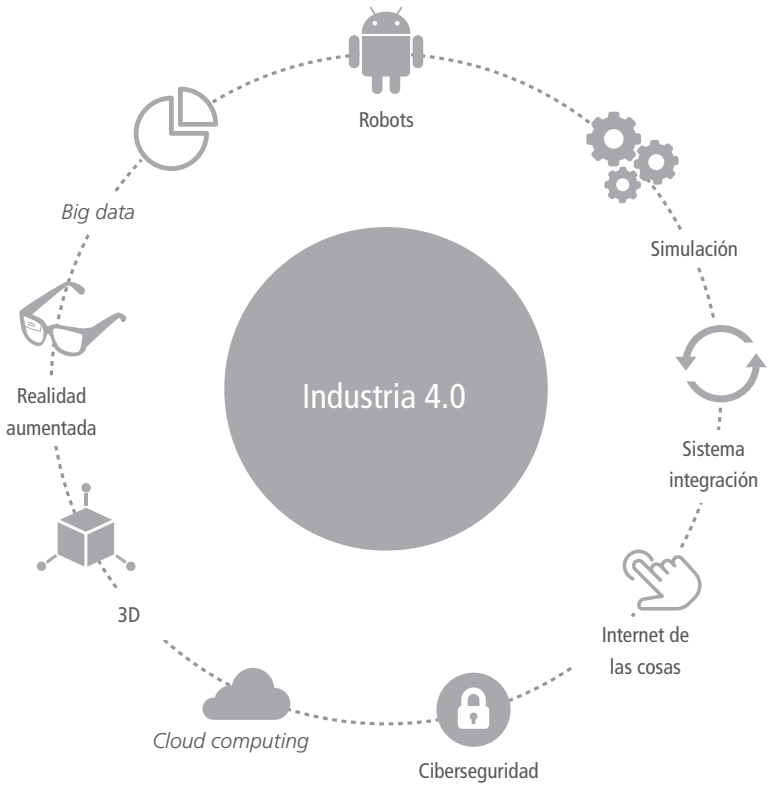
> Así, la instantaneidad soporta la globalidad, en el sentido de que, en ausencia de distancia física y técnica, la comunicación se puede establecer, indiferentemente, con cualquier punto de la aldea global. Nuevas organizaciones de escala planetaria. Nuevas formas y fórmulas organizativas en el ámbito local y en el global. Por su parte, la interactividad contribuirá a la desmasificación de los medios. Frente a la unidireccionalidad de los medios de comunicación de masas, la bidireccionalidad de la red telefónica y telemática configura a todo elemento de la red como emisor/receptor de señales, no sólo receptor pasivo. La comunicación punto a punto fragmenta las audiencias masivas. (Bericat Alastuey, 1996, p. 104)

La globalización y la aparición de nuevas tecnologías de información y comunicación generaron nuevas formas políticas cristalizadas en nuevas herramientas de gestión, la recomposición de la administración pública hacia modelos de gobernanza horizontal y cooperativa, y una ciudadanía orientada por la inclusión, la equidad y la participación eficaz. Todo esto lleva a la necesidad de plantear un Estado con las capacidades necesarias para concertar, coordinar y dirigir a la sociedad hacia sus metas de desarrollo (Rivera Méndez, 2010, p. 3).

La gobernanza transforma no solo las estructuras organizacionales e institucionales, sino que afecta las prácticas sociales y los métodos de creación, acceso y divulgación del conocimiento. De esta manera, se puede definir la gobernanza como la organización de la acción o toma de decisiones colectivas, que incluye mecanismos formales e informales para el uso de las reglas, todo ello coordinado por actores estatales y no estatales (Neiva Santos, pp. 49-53, citado por Reyes Beltrán, 2017, p. 59).

De esta manera, la cuarta revolución industrial comporta la aparición de nueve tecnologías cuyas transformaciones han tenido impacto en los sistemas de producción e información a escala global. Estas tecnologías son Internet de las cosas, sistemas ciberfísicos, realidad aumentada, simulación, robótica colaborativa, fabricación aditiva, *big data*, *cloud computing* y ciberseguridad.

Figura 1. Industria 4.0



Fuente: Paredes (2017) a partir de AMETIC

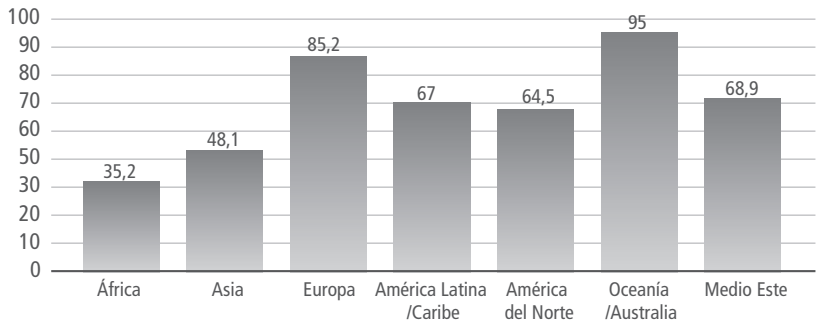
La integración horizontal y vertical de los sistemas permite la automatización de los procesos a través de la articulación de la información y comunicación entre diversas unidades y funciones. El Internet de las cosas hace posible la innovación de materiales y herramientas que coadyuvan en la elaboración de análisis descentralizados, mientras la nube facilita el almacenamiento y la disposición de información más allá de límites espaciales o territoriales con el propósito de disminuir el tiempo de reacción, consiguiendo la toma de decisiones con mayor agilidad. De otra parte, la simulación, los robots autónomos, la realidad virtual y la fabricación adaptativa permiten generar innovaciones en menos tiempo y con mayor calidad, transitando hacia dispositivos

que emplean información orientada hacia sistemas de preferencias y automatización.

1.2. Nuevas tecnologías

Internet es un sistema mundial de información que funciona de manera descentralizada. Esta red se ha convertido en la autopista de información pública y de interconexión de ordenadores más extendida del planeta. De acuerdo con las cifras presentadas por la agencia de *marketing* y comunicación *We are Social*, la Web internacional *Internet World Stats* y *World Telecommunication Indicators Database* de la Agencia Especializada sobre Tecnologías de Información y Comunicación de las Naciones Unidas (ITU), a diciembre de 2017 aproximadamente el 50 % de la población mundial cuenta con acceso a Internet con un total aproximado de 4160 millones de habitantes.

Figura 2. Tasa de Penetración de Internet (% Población)

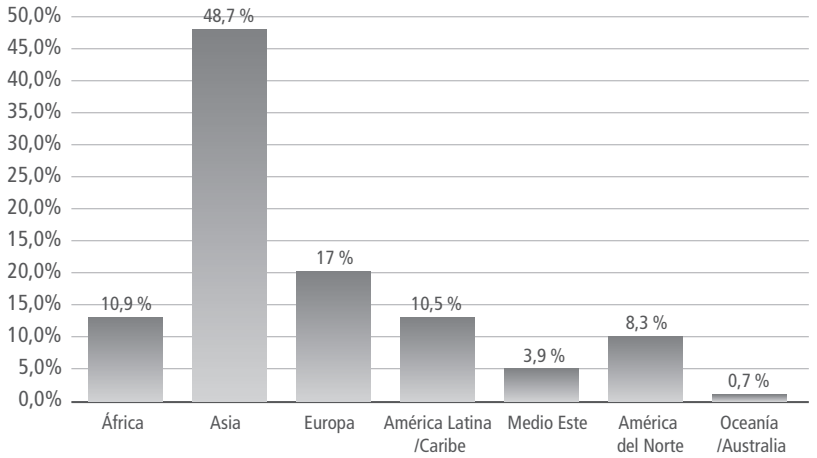


Fuente: Internet World Stats, 31 de diciembre de 2017

El mayor grado de penetración de Internet se encuentra en Norteamérica con 90 % aproximadamente, seguido por Europa con un 85 %, América Latina y el Caribe por su parte, cuentan con una penetración del 67 % seguido de cerca por Oriente Medio con un porcentaje de penetración del 64 % aproximadamente. Estos datos contrastan con el nivel de usuarios que se ubican en mayor proporción en Asia con un 48 %. No obstante, vale la pena señalar que las estadísticas acerca del

acceso a Internet, su porcentaje de penetración y el número de usuarios por región, varían rápidamente y parecen mantener una tendencia de aumento sostenido entre 2000 y 2018.

Figura 3. Usuarios de Internet



Fuente: Internet World Stats, 31 de diciembre de 2017

El Internet ha llevado a la comunicación e interacción digital en tiempo real entre diferentes objetos mediante Internet a través de redes fijas e inalámbricas, en lo que se conoce como el Internet de las Cosas o en inglés Internet of Things, IoT. Esta tecnología ha sido empleada en objetivos diversos como relojes, alarmas, sensores de velocidad, entre otros y ha implicado considerar que cualquier objeto puede ser un potencial generador de datos o de información.

Para que esta tecnología llegara a ser de uso cotidiano fue necesario la miniaturización de componentes, llevando a la generación de elementos cada vez más pequeños (*chips* y circuitos), lo que hace que se pueda conectar prácticamente a cualquier cosa, desde cualquier sitio, en cualquier momento. Así mismo, se requirió la superación de la limitación de la infraestructura de telefonía móvil, y la proliferación de las aplicaciones y los servicios que ponen en uso la gran cantidad de información creada a partir del IoT (Fundación Bankinter, 2011, p. 6).

Los objetos interconectados a través Internet posibilitan la generación de entornos inteligentes capaces de analizar, diagnosticar y ejecutar funciones, disminuyendo la ocurrencia de errores humanos. La interconexión entre los objetos se produce a partir de operaciones remotas, usando una dirección IP (Internet Protocol) para contactar con un servidor externo y enviar los datos recogidos, y de la misma forma, ser accedido para recibir instrucciones. Así, entre los objetos que hacen parte del IoT se puede distinguir entre aquellos que funcionan como sensores, los que realizan acciones y aquellos que combinan ambas funciones (Torres, 2014).

Tabla 1. Clasificación de Dispositivos IoT

Ámbito	Dispositivos
Vestibles	Relojes, lentes, anillos, ropa, cinturones, etc.
Doméstica	Alarmas, cerraduras, cámaras, refrigeradores, televisores, control de temperatura, riego de jardines, etc.
Industriales	Variedad de sensores para monitorear y controlar producción, monitorear estado físico y ubicación de los empleados, etc.
Ciudades inteligentes	Detectores de velocidad, sensores para monitorear el tráfico, sensores en las estructuras de los edificios para monitorear su estado, cámaras de vigilancia, estacionamientos inteligentes, vigilancia mediante drones, etc.

Fuente: Martínez, Mejía, Muñoz y García (2017, p. 81)

El Internet de las Cosas tiene como principio funcional las tecnologías máquina a máquina (M2M), que permiten la comunicación entre aparatos, captando información y convirtiéndola en acciones puntuales. En este esquema, M2M utiliza un dispositivo (como un sensor o medidor) para capturar un evento (como la temperatura, nivel de inventario, etc.), que se retransmite a través de una red hacia una aplicación (*software*), que traduce a su vez el evento capturado en información significativa (Molano, 2014).

Internet de las Cosas, agrega una nueva dimensión a la comunicación al permitir la comunicación en cualquier momento y lugar dando lugar a la posibilidad de generar respuestas autónomas, para lo cual es fundamental el involucramiento de la inteligencia artificial (García, 2015, p. 17). Es así como este sistema crea una extensa red que se asimila a una compleja red neuronal, con capacidad de proveer datos y analizarlos en tiempos récord y eficientemente, para lo cual se apoya a su vez, en tecnologías como el *Big Data* y la inteligencia artificial.

La integración en la comunicación posibilitada por el IoT llevo a la generación de Sistemas Ciberfísicos o Cyber Physical Systems (CPS), que consiste en dotar a los objetos de capacidades computacionales y de comunicación con el propósito de convertirlos en objetos inteligentes que pueden cooperar entre ellos, formando ecosistemas distribuidos y autónomos (Fernández y Sáez Domingo, 2015, p. 5). Estos sistemas comportan un alto grado de adaptación y autonomía, y su aplicación se extiende a múltiples posibilidades que abarcan desde la movilidad y la salud, hasta extensos complejos sociales como la interconexión en ciudades inteligentes.

La cibernética y la inteligencia artificial aportan elementos para generar el acople entre diversos niveles tanto de orden horizontal como vertical con el propósito de consolidar sistemas flexibles con una capacidad de respuesta eficiente y ágil frente a problemas complejos. La cibernética mantiene el sistema en funcionamiento, permitiendo reajustes a los caminos iniciales o a nuevos caminos donde ha habido desvíos u obstáculos, para adaptar el mecanismo a los objetivos establecidos (Bericat Alastuey, 1996, p. 107; Bell, 1984, pp. 47-48).

De esta forma y teniendo en cuenta los conceptos desarrollados a partir de la cuarta revolución tecnológica, se puede entender que el Estado reoriente su estructura hacia instituciones flexibles que buscan la resolución eficiente de conflictos y problemáticas sociales, políticas y económicas, con el propósito de avanzar en torno a objetivos concretos. En este esquema de funcionamiento, la retroalimentación es fundamental toda vez que permite generar los mecanismos de reajuste del sistema. El Estado como la sociedad es policéntrico, mientras la información se presenta en mecanismos descentralizados.

1.3. Nuevos actores

Con las nuevas Tecnologías de la Información y la Comunicación -TIC, emergieron nuevos actores políticos en los ámbitos locales e internacionales. Las redes de información favorecen las transacciones económicas, las trasferencias electrónicas de servicios especializados y la comunicación de grupos en diferentes lugares del planeta. Como anota Saskia Sassen:

> Las nuevas TIC, en especial la Internet de acceso público, han reforzado esta política de lugares y han expandido el espacio de los actores de la sociedad civil más allá de la red de ciudades globales, para abarcar también en algunos casos las localidades periféricas. (Sassen, 2015, p. 236)

En este contexto, el Estado desaparece o tiende a la fragmentación en un proceso que presiona su reconfiguración y su adaptación a una nueva realidad. Se produce una reformulación de las escalas en términos de los lugares estratégicos que articulan el nuevo sistema, generando a su vez, las condiciones necesarias para que asciendan las ciudades, regiones y zonas transfronterizas (escala subnacional), así como mercados electrónicos globales y otras entidades supranacionales (Reyes Beltrán, 2017, p. 62; Sassen, 2015, p. 43).

En este contexto, el Estado se ve limitado por nuevas instituciones y entidades cuyo carácter dinámico no logra ser regulado por marcos jurídicos nacionales. Esta situación requiere un abordaje sistémico en el que diferentes actores asuman la responsabilidad frente a los riesgos que representa un contexto cada vez más interconectado. Así mismo, los marcos jurídicos se transforman rápidamente conforme a las reglas del Derecho Internacional, con decisiones que pueden influir en el sistema financiero global.

Todo esto, hace necesario construir y consolidar nuevos conjuntos de datos para rastrear los movimientos de información, capital y personas (Sassen, 2015, pp. 44-45). La desterritorialización del riesgo ha supuesto la necesidad de avanzar en los estudios y análisis de las interacciones entre naturaleza, tecnología y sociedad en contextos geográficos

y espaciales a distintas escalas y niveles. El acople de las instituciones como un sistema global se presenta desde esta perspectiva como una respuesta al contexto de las sociedades complejas y globalizadas para dar cuenta de la diferenciación funcional (Reyes Beltrán, 2017, p. 153; Luhmann, 2007, pp. 3-10).

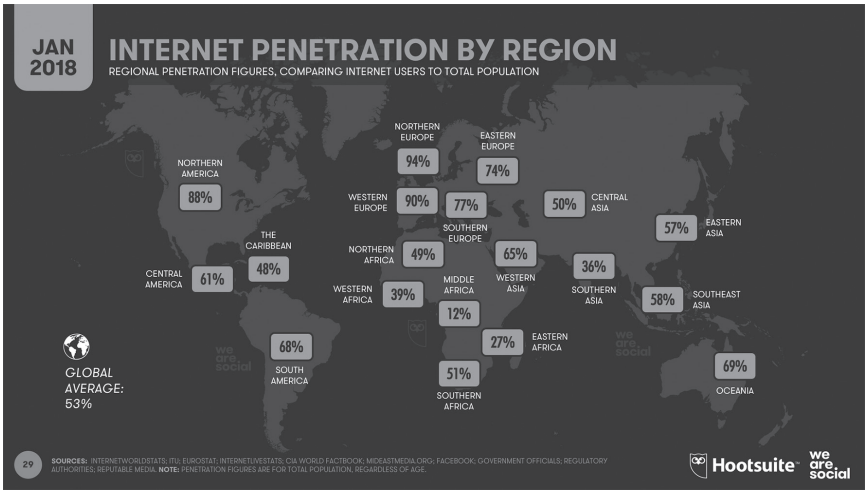
El nuevo contexto refuerza la actividad de organizaciones multilaterales de alcance regional y de naturaleza global. En la misma medida se ha reforzado el papel de actores no estatales como las Empresas y Organizaciones No Gubernamentales. Esta descentralización de las relaciones internacionales se da en el marco de las interacciones globales como en el ámbito del diseño de políticas nacionales de los Estados.

En este marco, es indispensable el establecimiento de una agenda internacional los Estados y los actores subnacionales para posibilitar una acción externa coordinada que refleje los diversos intereses de las naciones. La diplomacia adquiere un carácter descentralizado y supranacional, en el que se tienen en cuenta la multiplicidad de actores que interactúan en la compleja red de vínculos internacionales (Orozco, 2016, pp. 193-196).

Un reflejo de este escenario internacional tuvo lugar en 2011 con la celebración del primer foro denominado *e-G8* en el que participaron los presidentes y primeros ministros de Estados Unidos, Alemania, Francia, Gran Bretaña, Canadá, Japón, Italia y Rusia, junto a 22 directivos y personalidades del sector de Internet. En este foro se discutió la visión común sobre Internet y el modelo económico a aplicar para garantizar su desarrollo.

> Internet supone el 3.4 % del Producto Interno Bruto (PIB) en 13 países, entre los cuales figuran los del G8 y tres las principales economías emergentes, China, Brasil e India. Además, en los últimos cinco años Internet contribuyó en 10 % de su crecimiento, según un estudio dado a conocer en el e-G8 de París donde los fundadores de las principales redes sociales y del mayor buscador de Internet, abogaron "por un acceso libre y abierto" a Internet de todos los habitantes del planeta (Portafolio, 2011).

Figura 4. Usuarios de Internet y Redes Sociales en el Mundo, 2018



Fuente: González (2018)

En una escala diferente, la interconexión entre los individuos de forma continua y permanente ha permitido que los movimientos sociales adquieran un nuevo sentido y orientación. Lo anterior, es potenciado gracias a la facilidad de convocatoria, el anonimato y el alcance de la difusión (Mariscal, 2016, p. 27). Las nuevas tecnologías, particularmente las redes sociales, han traído consigo el desacoplamiento gradual de la continuidad y la simultaneidad, haciendo posible una organización sin contigüidad.

> Algunas de las características más importantes de estos medios sociales son la interacción continua entre los miembros, la existencia de convenciones formales e informales, la voluntad de las personas para interactuar, la dimensión global y la velocidad con la que las relaciones se desarrollan (Uribe Saavedra, Rialp Criado y Llonch Andreu, 2013, p. 207).

La nueva sociabilidad creada por Internet se configura a partir de la creación de un espacio público de interacción en el que se facilita la creación de nuevas identidades colectivas y las interacciones entre los miembros de los movimientos sociales y de ellos con los medios de

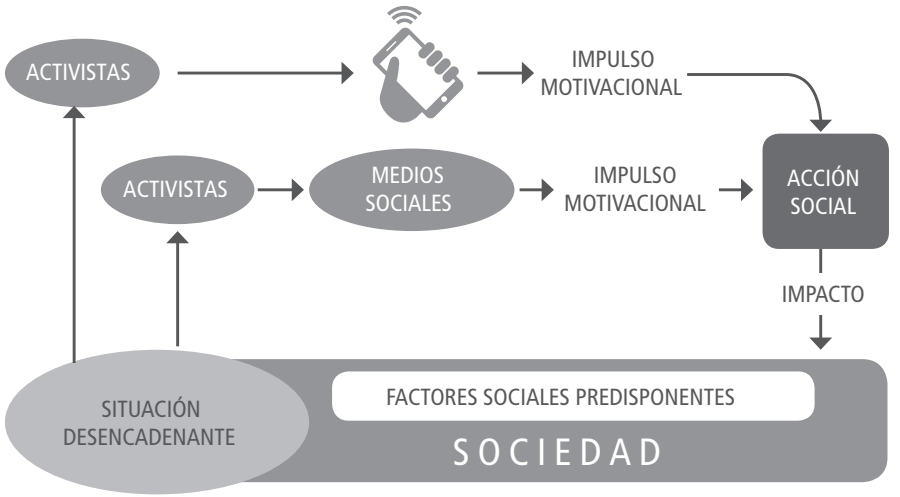
comunicación masiva y la prensa, multiplicando las posibilidades y frecuencias de comunicación entre individuos dispersos territorialmente (Mosca y Porta, 2009, pp. 194-202).

Las nuevas tecnologías de información pueden activar y revitalizar los movimientos sociales ya que permiten la planificación y ejecución de acciones y protestas, incluso antes de que se puedan producir reacciones o medidas para pararlas o contrarrestarlas. *Twitter* es un ejemplo del impacto que se genera a partir de líderes de opinión y que tienen la capacidad de situar temáticas coyunturales en la agenda mediática. El ciberespacio ofreció a los movimientos sociales la posibilidad de acceder a recursos de información a bajo costo en un proceso de difusión de doble vía en el que es posible comunicarse y recibir retroalimentación con otros usuarios (De La Rosa, 2014, pp. 35-48; De La Rosa, 2016, pp. 48-49).

Al respecto es necesario analizar el considerable aumento en el uso de *smartphones* y *tablets*, así como la información relacionada con el acceso a redes sociales. En este sentido se debe anotar que cerca de un millón de personas empezaron a utilizar las redes sociales por primera vez de forma diaria en el último año, lo que significa que hay cerca de 11 usuarios de redes sociales nuevos cada segundo (González, 2018). Es así como las medidas restrictivas o preventivas frente a las acciones de movimientos sociales o de ciberactivistas se produce tarde, cuando miles de personas los han leído en las pantallas de sus computadoras, teléfonos móviles o *tablets.*

Los ciberactivistas son compuestos en gran proporción por jóvenes interesados en participar en el cambio social y que hacen parte activa de procesos de empoderamiento digital. Esta participación se explica, adicionalmente, por su dominio de recursos y aplicaciones tecnológicas, la independencia de los medios de comunicación a través de Internet que hacen posible poner en circulación mensajes con estructuras novedosas y el acceso a dispositivos móviles con acceso a Internet que posibilitan la creación y envió de información actualizada mediante plataformas dinámicas (De La Rosa, 2014b, p. 122).

Figura 5. Los movimientos sociales en la Era Digital



Fuente: La Rosa (2014b, p. 121)

Los *hacktivistas* representan un movimiento orientado por un tipo de acción política de resistencia y lucha por una sociedad alternativa, relacionada con la libertad de información, con las luchas por la democracia y por una sociedad abierta (Vicente, 2004, p. 3). Los *hacktivistas*, como los *hackers* y *crackers*, emplean conocimientos y técnicas en sistemas informáticos para adelantar movimientos de respuesta a políticas, normas o situaciones sociales que consideran regresivas o contrarias a sus motivaciones intelectuales o políticas.

Al respecto es importante contemplar las diferencias entre los diferentes actores que se involucran en el ciberespacio:

Hacker. Personaje apolítico, que solo lucha por sus compañeros, por la libertad de la información o por sí mismo.

Cracker. Su objetivo es crear virus e introducirse en otros sistemas para robar información y luego venderla al mejor postor.

Hacktivistas. Emplean sus habilidades en los sistemas informáticos con fines políticos y sociales. Es decir, juegan al ataque y realizan lo que ellos llaman la Desobediencia Civil Electrónica (DCE) (Álvarez, 2013).

De otra parte, la aparición de poderes no institucionales favorecidos por las redes sociales y medios de comunicación de alcance masivo gracias a Internet, han representado un reto para las políticas públicas y la normatividad. La emergencia de nuevos actores en la escena internacional ha generado la emergencia de problemáticas asociadas a la corrupción y las economías ilegales, representando problemas de seguridad pública que se suman a la sensación de inseguridad de la ciudadanía debido al aumento de los delitos y la actividad criminal (Maira, 2005, pp. 233-235; Reyes Beltrán, 2017, p. 144).

2. La gestión del riesgo y las nuevas amenazas globales

La aparición de las nuevas tecnologías de información y comunicación ha transformado las sociedades contemporáneas. Internet posibilita el acceso a la información de manera asincrónica y sin límites en el tiempo y el espacio, conectando a las personas más allá de las barreras geográficas. El ciberespacio se ha convertido en el lugar de convergencia y negociación entre diversos actores que han replanteado los esquemas básicos de comunicación, situación que ha conllevado nuevos retos y amenazas en materia de regulación y políticas públicas.

En el nuevo escenario internacional las trasformaciones en la comunicación han conllevado igualmente, nuevos desafíos para la seguridad y la forma de enfrentar las amenazas. En este apartado se explorará el estado actual de la cuestión, atendiendo a los riesgos del mundo contemporáneo. En el primer momento se hará reconstrucción de la gestión del riesgo desde sus abordajes teóricos y prácticos como respuesta a los nuevos desafíos de seguridad. En la segunda parte se presentarán las principales amenazas del ciberespacio a los Estados y los individuos. En el último apartado se establecerán los principales elementos que componen la visión de la ciberdefensa desde las teorías de la gestión del riesgo.

2.1. La gestión del riesgo y los desafíos de la seguridad

El atentado al World Trade Center en New York, el 11 de septiembre de 2011, significó un cambio profundo en los marcos de sentido y de interpretación de asuntos como la seguridad y la protección. Tal acontecimiento y sus consecuencias, situó a las sociedades globales frente a la posibilidad de que cada elección pueda tener consecuencias indeseadas o no calculadas con precisión. Como señala Josetxo Berian (2005), hoy la contingencia se presenta como un atributo moderno, que paradójicamente enfrenta el mayor conocimiento a través de la ciencia a un umbral de seguridades menor al de las sociedades tradicionales (p. 12).

La latencia de las amenazas y la necesidad de anticipar la catástrofe ha llevado a la posibilidad de restringir algunas libertades en favor de la consolidación de un marco de seguridad que se configura en torno a la sospecha más que de la realidad. Como lo explica Ulrich Beck (2008)

> El riesgo es el patrón perceptivo e intelectual que moviliza a una sociedad enfrentada a la construcción de un futuro abierto, lleno de inseguridades y obstáculos, una sociedad que ya no está determinada por la religión la tradición o la sumisión a la naturaleza y que tampoco cree en los efectos redentores de las utopías (p. 20).

La globalización y la revolución de la información ha generado que el riesgo adquiera características espaciales, temporales y sociales deslocalizadas, toda vez que un incidente puede generar efectos más allá de las fronteras del Estado como es el caso del cambio climático, perdurar en el tiempo como en el caso de un ataque nuclear, o comportar un alto grado de complejidad social como en las crisis financieras (Casas Mínguez, 2016, p. 5).

La magnitud del riesgo está estrechamente ligada con la posición geoestratégica y el acceso a recursos como la información, lo que involucra, además, una competencia permanente por determinar las amenazas mundiales. Esta situación conlleva decisiones que en sí mismas comportan riesgos, toda vez que no existen opciones seguras o arriesgadas sino

alternativas que dependen de su conmensurabilidad y que afectan ámbitos cualitativamente diferentes (Beck, 2008, p. 18).

Las amenazas se presentan en un espectro amplio y muchas veces indeterminable, que pasan por el terrorismo, el riesgo nuclear, la intervención genética y el calentamiento global, siendo estos fenómenos en los que se conjugan el saber y el no-saber en un espectro amplio de probabilidades. En este mismo marco, los Estados mismos se convierten en un riesgo inminente frente a otros Estados por efectos de problemáticas como la contaminación, la migración y la posibilidad de la guerra nuclear, entre otros.

Adicionalmente, los riesgos tienen un alto componente democratizador en virtud de un doble proceso de deslocalización. Por un lado, la amenaza puede comportar un alto grado de incertidumbre con respecto a su origen, por lo que es necesario avanzar con una concepción que vaya más allá del estatismo metodológico. De otra parte, en virtud de este mismo cosmopolitismo, las consecuencias del riesgo conllevan alcances inimaginados que se extienden rápidamente más allá de las fronteras nacionales.

El riesgo puede comprenderse en términos generales como la causa o probabilidad de un suceso no deseado que puede o no ocurrir. Desde el valor de expectativa, es posible comparar un factor de riesgo frente a otros en términos de un dato relevante, por ejemplo, el número de víctimas que puede causar. Y desde la teoría de la decisión se pueden tomar en consideración el conocimiento de las probabilidades o la incertidumbre para diseñar cursos de acción (Hansson, 2000, citado por Lapuente Sastre, 2006 p. 5).

La percepción sobre el riesgo depende de complejos e imbricados sistemas culturales de creencias, valores e ideales que pueden ser modulados a través de las redes de información y comunicación (Tabernero, Moyano y Trujillo, 2014, p. 2). Así también, los criterios de evaluación del riesgo dependen en un alto grado de las diferentes clases de amenazas identificadas en contextos particulares de acuerdo con los intereses estratégicos de quien o quienes lo evalúan.

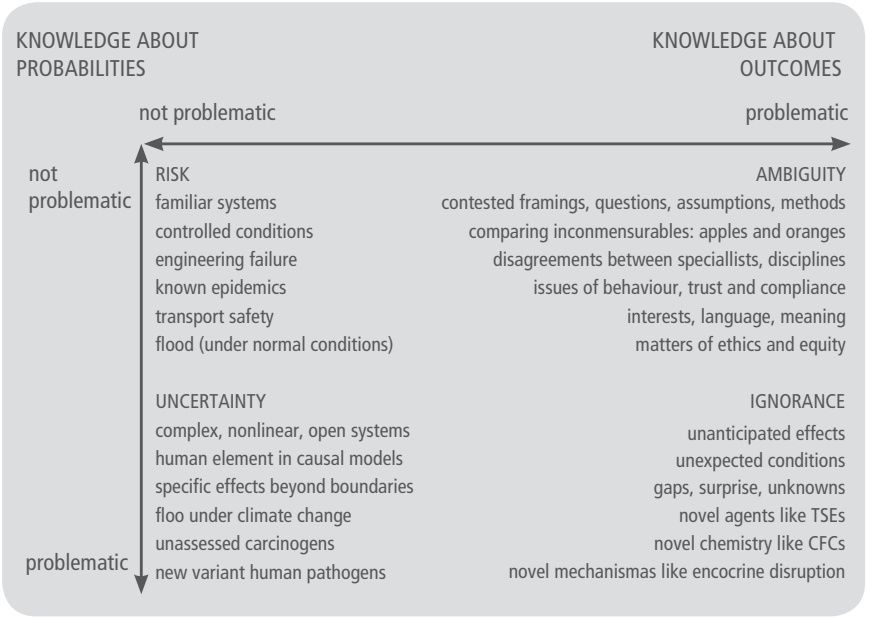
Las estrategias de gestión inteligente para el manejo de los riesgos dependen igualmente de estos intereses y de la posición respecto al espectro global del Estado que las pone en marcha. En este sentido es importante distinguir entre riesgo como amenaza potencial y riesgo como probabilidad de ocurrencia de un fenómeno no deseado. La claridad sobre los indicadores que permiten develar la probabilidad de que un fenómeno determinado ocurra, permite tomar decisiones graduales e inteligentes respecto al futuro (Tabernero, Moyano y Trujillo, 2014, p. 2).

Hay, en principio, cuatro estados de conocimiento lógicamente posibles pueden presentarse en la toma de decisiones, incertidumbre, riesgo, ambigüedad y desconocimiento (Stirling, 2009, pp. 330-331). La fiabilidad y calidad del conocimiento permite anticipar y responder al riesgo o a las amenazas de acuerdo con experiencias pasadas o efectos predecibles. De aquí se desprende el hecho de que hay riesgos que comportan un mayor grado de complejidad para su tratamiento. En un estadio de incertidumbre, por ejemplo, la probabilidad no existe por lo que los juicios adoptados comportarán a su vez, un alto grado de desconocimiento en cuanto a los alcances y resultados.

Cada uno de los estadios (riesgo, incertidumbre, desconocimiento, ambigüedad) son resultado de diferentes grados de conocimiento sobre las probabilidades de ocurrencia de un fenómeno y sus resultados. En el plano real, los diferentes planos no son excluyentes entre sí, por lo que se pueden presentar en diferente intensidad. En un estadio de incertidumbre se pueden caracterizar los resultados posibles, aunque no se cuente con información sobre las probabilidades de ocurrencia, por lo que la forma de proceder es reconocer el carácter abierto de una variedad de posibles interpretaciones para dar respuesta a ellas.

En el ámbito de la ambigüedad se conocen las probabilidades, pero no es posible calcular o puede no haber acuerdo sobre los resultados. Este escenario refiere a acontecimientos que no pueden ser evitados o sobre los cuales se pueden encontrar referencias en el pasado. En el ámbito de ignorancia, no se pueden caracterizar ni las probabilidades ni los resultados, prima el desconocimiento sobre los acontecimientos y sus consecuencias (Stirling, 2009, pp. 327-333).

Figura 6. Estados posibles del conocimiento incompleto



Fuente: Stirling (2009, p. 329)

Así, teniendo en cuenta estas condiciones, Andreas Klinke y Ortwin Renn, "formularon su aproximación al análisis del riesgo basándose en nueve criterios de evaluación, seis clases de riesgos, un árbol de toma de decisiones y tres categorías genéricas para su gestión" (Tabernero, Moyano y Trujillo, 2014, 3). El nivel de incertidumbre frente a las probabilidades y el impacto de las consecuencias o de los resultados se traduce en este modelo en una escala de nivel de tolerancia del riesgo, que recoge el área normal, intermedia e intolerable.

Los nueve criterios de evaluación del riesgo (Klinke & Renn, 2001; Klinke & Renn, 2002) comprenden:

1. Daño potencial
2. Probabilidad de ocurrencia
3. Incertidumbre
4. Ubicuidad (dispersión y propagación geográfica de los daños potenciales)

5. Persistencia (extensión temporal)
6. Irreversibilidad
7. Efectos de latencia (tiempo de retardo entre el evento y las repercusiones)
8. Violación de la equidad
9. Potencial de movilización

El objetivo de la gestión del riesgo es planear y disponer de estrategias viables y apropiadas para tomar decisiones. "Las estrategias de gestión del riesgo persiguen el objetivo de garantizar la seguridad e integridad, transformando riesgos inaceptables en riesgos aceptables" (Tabernero, Moyano y Trujillo, 2014, p. 6). Las nuevas tecnologías de información y comunicación obligan a estar preparados y ofrecer respuestas frente a riesgos de carácter global desde contextos complejos.

Con este propósito se proponen la Gestión de Riesgo basada en una perspectiva técnica, en el principio de precaución y en la deliberación. Desde el enfoque técnico, el riesgo se conceptualiza como una propiedad objetiva de los sucesos y actividades que involucran la tecnología. Esta perspectiva requiere un abordaje multidisciplinar que favorezca la convergencia conceptual para definir de forma apropiada los fenómenos y avanza en torno a herramientas de la estadística de variables en la búsqueda de una universalmente válida con ayuda de la cual puedan establecerse comparaciones entre distintas clases de riesgo (Rivera Berrío, 2009, p. 4; Tabernero, Moyano y Trujillo, 2014, p. 7).

La gestión del riesgo basada en el principio de precaución se asocia a un alto grado de incertidumbre, por lo que se requiere un método de evaluación de mayor complejidad. En este tipo de gestión del riesgo se involucran la mayor variedad de incertidumbres posible, posibles escenarios, indicadores de posible daño, tendencias, partes interesadas y grupos sociales afectados para determinar la resistencia que se puede producir (Stirling, 2009, pp. 341-343). La precaución contempla la posibilidad de prohibir con fines preventivos y puede referir a fenómenos como los ataques cibernéticos o la biotecnología (Tabernero, Moyano y Trujillo, 2014, p. 7).

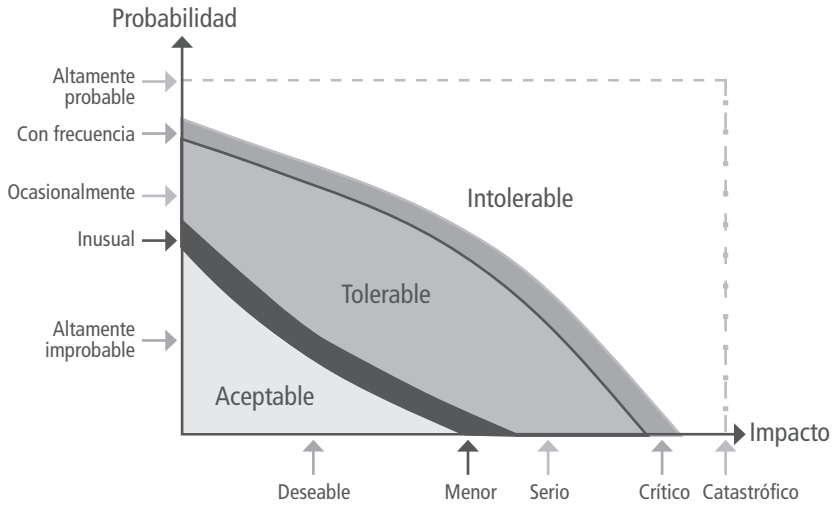
> Actuar con precaución es actuar con cautela para evitar posibles inconvenientes, dificultades o daños; es decir, cuando no hay suficientes razones para creer que un curso de acción está libre de riesgos. […] Un modelo racional es el denominado principio de precaución al que se acude cuando no se conocen los posibles impactos que genera la toma de decisiones de carácter técnico o científico; es decir, cuando los datos científicos o tecnológicos no permiten una evaluación del riesgo. (Rivera Méndez, 2010, p. 5)

La gestión basada en la deliberación, por su parte, tiene en cuenta la discusión participativa acerca de las justificaciones, posibles beneficios, costes y riesgos de los factores involucrados con el propósito de resolver ambigüedades y diferencias. Este esquema de deliberación señala la necesidad de la participación democrática y la posibilidad de llegar a consensos en la búsqueda de soluciones compatibles con los intereses y necesidades de los afectados. Este esquema permitiría resolver o evitar los posibles conflictos derivados del riesgo.

Es así como a cada modelo de gestión del riesgo, le sigue un esquema de acción determinado (Tabernero, Moyano y Trujillo, 2014, pp. 7-8). Con un esquema técnico, un alto nivel de daños y baja probabilidad de ocurrencia, las acciones estarán encaminadas a determinar la probabilidad, reducir el desastre potencial, incrementar la resistencia, prevenir y gestionar la emergencia. Una gestión del riesgo basada en el principio de precaución se puede poner en marcha en condiciones de incertidumbre frente a los daños y la probabilidad de ocurrencia, y las acciones estarán dirigidas a mejorar el conocimiento, reducir y contener la emergencia y evaluar la necesidad de aplicar prohibiciones.

Finalmente, la gestión basada en la deliberación puede incluir un rango de conocimiento sobre la probabilidad de ocurrencia y los posibles daños que abarcan tanto un alto como un bajo grado de incertidumbre. La participación puede ser empleada en este esquema con el propósito de concienciar, transmitir confianza, comunicar el riesgo y gestionar las contingencias.

Figura 7. Estrategias de la gestión del riesgo



Fuente: Renn y Klinke (2012) y Moncada (2015).

En este contexto, las amenazas que enfrenta la Fuerza Pública deben tener un enfoque de gestión del riesgo que maximice la efectividad de las acciones emprendidas por esta, haciendo hincapié en que la magnitud del problema y sobre todo sus implicaciones, hacen necesario la prevención de actos que alteren el normal funcionamiento del entorno, cuyo incremento en diversidad y cobertura se enfoca de manera principal en la ciudadanía (CONPES 3854, 2016) y dificultan el accionar de las autoridades.

Es así como la Política Nacional de seguridad Digital, establecida en el CONPES 3854, está enfocada en la gestión del riesgo y se basa en la atención de cinco problemas centrales:

Falta de visión estratégica en seguridad Digital basada en la gestión de riesgos:

1. Las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital.

2. El refuerzo de las capacidades de ciberseguridad con un enfoque de gestión de riesgos de seguridad digital.
3. El refuerzo de las capacidades de ciberdefensa con un enfoque de gestión de riesgos de seguridad digital.
4. La necesidad de aumentar los esfuerzos y la articulación de cooperación, colaboración y asistencia, nacional e internacional, relacionados con la seguridad Digital.

2.2. Ciberdefensa. Enfoques desde la gestión del riesgo

El orden inaugurado después de la crisis energética de 1970 involucró nuevos actores internacionales entre los cuales emergieron empresas de orden trasnacional y multinacional que transformaron el entorno geopolítico, económico y sociopolítico a nivel global. El modelo económico que supuso este nuevo orden conllevó un espacio altamente organizado y la aparición de relaciones que requieren un alto nivel de concertación en las escalas nacional, transnacional y supranacional.

Intervenciones sobre territorios geoestratégicos como Irak, Afganistán y Libia, reflejan la necesidad de consolidar y controlar espacios de acuerdo con un entorno global en constante trasformación. La complejidad del mundo contemporáneo debe apelar a una versatilidad de iniciativas y respuestas capaces de asegurar el acceso a fuentes de recursos estratégicos, la movilidad del capital y con ello, el establecimiento de una globalidad ordenada (Ceceña, 2008, p. 23).

> El impacto de la globalización en la regulación estatal es un fenómeno cualitativamente nuevo por dos razones: en primer lugar, reduce la intervención y regulación, ya que el movimiento actual produjo el debilitamiento de los poderes estatales, además de ejercer una presión sobre los Estados de forma monolítica bajo sus condiciones el modelo de desarrollo orientado hacia el mercado es el único compatible con el nuevo régimen global de acumulación. En segundo lugar, esta presión se refuerza con hechos tan dispares como el fin de Guerra Fría, las innovaciones tecnológicas de comunicación e información, los sistemas de producción flexible, la aparición de bloques regionales, la democracia liberal como régimen político universal y la imposición de la ley para proteger la propiedad intelectual (Santos, 2005, pp. 246-247).

En este contexto, los atentados del 11 de septiembre de 2001 al World Trade Center en Nueva York, marcó un punto de inflexión en los marcos interpretativos sobre la seguridad y la protección, desplazándolos de referentes nacionales hacia un orden global cuya gestión se lleva a cabo bajo la óptica del riesgo (Beck, 2008, pp. 15-46). La posibilidad permanente de que eventos catastróficos tengan lugar, potencializada con el auge de las tecnologías de información y comunicación, ha generado retos sociales, políticos, económicos y jurídicos cuya probabilidad de ocurrencia y consecuencias son difíciles de determinar.

Un primer problema de las nuevas Tecnologías de Información y Comunicación –TIC, está dado por la posibilidad de la comunicación de masas en una escala sin precedentes. Las nuevas formas de comunicación, cristalizadas en las redes sociales, se desarrollan a través de nuevas formas de interacción en las que la distinción entre lo público y lo privado se ve disminuida y eliminada; se relativizan el tiempo y el espacio favoreciendo interacciones de carácter predominantemente dialógicas cuya ubicación no se encuentra anclada a un espacio físico tangible; y es posible generar mensajes dirigidos a una masa de receptores sin que exista una orientación especifica de la acción (Muñoz, 2005, p. 560).

Las repercusiones políticas de este nuevo tipo de comunicación se han materializado en la posibilidad de convocar, gestionar y ejecutar manifestaciones globales que adquieren móviles diversos que abarcan la demanda de derechos, el rechazo frente a fenómenos o decisiones que trascienden el ámbito nacional o la visibilización de intereses de sectores sociales diversos. Tal es el caso de las movilizaciones de rechazo a la intervención de Irak en 2003, el movimiento 15-M también conocido como movimiento de los indignados en 2011 y las manifestaciones del mundo árabe entre 2010 y 2013 conocidas como la primavera árabe.

Los riesgos tecnológicos se han clasificado según su voluntariedad (Starr, 1969), de acuerdo con su probabilidad de ocurrencia y el alcance o magnitud de sus consecuencias (Cohen & Lee, 1979); en función de la percepción que el público tiene de ellos (Fischhoff, Slovic, Lichtenstein, Read, & Combs, 1978; Slovic, 1990). Sin embargo, uno de los más importantes aportes en este campo fue el producido por Hohenemser,

Kates, & Slovic (1983), quienes clasificaron los riesgos tecnológicos de acuerdo con la extensión espacial de su impacto, el tiempo de duración entre exposición y consecuencias, la mortalidad humana anual, la mortalidad humana potencial, el impacto sobre generaciones futuras, entre otras categorías (Saurí, 1995, p. 151).

En coherencia con las teorías sobre la gestión del riesgo, los riesgos tecnológicos se pueden agrupar en tres grupos, a saber, riesgos extremos de carácter múltiple, riesgos extremos y riesgos ordinarios (Saurí, 1995, p. 151). La evaluación, por su parte, ha implicado nuevos restos para el ámbito jurídico-político, ya que aceptar un nuevo riesgo y determinar su carácter o alcance, implica generar nuevos desarrollos para hacerle frente y con ello, complejizar el sistema.

> Puesto que las decisiones tecnológicas, así como la identificación, estimación, valoración y gestión del riesgo no son asépticas ni están libres de intereses (económicos, políticos, ideológicos y religiosos), las conclusiones de una evaluación muy difícilmente serán unánimemente aceptadas (Rivera Méndez, 2010, p. 2; Olivé, 2004, p. 171).

La conceptualización y aceptación del riesgo se produce desde la construcción psicológica y tiene un carácter contingente. Esta creación del riesgo depende en buena medida de la creencia en que la acción humana puede prevenir el daño, por lo que es fundamental la posibilidad de construir escenarios futuros a partir de determinar los tipos de riesgos tecnológicos que se pueden producir y sus consecuencias determinadas.

Es así como, pese a que el Estado tiene la potestad de establecer y clasificar los riesgos a los cuales hacer frente, el sentido social del riesgo lleva a que cada individuo lo reconfigure de acuerdo con su propia experiencia. De esta forma, la conceptualización del riesgo tecnológico responde a un doble sentido, de abajo hacia arriba de acuerdo con la experiencia social y de arriba hacia debajo de acuerdo con las amenazas que el Estado considere prioritarias. Las percepciones y experiencia del individuo juegan, de esta forma, un papel importante en las creencias culturales, los principios y valores y los contextos económico, político y

social en el que se crea y se recrea el riesgo (Renn, 2005, p. 23; OCDE, 2003, p. 67; Rivera Berrío, 2009, p. 2).

El ataque a las infraestructuras críticas de los Estados se encuentra entre una de las amenazas más importantes a nivel mundial. Al afectar los sistemas de suministros de servicios básicos tales como agua, luz y gas, se puede interrumpir seriamente el normal desarrollo de una sociedad y mermar su capacidad de respuesta colectiva. Así, avanzando frente a esta problemática, la *directiva 1148 de la Unión Europea* expedida en el 2016 ordena a todos los Estados miembros que identifiquen los operadores de servicios esenciales establecidos en su territorio para cada sector, entendiendo que de dicha acción se puede desprender la base para combatir amenazas potenciales de desestabilización de un Estado, o en este caso de un conjunto de Estados.

La percepción de la sociedad frente al riesgo tecnológico puede estar determinada también, por el índice de penetración y la posibilidad de acceso a las TIC. De esta manera, los niveles de preparación de los Estados frente a las amenazas tecnológicas son muy distintos, lo que ha dado lugar a planteamientos fragmentados en temas como la evaluación y la percepción sobre sus consecuencias, lo cual influya a su vez, en niveles desiguales de protección de los consumidores y las empresas (Directiva UE 1148, 2016).

Los Estados comparten la responsabilidad frente a los riesgos tecnológicos con sectores públicos y privados, así como con individuos, en virtud de su rol diferenciado y su participación en las nuevas tecnologías de información.[4]

Un ejemplo de ello es la Active Cyber Defense Certainty Act (H.R. 4036, 2017) en los Estados Unidos. Consciente de los retos que conllevan las TIC, ha expresado que el ciberfraude y los crímenes relacionados con él, representan una amenaza grave para la seguridad nacional y para

4 Al respecto la OCDE ha señalado lo que aquí se refiere: "All stakeholders should understand digital security risk and how to manage it. They should be aware that digital security risk can affect the achievement of their economic and social objectives and that their management of digital security risk can affect others. They should be empowered with the education and skills necessary to understand this risk to help manage it, and to evaluate the potential impact of their digital security risk management decisions on their activities and the overall digital environment" (OCDE, 2015, p. 9).

la vitalidad económica de los Estados Unidos. Estos hechos presentan la necesidad imperiosa de la protección de la ciudadanía, en el ciberespacio, como un valor estratégico para el conjunto del Estado.

En este marco, la Defensa del territorio y la posibilidad de respuesta de los cuerpos de seguridad del Estado son de vital importancia. En el mundo globalizado contemporáneo, donde se requiere el acceso a grandes cantidades de información, las nuevas Tecnologías de Información y Comunicación son un elemento fundamental para el funcionamiento de la sociedad. "Esta necesidad de acceso e intercambio de información lleva inherentemente asociada la seguridad, ya que dicha información debe estar protegida frente a accesos o modificaciones no autorizadas" (Escuela de Altos Estudios de la Defensa, 2014, p. 15).

Esta situación ha implicado que la localización de los riesgos sea cada vez más complicada, dando lugar a escalas geográficas globales en las que se dificulta establecer la localización de las amenazas o prever las infiltraciones a sistemas operativos, logísticos y de comunicaciones, lo que frecuentemente se suma a la falta de interés de las poblaciones afectadas y la ausencia de marcos regulatorios se convierten en límites para la innovación y retos para la seguridad.

En las últimas décadas, los Estados han venido reorientando esfuerzos y recursos para resguardar no solo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también el ciberespacial (Cornaglia & Vercelli, 2017, pp. 46-62). La dimensión ciberespacial, sin locación física específica propia, genera replanteos sobre las tradicionales categorías con las que se aborda la guerra y exige, por la dinámica propia de la innovación tecnológica, una rápida adaptación para los Sistemas de Defensa respecto de sus componentes.

Una baja percepción del riesgo en materia tecnológica, de otra parte, podría asociarse a la idea de que el problema es difuso o está asociado a causas diversas difíciles de establecer, cuyas consecuencias solo se harán reales en el escenario de un futuro lejano. Esta falta de interés en los riesgos tecnológicos se explicaría, además, por la falta de familiarización de la sociedad con el uso de las nuevas Tecnologías de Información y Comunicación.

> De acuerdo con el paradigma psicométrico sobre la percepción del riesgo tecnológico, desarrollado por psicólogos y geógrafos a finales de los setenta, el público en general contrapone al criterio de mortalidad humana anual otros criterios para valorar el riesgo, como por ejemplo el grado de control individual sobre este, su impacto potencial sobre las generaciones actuales y futuras y la familiaridad con la tecnología en cuestión. (Saurí, 1999, p. 152)

Uno de los elementos más importante en el ámbito de la Ciberdefensa es, entonces, asegurar el normal funcionamiento de la sociedad en el ciberespacio y entregarle la seguridad necesaria en el desarrollo de sus actividades diarias. De esta forma, se intenta asegurar los niveles de confianza suficientes e indispensables para el desarrollo de actividades cotidianas asociadas en gran medida al empleo de tecnologías asociadas al Internet de las cosas, IoT, de forma tal que se genere el contexto necesario el desarrollo de todo el potencial de este espacio para la sociedad.

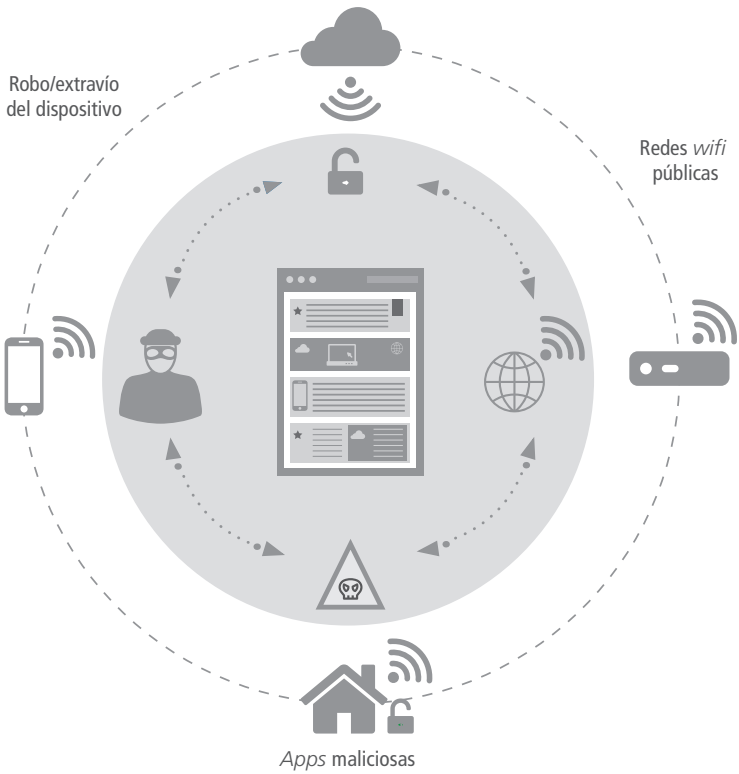
Son los particulares los que se enfrentan en su interacción diaria a la mayor cantidad de vulnerabilidades en el ciberespacio y así mismo, sus capacidades para actuar son limitadas. Por lo que se han hecho frecuentes las iniciativas que procuran informar e instruir a la ciudadanía frente a ataques de tipo *phishing* o ingeniería social; virus que acceden de forma no autorizada a los servidores de un servicio donde se almacenan las contraseñas de los usuarios o espías de las comunicaciones de red.

Frente a estas problemáticas, en Colombia la Policía Nacional ha puesto a disposición de la ciudadanía el Centro Cibernético Policial, con servicios como el análisis de *malware*, recomendaciones de ciberseguridad, un centro de atención a denuncias virtual que constituye la primera iniciativa en Iberoamérica en atención en línea policial y aplicaciones móviles para el fortalecimiento de la ciberseguridad, entre otros (Policía Nacional de Colombia; Ministerio de Defesa Nacional, 2018).

En este punto es relevante distinguir entre Ciberdefensa y ciberseguridad. La ciberseguridad o seguridad cibernética se refiere al combate y prevención de crímenes cibernéticos en la esfera de la seguridad pública o por parte de entidades del Estado. La Ciberdefensa o

Defensa cibernética, responde a un conjunto de acciones defensivas, exploratorias y ofensivas orientadas por Fuerzas Militares en un ejercicio de planeación estratégica para la salvaguarda de la seguridad nacional (López, 2013, p. 27).

Figura 8. Seguridad en Internet. Dispositivos Móviles

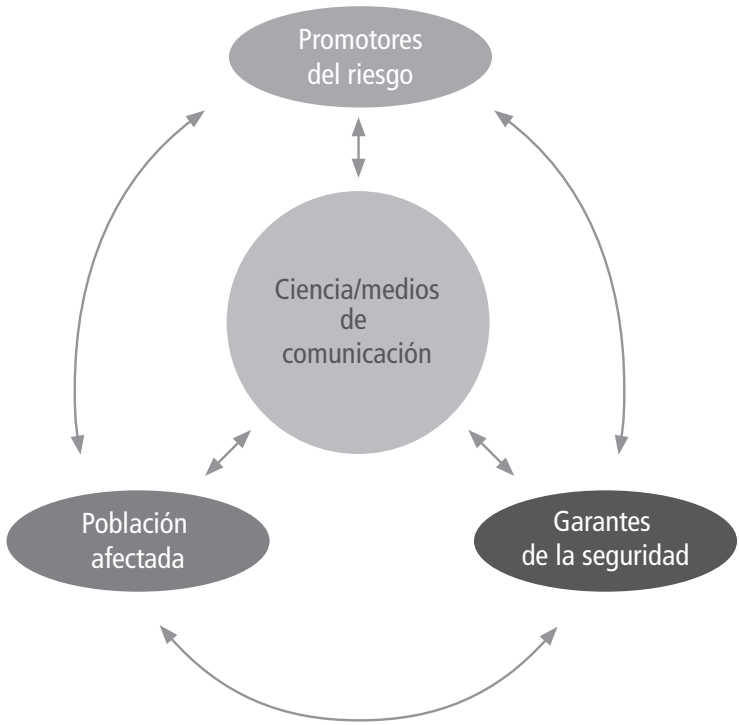


Fuente: AEPD; INCIBE, ficha 1, p. 4

En una perspectiva diferente, Wynne (1998) sugirió considerar las dimensiones institucionales del riesgo, es decir, los juicios sobre las instituciones involucradas en la gestión del riesgo, su independencia, su legitimidad, su competencia y la justicia percibida en sus acciones, entre otras (pp. 57-58; Espugla Trenc, 2006, p. 83) En este esquema la definición del riesgo tecnológico pasa por la interacción entre ciencia y medios de comunicación, toda vez que estos visibilizan las amenazas y juegan un

rol de impulsadores, amplificadores o mitigadores (Espugla Trenc, 2006, p. 84). Adicionalmente, en términos teóricos se podría considerar un esquema básico de interacción entre tres actores: los promotores generadores del riesgo, la población afectada y los encargados de garantizar la seguridad.

Figura 9. Sistema de interacción de conflictos sociales relacionados con riesgos tecnológicos



Fuente: Espugla Trenc, 2006, p. 83

No obstante, es importante tener en cuenta que la red es un nuevo espacio donde los roles de los diferentes agentes se construyen, evolucionan y cambian día a día (Alonso García, 2015, p. 18; Pons Gamón, 2017, p. 81). El ciberespacio se ha convertido en una de las fuentes de importancia para los Estados más dinámica y cambiante y en uno de los ejes de atención político-militar más relevante de las relaciones

interestatales. La popularización de Internet, no obstante, ha generado la eliminación de limitaciones en tiempo y espacio que dificultan las acciones encaminadas a determinar no solo amenazas potenciales sino a quienes perpetran los ataques.

A diferencia del mundo físico, donde los Estados tienen el monopolio legítimo de la violencia y los ataques son extremadamente costosos debido al alto costo de los recursos utilizados, el mundo cibernético permite superar estas limitaciones físicas asociadas al tiempo y el espacio, permitiendo acciones y ataques a bajo costo llevadas a cabo con gran precisión y efectividad (Gomes de Assis, 2017, p. 98).

Esta situación ha hecho que sea cada vez más relevante la gestión del riesgo desde un esquema de gobernanza internacional. La finalidad común de toda corporación multinacional como la gobernanza y la meta-gobernanza, es maximizar los entornos de seguridad en los ámbitos político y económico, para lo cual se generan grupos de presión encargados de vigilar e impactar en las regulaciones internacionales y locales de los Estados (Reyes Beltrán, 2017, p. 59).

3. Una perspectiva de futuro

La soberanía de los Estados ha sufrido importantes modificaciones en el contexto de la globalización y a propósito de la desterritorialización favorecida por la emergencia de las nuevas tecnologías de la información, particularmente, con el auge de las redes sociales. Las nuevas amenazas vinculadas a los Sistemas Ciberfísicos y el Internet de las Cosas -IoT, han presionado la necesidad de contar con un marco de comprensión común de seguridad y defensa del ciberespacio.

La sociedad del conocimiento, debido a un alto grado de incertidumbre frente a las amenazas tecnológicas, se ha visto de igual forma, abocada a establecer parámetros para la gestión del riesgo que se sobrepongan a la asimetría en el acceso y uso de la información y a la brecha tecnológica entre los países desarrollados y en vías de desarrollo. En esta vía, los avances de la seguridad Digital han estado encaminados a

fortalecer las capacidades de Defensa de los Estados con un mínimo de afectación en los derechos de los ciudadanos.

Aunque se ha reconocido el potencial de las nuevas Tecnologías de Información en aplicaciones de uso militar, las naciones se han comprometido con el respeto de los derechos humanos y las libertades fundamentales en el uso de las TIC (A/RES/71/28, 2016). Es así como organizaciones de carácter supranacional como la Organización de las Naciones Unidas -ONU, y la Organización para la Cooperación y el Desarrollo Económicos -OCDE, han proferido comunicaciones y recomendaciones encaminadas a mejorar la seguridad de los Estados en materia digital, respetando la libertad de circulación y acceso a la información.

3.1. El marco internacional

En las últimas décadas se ha evidenciado la necesidad de continuar las investigaciones, el diseño de estrategias y la consolidación de las acciones encaminadas a combatir las amenazas que puedan afectar la seguridad de los Estados. En esta medida, es importante considerar las nuevas Tecnologías de Información y Comunicación como herramientas que pueden ser empleadas con propósitos diferentes a mantener la estabilidad y la seguridad internacional. Se trata de esta forma, de evitar que las tecnologías digitales sean instrumentalizadas con objetivos delictivos o terroristas en detrimento de la seguridad del Estado en las esferas civil y militar.

En el contexto de la seguridad internacional y como respuesta a las amenazas potenciales a la seguridad de los Estados, la comunidad internacional ha adoptado políticas orientadas por la gestión del riesgo en materia digital y tecnológica, con el propósito de salvaguardar la seguridad del ciberespacio. Entre otros, el fortalecimiento de la seguridad Digital pasa por la consolidación de marcos jurídicos supranacionales y un sentido de la Defensa y la seguridad Nacional. Asimismo, se ha considerado que el desarrollo tecnológico y digital es fundamental para el desarrollo de las economías y para la prosperidad social (OCDE, 2015, p. 415 y ss).

El flujo constante de información en el marco de la globalización y la revolución de la tecnología de la información y las comunicaciones representó un cambio sustancial en la forma en que se conceptualizan y enfrentan los riesgos. El ataque del 11 de septiembre y la posterior respuesta contra el terrorismo configuró un entorno político mundial guiado por la constante amenaza de la violencia o de una guerra cuya duración y espacio no se pueden determinar con claridad. Esta imposibilidad de determinar el tiempo y espacio que ha de perdurar el conflicto se profundiza con la aparición de nuevas tecnologías y la expansión de un poder en red.

La OCDE ha señalado la necesidad de un sentido común en la comprensión de la seguridad Digital y la responsabilidad compartida de los diferentes actores que pueden tener parte en su gestión. Esto ha hecho que la Organización recomiende para América Latina y el Caribe disponer de instrucción y capacidades para entender el riesgo y gestionarlo, atendiéndolo como un desafío económico y social y no solo como una cuestión técnica o de seguridad Nacional (OCDE, 2015b).

La Organización de las Naciones Unidas, a través de la *Resolución 71/28*, sobre avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional exhortó a los Estados a promover en una escala multilateral, el examen de las amenazas reales y potenciales en la esfera de la seguridad de la información y de posibles con el propósito de encararlas de manera compatible con la necesidad de preservar la libre circulación de la información y con el propósito ultimo de fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

Para que la Estrategia de gestión del riesgo funcione, es necesaria la participación activa y comprometida de los diversos actores que se involucran en la gestión de los riesgos cibernéticos, comprendiendo empresas, sociedad civil, comunidad técnica de Internet y académicos, entre otros, en el desarrollo e implementación de estrategias y políticas públicas. De esta manera, se avanza, además, en el fomento de la cooperación internacional y la asistencia mutua, según la cual los responsables de políticas deben establecer relaciones multilaterales y bilaterales para

compartir experiencias y buenas prácticas y promover un enfoque de gestión del riesgo de seguridad Digital que no incremente el riesgo de otros países (OCDE, 2015b).

Desde esta perspectiva, el concepto de gobernanza se ha extendido, presentándose como una alternativa que favorece la articulación entre Estados y de estos con organizaciones no gubernamentales de diverso orden, en un entramado público/ privado e inter-sistémico. La gobernanza permite asumir una mirada supranacional, considerando los diferentes actores que tienen lugar en los procesos contemporáneos a nivel internacional, regional y local (Reyes Beltrán, 2017, pp. 156-160).

Un ejemplo de esta forma de acción de acuerdo con los principios de la gobernanza internacional es la adopción por Organización de Estados Americanos de una Estrategia Interamericana Integral de seguridad Cibernética desde un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Como parte de esta estrategia se crea una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de seguridad de Computadores como un esfuerzo conjunto de los Estados Miembros y sus expertos para incrementar la seguridad de las redes y sistemas de información con el propósito de abordar las vulnerabilidades y proteger a los usuarios, la seguridad Nacional y las infraestructuras esenciales del Estado (AG/RES. 2004, 2004).

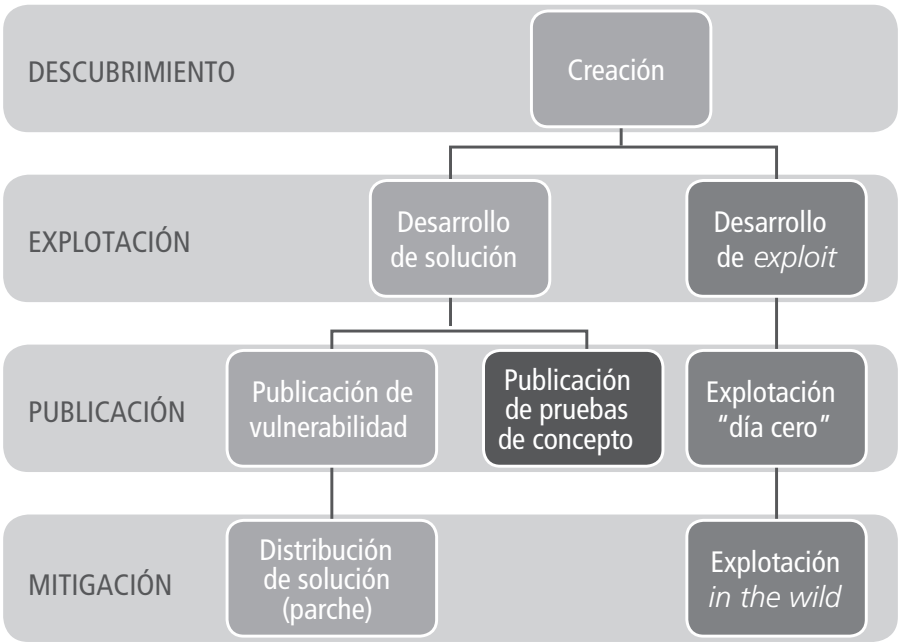
Esta necesidad de articulación ha sido reconocida por la ONU en la Resolución aprobada por la Asamblea General el 2 de diciembre de 2011. En ella se exhorta a los Estados a trabajar de forma articulada frente a las amenazas potenciales a la seguridad Digital, promoviendo normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza respecto del espacio informativo. (A/RES/66/24, 2011) Las recomendaciones de la ONU como de los paneles de expertos dispuestos por la organización señalan el camino para consolidar la seguridad tecnológica en el entendimiento de que las TIC son cimientos de la paz y la seguridad internacionales (UNODA, 2018).

En un sentido similar, la *Decisión 587 de la Comunidad Andina*, adoptada el 10 de julio de 2004, establece los lineamientos de la Política de seguridad Externa Común Andina, señalando dentro de los objetivos

de dicha política prevenir, combatir y erradicar las nuevas amenazas a la seguridad. En coherencia con esto, exhorta a los Estados miembros a actuar de manera conjunta a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.

El Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la seguridad Internacional encargado por la Organización de las Naciones Unidas, examina las amenazas reales y potenciales derivadas de la utilización de las TIC por los Estados y analiza las acciones necesarias para hacerles frente, incluidas normas, reglas, principios y medidas de fomento de la confianza.

Figura 10. Ciclo de vida de las vulnerabilidades



Fuente: Escuela de Altos Estudios de la Defensa (2014, p. 32)

Es así como la gobernanza global permite la articulación del Estado con una pluralidad de organizaciones autónomas cuyas acciones son

indispensables para el desarrollo de la pericia técnica y asesoramiento sobre la preparación de leyes, estrategias y marcos reguladores apropiados para hacer frente a las amenazas cibertecnológicas. Se trata de coordinar las acciones de diferentes entidades para producir y coordinar conjuntos de acciones que se consideran mutuamente benéficas.

3.2. El marco del Estado

La cooperación internacional, sobre la base del mantenimiento de la seguridad mutua, se establece de acuerdo con relaciones globales de carácter flexible. En este escenario y en el sentido que lo señalara Wynne (1998), la legitimidad de las instituciones y los métodos de creación, acceso y divulgación del conocimiento son fundamentales para evaluar el riesgo e identificar a sus principales impulsadores, amplificadores o mitigadores. Así pues, la gobernanza puede entenderse como:

> La organización de la acción colectiva o la toma de decisiones colectivas que incluye mecanismos formales e informales para el uso de las reglas, todo ello coordinado por una gran variedad de actores estatales y no estatales. (Haufler, 2006; Neiva Santos, 2009, pp. 49-53; Reyes Beltrán, 2017, p. 59)

El concepto de gobernanza ha permitido situar al Estado como instancia coordinadora entre otros muchos actores globales, sobreponiéndose a la desconfianza en las instituciones y decisiones del orden nacional y una sociedad en red erosionada. De esta forma, la gobernanza permite ir más allá de los límites del Estado frente a asuntos en los no puede intervenir, empleando para ello un modelo de gobierno basado en la evaluación, control y gestión democrática de los riesgos, cuyo propósito final es intervenir para conciliar los intereses, preferencias y objetivos científicos, políticos, económicos y sociales (Rivera Berrío, 2009, p. 2).

La premisa primordial que orienta las acciones de los Estados en materia de Ciberdefensa es que la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, requieren de acciones eficaces para abordar estas problemáticas, por lo que se

debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales (AG/RES. 2004, 2004).

Según lo anterior, la globalización como proceso estructural ha creado una interdependencia global entre las organizaciones e instituciones en diferentes ambientes funcionales, como la economía y la política, que afectan de forma diferente los diferentes espacios nacionales o locales, originando jerarquías complejas que se desarrollan de forma desigual en el espacio-tiempo, y genera una infinidad de variables dispersas de un amplio alcance espacial (Reyes Beltrán, 2017, p. 157).

El desarrollo de la sociedad del conocimiento se une a la concepción de fomento del desarrollo humano en el que la responsabilidad de los Estados en cuanto a la inversión en ciencia y tecnología es fundamental para disminuir la desigualdad. "El objetivo del desarrollo mediante la innovación exige también la instauración de incentivos financieros" (Unesco, 2005, p. 161). Así mismo, la toma de conciencia sobre riesgos globales y la posibilidad de interconexión en escalas sin precedentes, han fomentado las capacidades de movilización y organización transnacional, ofreciendo la posibilidad de generar una democracia prospectiva acorde con los lineamientos de un gobierno abierto y transparente (Unesco, 2005, pp. 201-202).

Las libertades de opinión, expresión e información, en un Estado democrático, deben favorecer la expresión de opiniones de cualquier índole y la búsqueda, acceso y difusión de la información sin restricciones. El fomento de estas libertades en los Estados debe reconocer y gestionar adecuadamente al menos tres dimensiones, a saber, las posibilidades tecnológicas para que fluya la información, la libertad individual para acceder a ella y el riesgo de que personas ajenas invadan la intimidad y la privacidad de los individuos (Valle, 2003, p. 48).

Es así como la posibilidad de administrar la seguridad Digital debe contemplar tanto los aspectos tecnológicos propios de esta tarea, como la Ley de seguridad, la seguridad Nacional y la Defensa de los intereses de los Estados y los ciudadanos. Los retos que imponen una acción de esta magnitud son fundamentales para la economía y la prosperidad

social por lo que debe contemplar así mismo, una cultura digital de protección desde el ámbito micro (individuos) hasta el supranacional., de forma coherente con los resultados de la aplicación las herramientas de evaluación y una visión general de la política de política pública.

3.3. En Colombia

En este sentido, la *Ley 1288 de 2009*, declarada inexequible por la Corte Constitucional, es un ejemplo de que los requerimientos de las agencias de inteligencia y las normas de una sociedad abierta plantean dilemas para el gobierno democrático. En el *Artículo 2* del primer capítulo, la Ley enuncia:

> La función de Inteligencia y Contrainteligencia es aquella que se desarrolla por organismos especializados del Estado, del orden nacional, dedicados al planeamiento, recolección, procesamiento, análisis y difusión de la información necesaria para defender los derechos humanos, prevenir y combatir amenazas, internas o externas, contra la convivencia democrática, la seguridad y la defensa nacional, y demás fines enunciados en esta ley.

Sin embargo, la Corte en los pronunciamientos *C-567 de 1997*, *T-729 de 2002*, *C-993 de 2004* y *C-981 de 2005*, alegan que en cuanto el derecho a la autodeterminación informática o *hábeas data* consiste en las facultades de conocer, actualizar y rectificar la información personal contenida en bases de datos, y que la forma como estas últimas sean configuradas y administradas delimita el ámbito de aplicación de las facultades que componen el objeto de ese derecho.

> Así mismo, la sentencia C-913 de 2010, establece que En lo atinente a los apartes acusados del artículo 16, explican que este asigna al Gobierno Nacional la competencia para reglamentar los procedimientos de acceso a esta información por parte de los miembros de la Comisión Legal Parlamentaria de Seguimiento a las Actividades de Inteligencia y Contrainteligencia, lo que tampoco sería constitucionalmente factible, al recordar que lo relativo al acceso a la información contenida en bases de datos es un tema que debe ser regulado únicamente por leyes estatutarias.

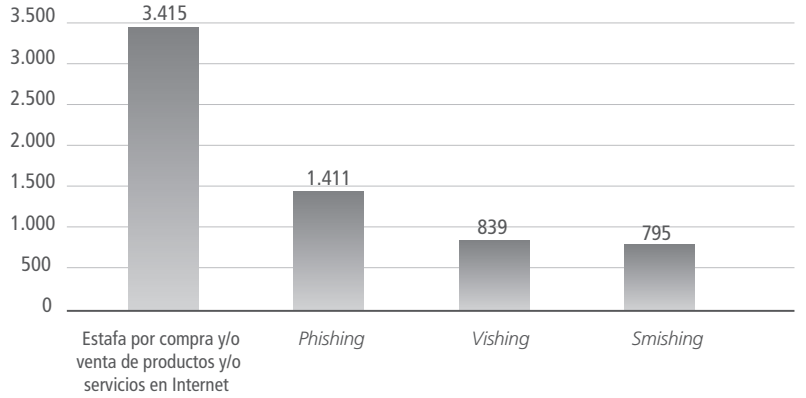
No obstante, en los últimos años se ha presentado un progreso importante frente al desarrollo y aplicación de las tecnologías de la información y las comunicaciones, así como en las acciones encaminadas a consolidar la seguridad y la Defensa en este ámbito. Un avance en este aspecto, luego de que la *Ley 1288 de 2009* fuera declarada inexequible por la Corte Constitucional, es la promulgación de la *Ley 1273 de 2009* por medio de la cual se está creando un nuevo bien jurídico tutelado denominado protección de la información y de los datos orientada hacia la preservación de los sistemas tecnológicos y los derechos de los ciudadanos.

La *Ley 1273 de 2009* crea el marco jurídico a partir del cual en Colombia se hace posible penalizar conductas como el acceso abusivo a un sistema informático, la obstaculización ilegítima de sistema informático o red de telecomunicación, la interceptación de datos informáticos, el daño informático, uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales (p. Cap. 1).

De esta manera, la *Ley 1273* responde a los principales problemas cibernéticos que enfrenta el país, aquellos que tienen que ver con los campos comerciales y financieros. Generalmente, los ciudadanos son quienes más reportan eventos con un 66% de los incidentes, debido a falsas ofertas (*phishing*) publicadas en portales web e incluso reconocidas tiendas de comercio electrónico como mercadolibre.com, OLX.com, tucarro.com.

Las estafas por *vishing* y *smishing*, corresponden a la difusión del mensaje y posterior llamada del delincuente. Una de las modalidades más empleados son los anuncios de premios por parte de operadores de telefonía celular y almacenes de cadena, las falsas ofertas en bolsas de empleo virtuales y la falsa llamada que asegura tener información sobre un sobrino retenido. En este panorama, el Internet de las cosas representa uno de los mayores retos para el gobierno colombiano debido al incremento de usuarios y dispositivos conectados con una cifra que se espera llegue a los 25 mil millones de dispositivos conectados a Internet para el 2020 (Policía Nacional, 2017, p. 12).

Figura 11. Ciberestafa en Colombia, 2016 – 2017



Fuente: Policía Nacional, 2017, p. 4

Las estrategias de Ciberdefensa y ciberseguridad se han desarrollado, además, a partir del *CONPES 3701 de 2011*, en donde se plantean tres pilares fundamentales, la adopción de un marco interinstitucional apropiado para prevenir, coordinar, controlar y generar recomendaciones para afrontar las amenazas y los riesgos que se presenten; el desarrollo de programas de capacitación y formación especializada en seguridad de la información; y, el fortalecimiento de la legislación nacional y la cooperación internacional en estas materias (A/69/112, 2014, p. 7).

Colombia integra el Comité Interamericano contra el Terrorismo, CICTE de la Organización de los Estados Americanos, OEA, que tiene como propósito principal promover y desarrollar la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo. (OEA, 2018) Como parte del CICTE, el país ha logrado trabajar con varios equipos de respuesta ante incidencias de seguridad, CSIRT en la región, proporciona formación técnica a personal especializado, promueve el desarrollo de estrategias nacionales sobre seguridad cibernética, y fomenta el desarrollo de una cultura que permita su fortalecimiento en el continente (CONPES 3854, 2016, p. 15).

Como parte de las estrategias de combate contra las amenazas al ciberespacio y en el marco de la cooperación internacional y las acciones

conjuntas entre los Estados, el Centro Cibernético Policial colombiano (2018) ha enfocado sus esfuerzos en la gestión del riesgo orientada no solo hacia la contención de las amenazas sino también hacia su prevención. En este marco el Centro Cibernético Policial adelanta campañas de concientización, sensibilización y educación de los riesgos de seguridad Digital, en coherencia con las recomendaciones del Consejo mundial de la industria de tecnologías de la información (ITI por sus siglas en inglés).

Asimismo, la política nacional de seguridad Digital consagrada en el *CONPES 3854 de 2016*, adopta una visión de la gestión sistemática y cíclica del riesgo, según la cual se define un objetivo o el diseño de una actividad, se evalúa cuál es el nivel de riesgo de dicha actividad determinando todos los resultados posibles de asumirlo sobre los objetivos sociales y económicos y se determina cómo debería ser modificado el mismo (CONPES 3854, 2016, p. 26).

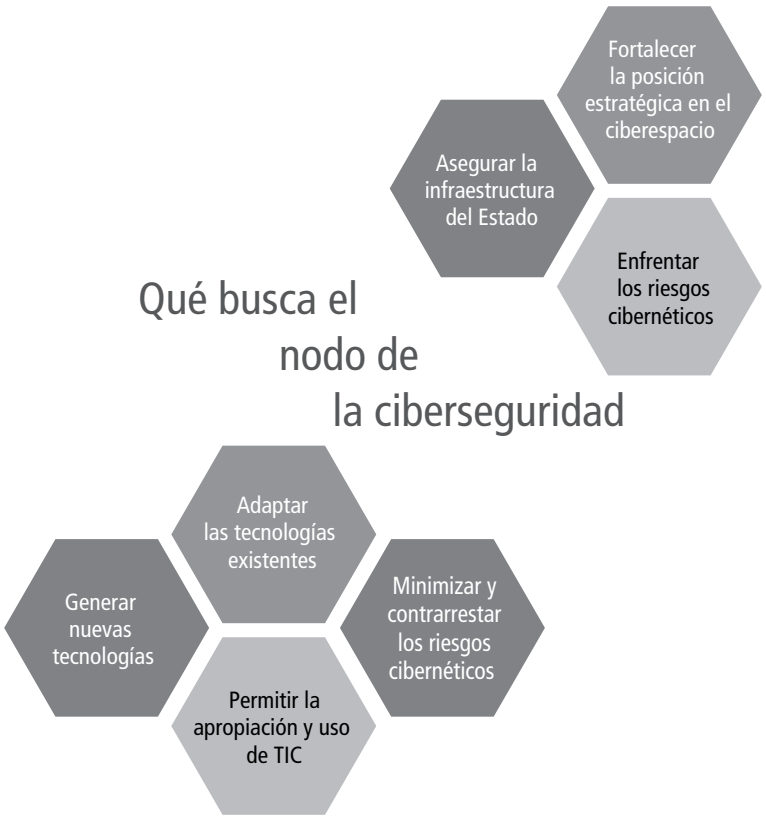
Esta gestión sistemática y cíclica del riesgo es liderada desde el alto nivel del gobierno en favor de la Defensa y seguridad Nacional para estimular la prosperidad económica y social en coherencia con los lineamientos de la OCDE. Adicionalmente, se adopta un enfoque multidimensional que incorpora tanto los aspectos técnicos y jurídicos como lo económico y lo social y a los diversos actores involucrados promoviendo la responsabilidad compartida en coherencia con los lineamientos de la ONU (CONPES 3854, 2016, p. 27).

De esta manera, el *CONPES 3701 de 2011*, concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética. El *CONPES 3854 de 2016*, por su parte, avanzó en el fortalecimiento del Estado frente a las amenazas en el ámbito cibernético comprendiendo la ciberseguridad y la Ciberdefensa Nacional adoptando el enfoque de prevención y gestión del riesgo.

> En el ámbito regional, Colombia se ha posicionado como uno de los países que más ha avanzado en aspectos relacionados con ciberseguridad y Ciberdefensa. Lo anterior, se refleja en indicadores de eficiencia compara-

tiva como el Índice Mundial de ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT). Según este, en 2014 el país se ubicaba en el quinto lugar del ranking a nivel regional, siendo superado por Estados Unidos, Canadá, Brasil y Uruguay mientras que en el plano mundial comparte la novena posición, junto con países como Dinamarca, Egipto, Francia y España (CONPES 3854, 2016, p. 16).

Figura 12. Nodo de ciberseguridad



Fuente: Elaboración propia a partir de MinTIC (2018)

Los esfuerzos de país en cuanto a la cooperación internacional de lucha contra el cibercrimen han avanzado en torno a la noción de gobernanza, entendiendo esta como la acción del gobierno en la coordinación y gestión de redes en las que participan multiplicidad de actores

públicos y privado. Desde esta perspectiva se han desarrollado grupos nacionales de alerta, vigilancia y prevención que contribuyen al desarrollo de estrategias nacionales sobre ciberseguridad en la región y en el mundo, y ha participado en Congresos sobre el manejo de incidentes relacionados con la seguridad de la información y el delito cibernético. (A/69/112, 2014).

En este mismo marco, Colombia ha establecido los vectores de desarrollo, directrices marco, orientadas a fortalecer la posición del país en términos de ciberseguridad, alineados con las diferentes estrategias nacionales provenientes desde las entidades del Estado y del sector privado. De esta manera el Estado colombiano ha afrontado una mayor articulación para prevenir, controlar y manejar las consecuencias de la complejización del mundo en la fase de la globalización.

La gestión del riesgo y la cooperación internacional en materia de ciberseguridad se complementa con procesos de innovación orientados a la generación de soluciones en TIC, con lo que se pretende fomentar las capacidades de los ciudadanos y el Estado para buscar, identificar, estructurar, analizar, recuperar, correlacionar y/o integrar datos relacionados con las incidencias de naturaleza cibernética (MinTIC, 2014, pp. 5-10).

Conclusiones

Las tecnologías de información y comunicación ofrecen oportunidades de interacción y articulación sin precedentes, pero en la misma medida plantea retos, debilidades y amenazas para los Estados y los ciudadanos. La ciberguerra y el cibercrimen son en este contexto, peligros que ponen en riesgo la infraestructura de los Estados, haciendo cada vez más importante aumentar la resiliencia cibernética, llegar a un acuerdo sobre leyes y normas que se apliquen a la utilización de las tecnologías de la información y las comunicaciones y participar en medidas de fomento de la confianza (A/69/112, 2014, pp. 2-3).

Dado el carácter dinámico de las tecnologías y su acelerado ritmo de cambio, el ciberespacio presenta limitaciones para los Estados debido

a la dificultad para establecer el origen de las amenazas y su autoría. De allí que sea necesario avanzar en estrategias que no solo contemplen los aspectos técnicos de las amenazas tecnológicas sino su dimensión social, trascendiendo la visión de la ciberseguridad hacia una de la innovación tal y como ha sucedido en el Estado colombiano.

La innovación y el fomento de la ciencia y la tecnología, permite avanzar en el fortalecimiento de habilidades y capacidades para el descubrimiento diario de nuevas vulnerabilidades en el *software* y *hardware*. El número de incidentes relacionados con ciberataques no parece disminuir en el corto plazo, por el contrario, las proyecciones en hacia el año 2020 indican un incremento acelerado de los dispositivos y usuarios de Internet y dispositivos móviles, incrementando a su vez las amenazas y los riesgos.

Los Estados se han venido preparando para afrontar este contexto en materia de seguridad cibernética, siendo Colombia un caso representativo en la región, manteniendo un suministro constante y fiable de información sobre amenazas y vulnerabilidades en el ciberespacio y determinando las acciones que le permiten responder ante estos incidentes y recuperarse de los mismos, en coherencia con las recomendaciones y acciones de organizaciones supranacionales como la ONU, OEA, OCDE y la Comunidad Andina de Naciones.

Los piratas informáticos, los grupos delictivos organizados y los terroristas que emplean la Internet para fines ilícitos, representan amenazas no solo para la infraestructura de los Estados sino también, para la prosperidad social y económica de sus ciudadanos. Impiden el crecimiento y desarrollo de las nuevas tecnologías de información y comunicación al fomentar el temor frente a medios inseguros y poco confiables para realizar transacciones personales, gubernamentales o de negocios.

En esta medida, se hace necesario continuar en el fortalecimiento de marcos jurídicos nacionales y supranacionales, que sin limitar o afectar las libertades de los usuarios relacionadas con el acceso y difusión de la información, establezca con mayor precisión las características y límites del ciberespacio y las posibilidades de acciones delictivas en él.

Una estrategia de este tipo requiere, además, continuar trabajando en los esfuerzos de articulación entre los Estados y de estos con usuarios y actores privados con posibilidad de acceder a Internet.

Sin duda, la gestión del riesgo y la gobernanza representan dos de las herramientas más importantes para el fortalecimiento de las capacidades de los Estados en materia de ciberseguridad y ciberdefensa. Estas permiten el abordaje cíclico y sistémico de las amenazas y proveen las posibilidades de cooperación que hace posible mantener un flujo de información constante y necesario para afrontar amenazas cambiantes que comportan un alto grado de incertidumbre. Estas herramientas y las relaciones que se posibilitan a partir de allí representarán en el horizonte 2020 un nuevo campo para las prácticas de la Inteligencia estatal.