CAPÍTULO X

CIBERGUERRA: NUEVOS DESAFÍOS A LA SEGURIDAD DE LOS ESTADOS*

Juan Pablo Monzón Torres

* Capítulo de libro resultado del proyecto de investigación "Nuevas Amenazas en el siglo XXI: Fronteras y Derechos Humanos", de la línea de investigación "Políticas y modelos de seguridad y defensa" del grupo de investigación "Centro de Gravedad", reconocido y categorizado en (A1) por COLCIENCIAS, registrado con el código COL0104976, vinculado al Centro de Estudios Estratégicos en Seguridad y Defensa Nacionales -CSEDN-, adscrito y financiado por la Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia.

Resumen
Actualmente, los escenarios clásicos en los cuales se llevaban a cabo los enfrentamientos armados directos entre los Estados han cambiado. Se tiene conocimiento previo de que los cuatro dominios de la guerra son la tierra, el aire, el mar y el espacio; pero hoy en día, se ha instaurado un nuevo dominio el cual, hace unas décadas no era considerado como un posible escenario para que se desarrollara un conflicto. Dicho dominio es el ciberespacio, el cual es normalmente utilizado como una plataforma virtual en donde se establecen redes e interconexiones entre los usuarios. Sin embargo, actualmente es utilizado como un escenario ideal para las ciberguerras entre los Estados, ya que, al establecer una relación costo-beneficio, es posible evidenciar que son más los beneficios para los Estados que emplean este método de ataque cibernético. Ahora bien, lo anterior genera el siguiente interrogante ¿de qué manera algunos Estados han empleado la ciberguerra como una nueva amenaza a la seguridad nacional de los Estados en el sistema internacional? Para ello se van a mostrar ejemplos claros de conflictos entre algunos Estados en los últimos años en donde se utilizó la ciberguerra como nueva alternativa para vulnerar la seguridad y defensa de estos.

Palabras clave
Ciberguerra, Ciberseguridad, Tecnología, Ciberespacio, Seguridad, Defensa, Estados, Ciberdefensa, Información, Soberanía.

Abstract
Today, the classic scenarios of direct armed encounters between states have changed. Previous knowledge about the realms of war suggests four–land, air, sea, and the outer space, but now a new realm, which decades ago was not considered as such, has achieved a paramount status on its own. Cyberspace, usually considered as a virtual platform where networks are established between users, nonetheless, today is being used as an ideal scenario to wage interstate cyberwarfare, as from a cost-benefit calculation States would find positive incentives using cybernetic attacks. How do some States have employed cyberwarfare to threaten the national security of other States members of the international system? This question remains to be answered and, for this reason, I will use examples of interstate conflict from recent years where cyberwarfare

was used as an alternative to weaken or erode the security and defence capacity of target countries.

Keywords
Cyberwarfare, Cybersecurity, Technology, Cyberspace, Security, Defence, States, Cyberdefence, Information, Sovereignty.

Los avances tecnológicos de las últimas dos décadas han permeado directamente el accionar y proceder de los Estados del sistema internacional, puesto que la tecnología se ha vuelto en un factor definitorio y diferenciador entre los Estados. Hoy en día, la capacidad militar de un país tiene una estrecha relación con los alcances tecnológicos a los que un Estado pueda acceder de acuerdo con el presupuesto nacional que le sea destinado a los ámbitos de Seguridad y Defensa Nacionales, por esto, resulta ser un punto de inflexión a la hora de establecer una diferencia en qué Estado es más desarrollado, o no, en estos temas. Sin embargo, como el sistema internacional no solo abarca un actor sino muchos más, que no solo pueden ser catalogados como Estados sino también ONG´S, organizaciones de crimen organizado, grupos terroristas, entre otros; entonces estos avances tecnológicos están disponibles para el que quiera hacer uso de ellos, por lo que las ventajas en términos de seguridad y defensa no son para uno sino para varios actores.

Así pues, en este nuevo siglo los avances tecnológicos han sido tan inherentes en los campos de acción de la Seguridad y Defensa de los Estados, que el teatro de operaciones o campo de batalla clásico en donde se llevaban a cabo los enfrentamientos directos militares entre Estados o entre un Estado y una organización criminal han cambiado de manera drástica; si bien hace unos años el ciberespacio no era considerado como un escenario para las guerras, hoy en día:

> El ciberespacio se ha convertido en la quinta dimensión de la guerra. Así lo explicó a comienzos del año 2011 el Secretario de Defensa de los Estados Unidos de América, Robert Gates. El ciberespacio se une a la tierra, el mar, el aire, y el espacio, como dimensiones de la guerra para los que los Estados deben estar preparados. (Gaitán, 2012, p. 5)

Ahora bien, este nuevo escenario para los conflictos ha tomado mayor fuerza en los últimos años por el alcance y el impacto que pueden generar los ciberataques, desde un individuo hasta un Estado como tal sin la necesidad de estar físicamente en el mismo lugar del objetivo.

> El ciberespacio se ha configurado como el entramado de tecnologías informáticas que se constituye como el pilar sobre el que se erige y sustenta un medio ambiente virtual de información y de continua interacción humana y artificial trasgrediendo el espacio geográfico del mundo y las barreras temporales de comunicación, por lo que forma parte de todas las actividades diarias del mundo. Por lo anterior, este nuevo escenario se ha descrito como una red interdependiente de sistemas de tecnologías informáticas, entre las que se denotan los computadores o procesadores, la internet, y los sistemas de control de la infraestructura crítica del Estado. (Gaitán, 2012, p. 19)

Hay que tener en cuenta también, que el ciberespacio se ha vuelto una nueva dimensión de la guerra, por la cantidad de beneficios que se le puede ofrecer al usuario que quiera realizar un ciberataque dentro de este medio ambiente virtual, entre ellas está un alto grado de anonimato y de posible indetectabilidad del individuo, o los individuos, que quieran realizar un ataque en representación de un Estado, o simplemente una organización criminal o, a su vez, de una gran empresa. Asimismo, la variedad de autores de los ciberataques es muy amplia por las mismas libertades expuestas dentro de este nuevo escenario de guerra. También está la velocidad de los ataques, que van en concordancia con lo que ya se mencionó: no hay la necesidad de estar físicamente en el lugar al que se quiera afectar con los ciberataques y, por consiguiente, no está la amenaza de exponer la integridad física por el riesgo que implica querer afectar algo o a alguien en el ciberespacio; así mismo, el ciberespacio ofrece la posibilidad de crear conexiones entre individuos y redes de información de manera muy rápida lo que posibilita que los ataques sean en su mayoría muy efectivos.

Adicionalmente, el ciberespacio acoge una gran variedad de conceptos que hoy en día, con la globalización de las comunicaciones, han tomado gran relevancia. Algunos de esos conceptos son: la guerra de redes, el ciberterrorismo, las operaciones de información, la ciberdefensa,

la ciberseguridad, la ciberguerra, entre otros. Aunque, como se mencionó anteriormente, este escrito se va a centrar principalmente en los últimos tres y, en la relación que se establece entre estos conceptos respecto a los nuevos desafíos a los que se enfrentan la seguridad y defensa de los Estados hoy en día. Según Richard Clarke (2004), especialista en seguridad del gobierno de Estados Unidos, "la ciberguerra son las acciones efectuadas por una organización-nación-Estado con el propósito de penetrar los sistemas informáticos y redes de computadores de otra nación-Estado, con el fin de causar daños o interrupción de estos" (Citado en Salazar, 2016, p. 25).

Así pues, es evidente que la globalización de las comunicaciones y las redes de información han adquirido un nivel de importancia muy alto en el sistema internacional. La información hoy en día se ha convertido en un elemento disuasorio para los Estados y el resto de los actores en el sistema, tanto así que, ésta puede llegar a ser un factor decisivo en la elección de un presidente de una nación, como se pudo ver reflejado en las pasadas elecciones en Estados Unidos, en donde Hillary Clinton aparentemente tenía una amplia ventaja sobre su máximo contendor en ese momento, Donald Trump. Pero, cuando salieron a la luz más repercusiones del escándalo de los correos electrónicos de la ex Secretaria de Estado, perdió la buena imagen que tenía en ese entonces para los votantes, lo que hace entrever que la información es un material clave, pero pasa a ser un elemento de poder definitorio para quien le emplee de mejor manera. Ahora bien.

> La […] dependencia de los y de las personas abre una ventana de riesgo para todas las actividades desarrolladas en la sociedad digital. […] Entre mayor dependencia exista […], mayor será la capacidad de las nuevas tecnologías para afectar la vida de los individuos, lo que hace del ciberespacio un escenario propicio para la guerra. (Gaitán, 2012, p. 30)

Por otro lado, los personajes que toman un papel preponderante y vital en el ciberespacio como teatro de operaciones para las nuevas guerras digitales son los hackers, que también reciben el nombre de soldados digitales y son los individuos que tienen la capacidad desde

poner en jaque infraestructuras críticas de los Estados hasta robarse información confidencial de las agencias de inteligencia de estos mismos para someterlos de acuerdo con la importancia de la información que es raptada, ya sea para otros Estados o para algunas organizaciones criminales.

> Con la ciberguerra se busca que hidroeléctricas abran sus compuertas sin aviso para inundar poblaciones aledañas, que reactores nucleares se recalienten y entren en crisis (o bien que dejen de funcionar), que oleoductos y refinerías ardan en llamas, que los sistemas bancarios y financieros nacionales sufran desplomes informáticos (que después se reflejan en desplomes reales de la economía), que los controladores aéreos no puedan guiar el tráfico aéreo, o bien, que el Gobierno quede incapacitado de prestar servicios y generar vínculos de comunicación de manera efectiva con los ciudadanos. (Gaitán, 2012, p. 78)

Lo anterior demuestra entonces, el nivel de alcance en cuanto a daño que pueden generar los ataques cibernéticos en una hipotética guerra entre Estados. Sin embargo, el concepto de ciberguerra sigue siendo un tema muy poco valorado y no tomado en serio en cuanto a su alcance y su realidad; hoy en día, en el mundo son más los Estados y la población del común, que ignoran al ciberespacio como nuevo dominio de la guerra y, por consiguiente, a la ciberguerra como método veraz para vulnerar la seguridad y defensa de los Estados.

La ciberguerra es una realidad, no es un ámbito a futuro como han querido dejar entrever distintos medios en el mundo, que han querido tocar este tema que, evidentemente es novedoso, pero, es un concepto que puede empezar a ser clave en la actualidad en cuanto a cómo un Estado puede afectar efectivamente a otro, reduciendo costos, tanto operacionales como físicos, y en un tiempo mínimo. Así, es perceptible el nivel de importancia que tiene la ciberguerra y, específicamente, las acciones que pueden llegar a protagonizar individuos que tengan un acceso al ciberespacio. Aunque en el papel, el nivel de alcance de las acciones o ataques de un hacker con acceso a este medio ambiente virtual dependería de la experiencia y claramente de las habilidades en este tema. Pero, yendo a la práctica no se puede subestimar a ningún

individuo por falta de experiencia o por no tener amplios conocimientos en el medio, ya que hasta un niño puede llegar a tener desde la habilidad de hackear cajeros automáticos para sustraer grandes cantidades de dinero, hasta adaptar un simple control remoto de televisión para manipular el control de las intersecciones viales de un tren a su antojo, al punto de, como ya ocurrió, desviar los rieles del tren causando un accidente que provocó que aproximadamente 12 personas salieran heridas por este hecho (Bella, 2008), lo cual demuestra que con conocimientos mínimos en cibernética se puede llegar a causar un gran daño a la sociedad.

Por otro lado, es necesario mencionar que los Estados más desarrollados en el sistema internacional sí le han dado la atención e importancia que merece a este innovador método de guerra entre Estados; es el caso de Estado Unidos, Rusia, China, Israel, por mencionar algunos. Estos son Estados que están a la vanguardia de todos los avances tecnológicos y medios no convencionales que les permitan superponer sus intereses económicos y geopolíticos por encima del resto de actores del sistema y es que en la ciberguerra no es fundamental, como tampoco lo son tiempo, ni el espacio, ni el clima, ni el arsenal, ni el número de tropas, ni la movilización, ni las pérdidas humanas. El factor central de la ciberguerra radica en encontrar brechas de seguridad para afectar las redes de información y comunicación de otros Estados. "Los ataques cibernéticos capitalizan las debilidades que tiene el sistema informático para extraer información estratégica o boicotear procesos vitales para la nación" (Gaitán, 2012, p. 30). Por esto, los Estados hoy en día emplean parte del presupuesto destinado al sector defensa de la nación, a fortalecer los ámbitos de la ciberseguridad y ciberdefensa, puesto que, como se ha podido ver, son formas de vulnerar la soberanía de los Estados seguido de todo lo que ello implica.

> La ciberdefensa, en caso de que se produzcan ciberataques, será una de las responsables principales de actuar en el ciberespacio para obtener, analizar y explotar la información de los incidentes y ejercerá la respuesta oportuna, legitima y proporcionada en el ciberespacio ante amenazas o agresiones que

> puedan afectar a la Defensa Nacional, a su vez, está bajo la responsabilidad de un Mando Conjunto de Ciberdefensa que es instaurado dependiendo del Estado en cuestión. (Segura & Gordo, 2013, p. 160)

A pesar de ser un campo tan novedoso y reciente, el ámbito de la ciberdefensa debe ser inherente al campo táctico y estratégico de las Fuerzas Armadas de los Estados, puesto que actualmente, el ciberespacio ha pasado a tener el mismo nivel de relevancia que los demás dominios de la guerra (agua, aire, tierra y espacio) y, por ello, deben ser complementarios. Sin embargo, al ser el ciberespacio un medio digital o virtual permanente y dinámico, que está disponible en todo el mundo, a cualquier hora y con restricciones muy leves para todos los usuarios que deseen navegar en ella; sugiere que las Fuerzas Armadas a nivel mundial, se enfoquen en mayor medida o principalmente en este nuevo dominio.

Ahora bien, hay que tener en cuenta que la ciberdefensa comandada por las Fuerzas Militares y los servicios de inteligencia de un Estado, no sólo manejan dentro de sus funciones la de prever y protegerse de posibles ciberataques que puedan ocurrir dentro del ciberespacio y que causen algún tipo de afectación al Estado, sino también está dentro de sus alcances y acciones a tomar; la de repeler, contrarrestar o incluso anticiparse a posibles amenazas a la seguridad nacional por medio de ataques mancomunados con las Fuerzas Armadas, ya sea en un plano físico y real o simplemente en el ciberespacio. Aunque, en las últimas dos décadas no había registros de respuestas físicas a un ciberataque o respuestas anticipadas a una posible amenaza, ya que siempre los conflictos se manejaban únicamente en el plano virtual, pero, en el mes de mayo de 2019, las Fuerzas Militares de Israel, lanzaron misiles hacia un edificio situado en la Franja de Gaza, donde según ellos, estaban asentados unos supuestos hackers de Hamas (grupo extremista religioso palestino) y, que planeaban desde esa locación un ciberataque en contra del Estado israelí (Nemirovsci, 2019). Así entonces, esto abrió el debate sobre si la única forma de combatir o repeler ciberataques o amenazas latentes dentro del ciberespacio, eran dentro de este medio. No obstante, a partir de este hecho, está claro que no es así, por lo que Israel se convirtió en el

primer Estado que comandó una respuesta física ante la amenaza de un posible ciberataque dentro del conflicto palestino-israelí.

Entre tanto, como se mencionó anteriormente, el hecho ocurrido en la Franja de Gaza es una indudable expresión de lo que ya se ha dicho sobre la ciberdefensa y su manera de operar, pero, puntualmente a la hora dar una respuesta anticipada a un posible ciberataque y no solo previendo o protegiendo ante posibles amenazas. Entonces:

> Las capacidades de la ciberdefensa radican en primer lugar en la defensa; que incluya las medidas y acciones de protección, proyección, detección, reacción, recuperación frente a ataques, intrusiones, interrupciones u otras acciones autorizadas que puedan comprometer la información y los sistemas que la manejan. En segundo lugar; la explotación, que permita la recopilación, análisis y aprovechamiento de información de los ciberataques para determinar la procedencia e impacto y, por último; la respuesta que incluya las medidas y acciones a tomar ante amenazas o ataques. (Segura & Gordo, 2013, p. 166)

Por otro lado, al abordar el concepto de seguridad, es común que se genere la discusión sobre la diferencia entre el tema de la seguridad y la defensa. También, al hablar del ciberespacio y, puntualmente de cómo un Estado se blinda ante las posibles amenazas no convencionales que se presentan dentro de este medio virtual, aparece también el ámbito de la ciberdefensa y, por supuesto, el de la ciberseguridad, que tienen la misma función pero su nivel de alcance es diferente, ya que la ciberseguridad "se refiere a la capacidad de un Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética (CONPES 3701, 2011). Y si bien, sus objetivos dentro del Estado son los mismos, los de proteger al Estado y sus habitantes ante cualquier incidente en el espacio cibernético, se diferencia de la ciberdefensa en que, dentro de las funciones de una política de ciberseguridad instaurada por un Estado, está la de únicamente proteger y velar, como ya se ha mencionado y, en el caso de la ciberdefensa si puede actuar y darles una respuesta a dichas posibles amenazas como manera preventiva. Pero, son dos conceptos totalmente complementarios y, que, al fin y al cabo, tienen el mismo fin dentro del sector defensa de una nación.

Ahora bien, luego de contextualizar sobre los desafíos a los que se puede enfrentar un Estado y su población al estar inmersos dentro del extenso mundo del ciberespacio, es posible denotar que los niveles de riesgo son muy altos. A su vez, dentro de este medio virtual se pueden encontrar hackers para los cuales una de sus finalidades sea la de la captación ilegal de dinero, al mismo tiempo que se pueden encontrar ciberterroristas, mafias, ciberejércitos, ciberactivistas, ciberdelincuentes, entre muchos otros criminales que simplemente con acceso a un computador e internet, pueden causar mucho daño a la sociedad. Sin embargo, el objetivo de este escrito no es el de abordar a todos estos ciberatacantes, sino centrarse principalmente en la manera en que un individuo o un grupo de especialistas en la captación de información o expertos en control de tecnologías; han sido utilizados por el sector de Defensa e Inteligencia de un Estado para superar las barreras de ciberseguridad y ciberdefensa de otro Estado, para generarle ya sea una afectación considerable en alguna de sus infraestructuras críticas o la captación de información clave, que son los fines de la ciberguerra como ya se ha mencionado en este escrito.

En primer lugar, está el que para diferentes medios académicos es considerado como el primer hecho registrado de ciberguerra y es el que protagonizó el Estado ruso contra el gobierno estonio:

> En abril de 2007, el gobierno de Estonia anuncio públicamente la remoción y reubicación de un monumento soviético que se encontraba en la capital del país, Tallin, para ser trasladada a un cementerio central militar nacional. La decisión gubernamental genero de inmediato controversias entre los estonios de descendencia rusa que veneran la estatua, y los estonios naturales que ven en el monumento un símbolo del antiguo régimen de represión. Los ataques que recibieron las paginas cibernéticas gubernamentales y comerciales, de redes bancarias estonias, a partir del mes de abril fueron decisivos. A través de ciberataques, el gobierno ruso logro tomar control de los contenidos de los sitios públicos y sustituyo su información por propaganda política a favor de la causa rusa, y otros más fueron bloqueados para inhabilitar su funcionamiento y comunicación. En tanto que los ataques perduraron por semanas, para el nueve de mayo, día en el que los soviéticos conmemoran la derrota de Hitler, los ataques cibernéticos

> se intensificaron y recrudecieron significativamente; hasta el punto de que las páginas webs ministeriales se transformaron en sitios inservibles, y los ciudadanos no pudieron hacer compras *on-line* durante varios días, lo que perjudicó severamente la economía estonia, que se dinamiza en gran medida a través del ciberespacio. (Gaitán, 2012, pp. 180-181)

Así pues, Estonia es conocida como uno de los países en el mundo que está a la vanguardia de todos los avances tecnológicos, tanto así, que tienen incorporada la tecnología en casi todos los servicios prestados por el Estado. Es decir, en Estonia prácticamente todo funciona automatizado y si bien, hoy en día es un Estado que es sólido en cuanto a ciberdefensa, ciberseguridad y políticas fuertes de seguridad de la información, donde toda la información a nivel estatal, público y privado mantiene viajando por el ciberespacio; han sabido transformarse en una de las potencias cibernéticas por el alto porcentaje de invulnerabilidad. Sin embargo, en el papel, ese amplio conocimiento, buen manejo y control del ciberespacio los catalogaría como un Estado fuerte en el ámbito de la ciberguerra, pero, esa misma dependencia tecnológica y automatización de gran parte de sus procesos sociales, políticos, económicos, culturales, etc., fue lo que los hizo más vulnerables al momento de que fueran blanco de los ciberataques perpetrados por el gobierno ruso.

En segundo lugar, tal vez, el caso de ciberguerra sin parangón alguno hasta el momento es el ataque que sufrió Irán en el año 2010:

> Una ciber-arma denominada como *gusano Stuxnet* invadió los sistemas informáticos que controlan específicamente la infraestructura crítica de ese país. Según los análisis de las autoridades y sectores de defensa e inteligencia iranís, el gusano, con la capacidad de reproducirse rápidamente por el ciberespacio y por terminales conectadas, entro a la red informática de Irán por medio de una *flahsdrive* que fue enlazada al procesador con conexión a esta. Posteriormente, al llegar al mes de junio de 2010, el *Stuxnet* se activó desde cada una de las computadoras en las cuales se había alojado anónimamente, y así el ataque fue perpetrado. El gusano, una vez inició su ofensiva, fue programado para que buscara específicamente los sistemas informáticos que controlaban el comando y control del reactor nuclear de *Natanz.* (Gaitán, 2012, p. 187)

Para este hecho, si bien no hubo una fuente oficial que adjudicara el ataque, se dice que fue perpetrado mancomunadamente entre Estados Unidos e Israel para afectar directamente dicho reactor nuclear. Ahora bien, el *gusano Stuxnet,* es una ciber-arma muy avanzada que, aunque hoy en día no es la más poderosa y actualizada, en ese entonces sí lo era, y era considerada de las ciber-armas más letales dentro del ciberespacio y utilizada en una ciberguerra entre Estados. Adicionalmente, esta ciber-arma contaba con el plus de poseer un desarrollo informático muy sofisticado, y el personal humano que la manipulara tenía la potestad de asignarle un objetivo específico, con rutas y efectos preestablecidos, lo que generaba que el margen de error fuera muy reducido. Lo cual, deja entrever que este ciberataque no podía haber sido producto del azar o por un accidente en cuanto a su manipulación, ya que es una ciber-arma que funcionaba de acuerdo con una misión asignada y, en este caso puntual, el objetivo claro era afectar al reactor nuclear iraní.

Además, se debe que tener en cuenta que este reactor nuclear iraní, tenía como función principal la de proveer electricidad a las redes eléctricas nacionales, y así, ser de los principales suministros de energía alternativa para el Estado, lo cual lo convierte claramente en una infraestructura crítica que, desde hace una década la seguridad de las infraestructuras críticas vienen ocupando la agenda de los responsables políticos en todo el mundo como un aspecto estratégico para garantizar la propia seguridad de los países y sus ciudadanos. "Las infraestructuras críticas, son el conjunto de recursos, servicios, tecnologías de la información y redes, que, en el caso de sufrir un ataque, causarían un gran impacto en la seguridad, tanto física como económica de los ciudadanos o en el buen funcionamiento del Gobierno de la Nación" (Segura & Gordo, 2013, p. 215). Por ello, y teniendo en cuenta el caso iraní, es evidente que el objetivo de dicho ciberataque era establecer un daño a esta infraestructura crítica que impidió un avance y una mejora en la calidad de vida de la población, ya que este reactor nuclear, luego de este hecho, estuvo aproximadamente un año y medio sin funcionamiento y sin la posibilidad de que se hiciera su apertura oficial. Otro aspecto relevante del hecho fue que el virus informático, atacó principalmente el software

que controlaba y mantenía en movimientos establecidos a las máquinas centrifugadoras del reactor, causando la destrucción de estas y, que además de ayudar a la generación de energía, servían para la separación de uranio enriquecido, material propicio para el desarrollo de armamento nuclear.

> En el mes de julio de 2008 una firma georgiana de seguridad de la internet registró un ataque del tipo *DDoS* (*Distributed Denial of Service,* por sus siglas en inglés) contra las páginas web del Estado. Un mes después, se presentó un segundo ataque mucho más poderoso que afectó contundentemente a las páginas del gobierno de Georgia hasta llevarlas a la parálisis temporal, generando así que los servidores públicos tanto políticos como militares quedaran impedidos para comunicarse a través de la internet. Según las investigaciones de los analistas del ciberataque, paralelamente al advenimiento del segundo ataque, se desarrolló una movilización de tropas del Ejército ruso hacia la región del sur de Georgia denominada Osetia, un día después de que el gobierno local también movilizara algunas escuadras sobre su frontera. Desde esta perspectiva, el ataque *DDoS* se llevó a cabo con el fin de deshabilitar la comunicación gubernamental por medio de canales informáticos para desestabilizar las capacidades de mando y control; elemento que influiría contundentemente en la capacidad de respuesta a la invasión militar que se llevaba a cabo, de manera simultánea, en la frontera entre Rusia y Georgia. (Gaitán, 2012, p. 181)

En tercer lugar, está el caso de ciberguerra entre Rusia y Georgia, en donde, como ya se mencionó anteriormente, el gobierno ruso utilizó un ciberataque *DDoS*, o también llamado ataque de denegación de servicio, "dónde existen múltiples focos distribuidos y sincronizados que canalizan su ataque en un mismo destino. Y en donde existe la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros" (Universidad Politécnica de Cataluña, 2019), este ataque fue llevado a cabo con fines geoestratégicos por el momento coyuntural que atravesaba la frontera ruso-georgiana, ya que las Fuerzas Militares rusas buscaban desactivar el contacto entre los centros de comando de las Fuerzas Armadas de Georgia con los militares que ya estaban asentados en la frontera con la federación rusa, y así, evitar que dicha infantería

fuera notificada a tiempo de las tropas rusas que se desplazaban hacia ese territorio. Lo cual, hace denotar la estrategia en cuanto a guerra implementada por las Fuerzas Militares rusas para asegurar en mayor medida un resultado más fructífero por dicha avanzada de sus tropas. A su vez, este accionar puede llegar a ser considerado como uso de la fuerza por parte del gobierno ruso, ya que capacitó o utilizó personal con conocimientos en estos servicios cibernéticos, dentro de sus fuerzas militares para que llevaran a cabo este ciberataque al esquema militar georgiano y así hacerlo más vulnerable.

Por otra parte, otro ejemplo de ciberguerra que va al caso fue el ocurrido en septiembre de 2007, en donde "Aviones F-15 y F-16 israelíes bombardearon una supuesta planta de armas nucleares en Siria después de **burlar misteriosamente la sofisticada red rusa de defensa aérea**. Varios comentaristas especularon que Israel hackeó esta red utilizando un programa informático conocido como *Suter*, diseñado para inhabilitar redes de comunicaciones enemigas. *Suter* fue desarrollado por *BAE Systems,* y funciona mediante el bombardeo de sistemas de radar con datos que incluyen falsos objetivos y mensajes engañosos" (Blog, 2015). En efecto, este ciberataque a manos del Estado israelí en su momento fue una maniobra que mostró claramente los intereses geopolíticos de esta nación, ya que siempre se ha tenido conocimiento del interés marcado de Israel de que no se desarrolle o se potencie en gran medida armamento nuclear a lo que respecta en su periferia o Estados contiguos en su hemisferio.

También claro está, que impulsado por el respaldo de Estados Unidos y, bajo las directrices de lo que infiere su ya conocida alianza geopolítica, económica y militar, que siempre han actuado como vigilantes en cuanto al tema de la proliferación nuclear. Adicionalmente, como ya se ha mencionado, el poderío de Israel en cuanto a ciberguerra es muy extenso y notorio en el sistema internacional. Su capacidad de efectuar ciberataques dentro del quinto dominio de la guerra, hacen denotar que actualmente podría llegar a ser considerado como una de las más grandes superpotencias en la manipulación del ciberespacio y por ende, de la ciberguerra; una demostración clara fue el hackeó efectuado a la red

de defensa aérea rusa asentada en el territorio sirio, por medio de dicho bombardeo de datos a los radares que vigilaban cualquier presencia de misiles, inclusive, siendo la tecnología militar rusa de las mejores del mundo.

"La agencia oficial Xinhua hacía público un informe, elaborado por el Centro de Coordinación Nacional de Respuestas a Emergencias de Red (CNCERT), en el que se detalla que 85 páginas web de instituciones y compañías estatales chinas, habían sido atacadas desde el exterior entre septiembre de 2012 y febrero de 2013. El documento ubica en Estados Unidos el epicentro de operaciones del 73,1% de los servidores que utilizaron sistemas de control para apoderarse ilegítimamente de los datos contenidos en los ordenadores chinos. Entre los objetivos vulnerados figura la web oficial de El Diario Pueblo (people.com.cn), el Portal de Información Gubernamental (China.com.cn), además de una compañía de seguros de la propiedad y un centro de investigación de virus en el centro de China. Por otro lado, El Pentágono declaró que el Ejército Popular de Liberación Chino realiza frecuentes ejercicios militares, en los que demuestra los avances en tecnología de la información juntamente con Fuerzas Militares convencionales. Bajo el epígrafe Ciberactividades dirigidas contra el Departamento de Defensa, un informe del Departamento de Defensa acusa formalmente a China de actividades ilegítimas en el ciberespacio: en 2012, numerosos sistemas informáticos de todo el mundo, incluyendo aquellos que pertenecen al gobierno de Estados Unidos, continúan siendo objetivo de intrusiones, alguna de las cuales parecen ser atribuibles directamente al gobierno y militares chinos. Estas intrusiones están dirigidas a obtener información. El informe continúa afirmando que China utiliza las capacidades de sus redes informáticas para incrementar sus conocimientos de inteligencia, que luego podrían ser utilizados contra la diplomacia y la economía de Estados Unidos (Illaro, 2013).

Por último, y quizás sea el ejemplo de ciberguerra más controversial y que ha perdurado más a pesar del paso de los años, es en el que se enfrentan a los Estados Unidos de Norteamérica y a la República Popular de China que, como se ha podido evidenciar anteriormente, no ha sido

una disputa únicamente en términos comerciales y por quien asumirá el título de potencia hegemónica de los últimos años en el sistema internacional. Sino que también, ha sido una disputa que ha trascendido al ciberespacio y con ello a la ciberguerra entre Estados.

Ambos hechos expuestos anteriormente, dejan entrever que tanto Estados Unidos como China, por medio de sus Fuerzas Militares y sus comandos de inteligencia, han llevado a cabo operaciones de incautación de información en contra del otro país, con fines más allá de la común guerra comercial que han protagonizado por años; sino más llevado a los intereses geopolíticos por mantenerse informados de la situación financiera de cada uno y de cómo están preparados en cuanto a los ámbitos de Seguridad y Defensa Nacionales. Otro aspecto para tener en cuenta, es que si bien uno de los hechos que caracteriza a la ciberguerra entre Estados es la vulneración de la ciberdefensa y ciberseguridad para la obtención de información confidencial de los Estados, en este caso puntual, y a diferencia de algunos de los casos ya mencionados a lo largo del escrito, Estados Unidos y China, no captaron la información con fines bélicos o con el objetivo de afectar directamente alguna infraestructura crítica de su contraparte, lo que denota el respeto de alguna forma entre ambas naciones y, que si se hubiera dado en alguno de los casos, habría sido una clara muestra del uso de la fuerza hacia el otro Estado, lo cual muy seguramente causaría un quiebre en el orden internacional.

De igual forma, también hay que resaltar que ambas naciones fueron blancos de ciberataques, pero específicamente corporaciones de renombre con procedencia en dichos Estados, aunque, algunas con presencia a nivel mundial como fue el caso de Coca Cola, por nombrar alguna. Es decir, al ser Estados Unidos y China dos potencias desarrolladas y, sin entrar en la discusión de quién por diversos hechos es quien opta hoy en día por el título de la más grande potencia en el sistema; lo que hay que destacar es que éstas naciones recurrieron a ciberataques dentro de esta ciberguerra, puntualmente a empresas nacionales con información de estos Estados, pero, no optaron por atacar propiamente a organismos militares y de inteligencia de su adversario, que claramente van a tener

mucho más fortalecidas sus políticas y acciones en cuanto a ciberdefensa y ciberseguridad.

> Siguiendo a Gaitán (2012), "la ciberguerra, con bajos riesgos para los cibersoldados, puede ser vista por los niveles decisorios de la guerra como una forma de establecer un objetivo, pero sin disparar una sola arma. Un atacante podría pensar en una ciber-ofensiva que inhabilite la red de energía eléctrica, y adicionalmente destruya algunos de los componentes principales del sistema informático de la misma (el sistema queda inservible por semanas), un movimiento poco antiséptico; un camino para tener las tensiones en sus niveles más bajos posibles. Pero para millones de personas entrar en un escenario de oscuridad y tal vez de frío, imposibilitada para conseguir alimentos, sin acceso al dinero ni posibilidad de intercambio producto del desorden social, podría ser, en muchas formas, lo mismo que haber lanzado una bomba sobre una ciudad". (p. 188)

Así entonces, lo que se puede ver reflejado es la magnitud del daño que se puede llegar a provocar por medio de la ciberguerra, siendo un arma no convencional con un impacto y repercusiones casi iguales a las de otras armas con gran despliegue operacional y tecnológico.

Ahora bien, no se puede pasar por alto el hecho de que, a medida que sigan pasando los años, más va a crecer el porcentaje de exposición de los Estados y de sus habitantes en cuanto a lo que conlleva estar inmersos en el ciberespacio. Y más aún, ahora que está cada vez más cerca la llegada de las plataformas 5G, pues la superficie de ataque para que se lleven a cabo las ciberguerras entre Estados va a ser mucho más amplia. Hoy en día, las potencias en el sistema internacional están luchando incansablemente por adoptar en el menor tiempo posible las redes de datos 5G, puesto que les implicaría ampliar y abarcar de gran manera las redes de información dentro del ciberespacio. Aunque, de igual manera, las brechas de seguridad que pueden ir apareciendo serán paralelas al incremento en las redes de datos. Lo cual no garantizaría que los Estados que adapten la nueva red 5G, sean inmunes al ciberespacio y a los desafíos que este conlleva.

Hay que tener en cuenta que, en la gran mayoría de los ciberataques perpetrados en las últimas décadas, no siempre hay fuentes oficiales de

los gobiernos que se adjudiquen la total autoría de estos hechos, principalmente porque por razones evidentes no les conviene a estos gobiernos revelar uno de sus métodos para atacar a otros Estados. Además, que después del ejemplo de ciberguerra ocurrido entre Estonia y Rusia, el gobierno estonio pidió apoyo y respaldo a la Organización del Tratado del Atlántico Norte (OTAN), para que se le brindara una asistencia comunitaria de todos los Estados miembro por el ciberataque que sufrió. Sin embargo, en ese entonces al ser una forma de ataque entre Estados tan poco conocida, la OTAN no tenía políticas de ciberdefensa sobre esta modalidad y se le imposibilitó una reacción como organización internacional para poder darle un apoyo propicio a uno de sus Estados miembro. Aunque, también dificulto el accionar de la OTAN, que el Gobierno ruso no se haya adjudicado oficialmente el ataque y, por el contrario, siempre negó su participación en dicha problemática.

Además de lo mencionado, no es conveniente para los Estados atacantes en una ciberguerra confirmar su accionar puesto que se podría esperar una repercusión a gran escala de la comunidad internacional. Por otro lado, como ya se ha mencionado, una de las amplias ventajas de la ciberguerra y precisamente de los ataques dentro de estos ciber conflictos es que el porcentaje de anonimato del responsable de los hechos es muy alto, e imposibilita a los comandos de ciberdefensa y ciberseguridad de los Estados vulnerados, a que puedan identificar con exactitud quien o quienes fueron los responsables; y, bajo el respaldo económico y político de qué Nación exactamente, para que hayan recibido esa misión de violar la seguridad nacional de estos.

Para finalizar, al ser el tema de la ciberguerra entre Estados un concepto que si bien es una realidad y están los hechos verificados en donde hubo Estados que la utilizaron y otros que la sufrieron; no deja de ser un brazo de la guerra muy moderno dentro del sistema internacional. Por ello, actualmente no hay registros dentro de las directrices y postulados del Derecho Internacional, en donde esté expuesta una norma clara y precisa que tipifique a la ciberguerra como un delito de este marco legal internacional. Aunque dentro del Derecho Internacional se juzga por crímenes de guerra, se regula el uso de la fuerza entre Estados, hay un

vacío conceptual y jurídico dentro del sistema internacional para poder juzgar a un Estado por actos de ciberguerra, lo cual es preocupante porque ya se ha podido evidenciar dentro de este capítulo los alcances de esta modalidad de guerra, y por ello, es de vital importancia para el orden internacional establecido que sea próxima la tipificación como delito de la ciberguerra ya sea dentro del Derecho Internacional o por medio de la creación de un acuerdo multilateral que aglomere, suscriba y haga vinculante a todos los Estados.

También, fue posible demostrar el gran desafío que representa el tema de la ciberguerra para la seguridad y defensa de los Estados y, más aún, en dónde ha sido necesario la creación de políticas y comandos conjuntos para que se encarguen de los ámbitos de la ciberdefensa y ciberseguridad estatal. En suma, al ser la ciberguerra una modalidad en donde prima el anonimato, la velocidad de los ataques, la no exposición de la integridad física de las tropas militares, entre otros beneficios; hacen que sea una forma de sobrepasar las barreras de Seguridad y Defensa de los Estados con un porcentaje muy alto de efectividad y así, para los Estados que más inviertan en ser potencias y en estar a la vanguardia respecto a esta alternativa de guerra, será cada vez más fácil que impongan sus intereses geopolíticos y económicos dentro del nuevo orden internacional.