TÍTULO

LA COOPERACIÓN INTERNACIONAL COMO INSTRUMENTO MITIGADOR CONTRA CIBERATAQUES A LOS PAÍSES DESDE UNA VISIÓN GEOPOLÍTICA

AUTOR

Abraham Alcides Trillo Sarmiento

Esta edición electrónica ha sido realizada en 2024

Tutora	Dra. Dª. María Libia Arenal Lora
Institución	Universidad Internacional de Andalucía
Curso	*Máster de Formación Permanente en Estudios Contemporáneos sobre Geopolítica, Conflictos Armados y Cooperación Internacional (2022/23)*
©	Abraham Alcides Trillo Sarmiento
©	De esta edición: Universidad Internacional de Andalucía
Fecha documento	2023

“LA COOPERACIÓN INTERNACIONAL COMO INSTRUMENTO MITIGADOR CONTRA CIBERATAQUES A LOS PAÍSES DESDE UNA VISIÓN GEOPOLÍTICA”

Autor: Abraham Alcides Trillo-Sarmiento

Tutora: Dra. María Libia Arenal Lora

MASTER EN FORMACIÓN PERMANENTE EN ESTUDIOS CONTEMPORÁNEOS SOBRE GEOPOLÍTICA, CONFLICTOS ARMADOS Y COOPERACIÓN INTERNACIONAL

Curso Académico

2022 – 2023

Universidad Internacional de Andalucía, 2024

“LA COOPERACIÓN INTERNACIONAL COMO INSTRUMENTO MITIGADOR CONTRA CIBERATAQUES A LOS PAÍSES DESDE UNA VISIÓN GEOPOLÍTICA”

Autor: Abraham Alcides Trillo-Sarmiento

Tutora: Dra. María Libia Arenal Lora

MASTER EN FORMACIÓN PERMANENTE EN ESTUDIOS CONTEMPORÁNEOS SOBRE GEOPOLÍTICA, CONFLICTOS ARMADOS Y COOPERACIÓN INTERNACIONAL

Curso Académico: 2022 – 2023

Vo. Bo. Tutora:

Fdo. Profa. Dra. María Libia Arenal Lora (U. Sevilla)

ÍNDICE GENERAL

RESUMEN

El ciberespacio se ha transformado en la nueva dimensión para la producción de conflictos entre Estados que buscan incidir en la expansión de sus zonas de influencia en el mundo físico apoyados en las tecnologías de información y comunicación. La producción de ciberataques en contra de las infraestructuras de los países objetivos, denotan que no son improvisados sino responden a planificaciones de los países atacantes, quienes actúan de forma no lineal en conflictos híbridos, en los que el uso de la fuerza también se contempla. Para esto utilizan la denominada Zona Gris, en la que las reglas del conflicto armado y sus limitaciones no aplican, buscando de forma encubierta afectar la estabilidad del país objetivo. Las organizaciones internacionales han tenido que adaptarse y sobre todo reaccionar rápidamente a los cambios que trajeron las tecnologías, trabajando en base a la Cooperación Internacional para instrumentar soluciones, regulaciones y normas dentro del Derecho Internacional para mantener la paz en el Sistema Internacional. Los Estados están trabajando juntos y utilizan la Cooperación que les brinda sus organizaciones internacionales para fortalecer sus estructuras de ciberseguridad y hacer uso de sus capacidades conjuntas para reaccionar y mitigar ciberataques a sus propios Estados por parte de terceros. El presente trabajo hace una descripción del fenómeno, se analizan algunos casos de ciberataques relevantes, incluyendo el actual conflicto en Ucrania como en Israel, describiendo los conflictos desde una visión geopolítica y destacando el valor de la Cooperación Internacional como herramienta de mitigación ante los mismos.

Palabras claves: Ciberataques, Geopolítica y Cooperación Internacional

ABSTRACT

Cyberspace has become the new dimension for the production of conflicts between States that seek to influence the expansion of their zones of influence in the physical world supported by information and communication technologies. The production of cyberattacks against the infrastructure of the target countries denotes that they are not improvised but respond to planning by the attacking countries, who act in a non-linear manner in hybrid conflicts, in which the use of force is also contemplated. For this they use the so-called Gray Zone, in which the rules of armed conflict and its limitations do not apply, covertly seeking to affect the stability of the target country. International organizations have had to adapt and, above all, react quickly to the changes brought by technologies, working based on International Cooperation to implement solutions, regulations and standards within International Law to maintain peace in the International System. States are working together and using the Cooperation provided by their international organizations to strengthen their cybersecurity structures and make use of their joint capabilities to react and mitigate cyber-attacks on their own States by third parties. This work describes the phenomenon, analyzing some cases of relevant cyberattacks, including the current conflict in Ukraine and Israel, describing the conflicts from a geopolitical vision and highlighting the value of International Cooperation as a mitigation tool against them.

Keywords: Cyberattacks, Geopolitics and International Cooperation

Índice de Abreviaturas

BRICS+	**Brasil, Rusia, India, China, Sudáfrica y otros miembros**
CCDCOE	**Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN**
CCT	**Centro de las Naciones Unidas Contra el Terrorismo**
CDMB	**Junta de Gestión de Ciberdefensa**
CEE	**Comunidad Económica Europea**
CIRC o CERT	**Grupo de Respuesta de Incidentes Informáticos**
CSNU	**Consejo de Seguridad de las Naciones Unidas**
DDoS	**Ataque Distribuido de Denegación de Servicio**
DI	**Derecho Internacional**
DIH	**Derecho Internacional Humanitario**
DDHH	**Derechos Humanos**
EGCT	**Estrategia Global de las Naciones Unidas contra el Terrorismo**
EMPACT	**Plataforma multidisciplinar europea contra las amenazas delictivas**
GEC	**Grupo de Expertos Gubernamentales**
HW	**Hardware o componentes físicos informáticos**
IA	**Inteligencia artificial**
I+D+i	**Investigación más Desarrollo más innovación**
IoT	**Internet de las Cosas**
LCT	**Lucha Contra el Terrorismo**
NAC	**Consejo del Atlántico Norte de la OTAN**
NC3	**Junta de Consulta, Control y Comando de la OTAN**

NCIRC	**Capacidad de Respuesta de Incidentes Informáticos de la OTAN**
NCRS	**Sistema de respuesta a Crisis de la OTAN**
NNUU	**Naciones Unidas**
OCDE	**Organización de Cooperación y Desarrollo Económico**
OI	**Organizaciones Internacionales**
OLCT	**Oficina de Lucha contra el Terrorismo de Naciones Unidas**
ONU	**Organización de las Naciones Unidas**
OTAN	**Organización del Tratado del Atlántico Norte**
PCNT	**Programa de Ciberseguridad y Nuevas Tecnologías de NNUU**
PMCLCT	**Pacto Mundial de Coordinación de la Lucha contra el Terrorismo de las Naciones Unidas**
RRNN	**Recursos Naturales**
SAA o SAAL	**Sistema autónomo de armas o Sistema autónomo de armas letales**
SEAE	**Servicio Europeo de Acción Exterior**
SITCEN	**Sistemas de Comunicaciones de la OTAN**
SRI o SRI2	**Directiva sobre la seguridad de redes y sistemas de información o su segunda versión**
SW	**Software o conjunto de programas de informática**
TIC	**Tecnologías de Información o Comunicación**
UE	**Unión Europea**
UAV	**Vehículo Aéreo No Tripulado**
USA	**Estados Unidos de Norteamérica**
URSS	**Unión de Repúblicas Socialistas Soviéticas**

CAPITULO I

1. *INTRODUCCIÓN*

El Sistema Internacional funciona a partir de intereses de los diversos sujetos que participan en él, no circunscrito sólo a los Estados, organizaciones internacionales, compañías o empresas, sociedad civil u organizaciones no gubernamentales, también está influenciado por sus líderes y sobre todo el individuo de forma particular. Elementos que fueron considerados por el Prof. Kenneth Waltz en 1959, dando inicio a lo que se conoce como el Realismo Estructural.

Sin embargo, los avances tecnológicos insertados en las sociedades, tienen efecto para su desarrollo y sobre todo comportamiento, ya sea cambiando hábitos o brindándole funcionalidad buscando mejorar su productividad y la vida de las personas, pero como toda aportación en inicio pueden perseguir fines benéficos para la humanidad, pero esta última no siempre la utilizará para logar los mismos, distorsionando su uso y aprovechando las mismas para procurar obtener ventajas, siendo los Estados, que no es más que una organización humana, los que buscaran sacar ventaja para buscar potenciar su posición frente a los otros Estados en el Sistema Internacional del que forman parte.

La informática, que combina componentes físicos e intangibles conocidos como programas de computación, ha permitido que el hombre las utilice para procesar datos de manera mucho más ágil y productiva, en la que tanto su uso de forma restringida en un inicio y el desarrollo de componentes más pequeños, permitió que expanda su adquisición para que las personas accedan a estos con mayor facilidad, poseyendo hoy en día la mayoría de la población dispositivos portátiles en la mano con capacidades de computación que superan muchas veces a las primeras computadoras que ocupaban espacios físico enormes.

La suma de la conectividad a través de Internet o la red internacional de comunicación informática, no sólo representó el acortamiento de espacios físicos, pues se puede conocer diversas culturas con sólo realizar búsquedas en programas de navegación, acceder a información, datos, noticias, realizar transacciones de diversa naturaleza e interactuar de manera más fluida a través de las redes sociales con personas residiendo en diferentes ubicaciones del mundo.

La conectividad y los sistemas informáticos, unidos facilitan y optimizan costos para la producción, el crecimiento de la población humana, exige que se les brinde bienes y servicios de manera más rápida, que frente a la cantidad de datos que deben procesarse es imprescindible que se utilicen a diario, expandiendo sus aplicaciones no sólo para fines civiles, también estatales y militares. Denotando ventajas pero también desventajas, pues de estas últimas el propio hombre busca la forma de obtener beneficios usando las tecnologías para fines maléficos o distorsionados, esta vez actuando en el nuevo espacio denominado ciberespacio.

El poder que buscan los Estados, ya no sólo se circunscribe a los espacios físicos tradicionales, aire, tierra, mar o espacio extraterrestre, ahora también el dominio del ciberespacio, para lo cual buscan la forma de automatizar y combinar actuaciones tanto en esa dimensión como en la física, para provocar debilitar al enemigo y obtener supremacía sobre este aprovechando la interconectividad que le brindan los sistemas informáticos que siguen evolucionando.

Si a esto se le adiciona, la actuación de grupos irregulares tanto delictivos y dentro de estos de corte terrorista, cuyas actividades se denominan ciberterrorismo, se configura una mezcla altamente peligrosa, cuyo control es altamente complejo y establece escenarios asimétricos para las diferentes fuerzas de seguridad que deben enfrentarlos. Es decir, tiene una caracterización aproximada de su enemigo, pero no lo conocen y no lo pueden identificar plenamente para combatirlo eficientemente, constituyendo verdaderos desafíos para los Estados y sus sociedades.

En el presente trabajo, ante la realidad descrita, se pretende presentar una descripción sobre las acciones que están realizando los Estados a través de la Cooperación Internacional y sus Organizaciones Internacionales de las que forman parte, en temas circunscritos al ciberespacio, ciberataques y ciberseguridad, en las que el Derecho Internacional busca dar respuesta para garantizar su utilización de manera lo menos restringida posible, pero al mismo tiempo responsable.

Para el Derecho Internacional Humanitario, en caso de conflictos el desafío se circunscribe a la aplicación de sus principios y las restricciones o limites que deben cumplir los Estados en casos de combate o las denominadas ciberguerras, efectos que no son solamente virtuales, son fundamentalmente físicos y repercuten contra las sociedades. Incidiendo en la responsabilidad que deben tener y por la cual deben responder los actores, principalmente los Estados.

La descripción que se realiza en el trabajo, procura insertar un enfoque en clave geopolítica apoyada en el realismo estructural y busca brindar una pequeña base para la aportación a trabajos más profundos y especializados sobre diferentes aristas que posee este campo y que serán de relevancia tanto para el Derecho Internacional en todas sus vertientes, sobre todo el de los Derechos Humanos y el poder que lograran los países, acorde a sus capacidades que demuestren en un Sistema Internacional cada vez más polarizado, conflictivo y por ende caótico.

Para esto, el trabajo se dividió en tres partes, la primera enfocada principalmente a la descripción de la situación del fenómeno en estudio, significados relevantes, la descripción e importancia de las Organizaciones Internacionales, la Cooperación Internacional que deriva de estas y la descripción general sucinta del significado de ciberataques y sus variedades. El segundo capítulo, enfocado a la descripción de las acciones que están realizando las Organizaciones Internacionales más relevantes en el campo de estudio, la descripción de algunos ejemplos reales y sus implicancias tanto geopolíticas como para la Cooperación Internacional. Concluyendo en el capítulo tercero sobre lo observado en el trabajo.

2. *JUSTIFICACIÓN*

La necesidad del presente trabajo se circunscribe a observar la forma como el Sistema Internacional está reaccionando ante los avances informáticos enfocados en las tecnologías de información y comunicación, cuando estos son utilizados para interactuar en el nuevo espacio de influencia denominado ciberespacio, caracterizado no sólo por su virtualidad, también por la necesaria e importante conectividad que requiere para su existencia y por ende capacidad para que los que interactúan dentro de él puedan hacerlo, incluyendo a los propios Estados.

Dado que dentro los usuarios del ciberespacio se hallan actores con disimiles intereses, intervienen los sujetos que tienen vínculos con el terrorismo, la delincuencia y violencia extendiendo sus actividades al mundo virtual para difundir sus mensajes, captar adeptos a sus movimientos y reclutarlos para que participen activamente en él, financiar y realizar operaciones económicas que los sustenten, hasta interactuar atacando a sus cibervictimas para buscar generar

daño a sistemas informáticos establecidos como objetivos o capturar su control para diferentes fines. Afectando su seguridad, integridad y utilización; lo que implica hablar de ciberseguridad y ciberdefensa.

Cuando las capacidades de respuesta ante ataques injustos en el ciberespacio buscan afectar la integridad de las redes informáticas y sus infraestructuras criticas conectadas a los primeros, las victimas reaccionan y si estas tienen capacidades potentes, siendo además Estados u organizaciones establecidas por estos, se producen las denominadas ciberguerras, en la que se busca afectar al enemigo y sus capacidades, para destruirlo o apoderarse de los mismos. En la que el Derecho Internacional y el Derecho Internacional Humanitario deben adaptar sus reglas y normas para establecer límites, responsabilidades y condiciones para evitar la destrucción total entre los intervinientes, que siempre buscaran la suma cero a su favor en contra de sus enemigos.

Los conflictos armados, han trascendido al ciberespacio, sus repercusiones se extienden de la virtualidad a la realidad física, la geopolítica es más valiosa que nunca al insertar elementos de análisis que permitan comprender de mejor forma lo que acontece en la actualidad y la necesidad del fortalecimiento de la Cooperación Internacional que ayude no sólo a controlar lo que acontece en el ciberespacio, sino la construcción de estamentos que obliguen a los Estados a actuar con la debida diligencia en sus territorios cuando actores presentes en el mismo actúan en el ciberespacio, constituyendo a los primeros en garantes del respeto al orden que debe imperar en el Sistema Internacional para mantener el statu quo o como mínimo el respeto, en busca del mantenimiento de la paz y el desarrollo de la humanidad.

Por lo que este trabajo, es una aproximación que destaca la labor de las Organizaciones Internacionales, los efectos geopolíticos que se generan en casos concretos que ejemplifican la necesidad de control de lo que sucede en el ciberespacio y la importancia que conlleva la Cooperación Internacional como herramienta mitigadora de efectos negativos provocados por los ciberataques a los países y sus recursos interconectados en el ciberespacio, que repercutirán en sus capacidades o fuentes de poder en el Sistema internacional y el equilibrio que puedan aportar a este.

3. *OBJETIVOS*

3.1 OBJETIVO GENERAL

El objetivo del presente trabajo es el de describir los ciberataques a los países desde una visión geopolítica y destacar la importancia de la Cooperación Internacional como instrumento de mitigación contra los primeros en base a sus Organizaciones Internacionales.

3.2 OBJETIVOS ESPECÍFICOS

1. Describir las acciones asumidas por Organizaciones Internacionales sobre el ciberespacio, ciberseguridad y/o ciberataques.
2. Describir casos relevantes de ciberataques producidos y su implicancia geopolítica.
3. Establecer el rol de la Cooperación Internacional frente a los ciberataques e implicancias para la ciberseguridad y el uso del ciberespacio.

4. *FUENTES Y METODOLOGÍA*

Las fuentes recurridas en el presente trabajo son secundarias, principalmente, a través de documentos publicados en formato digital, registros en páginas web, notas de prensa digital, videos especializados en plataformas como youtube, de manera de lograr configurar descripción del fenómeno en estudio acorde a lo que acontece en la realidad, con énfasis en clave geopolítica.

El diseño metodológico parte del enfoque cualitativo que se aplica por las características de investigación seleccionada, con carácter jurídico y geopolítico de nivel explicativo acorde al enfoque elegido, sistematizando la documentación colectada. Los primeros dos capítulos serán del tipo exploratorio, descriptivo y explicativo; mientras que el ultimo será descriptivo, explicativo y propositivo. La técnica que se utilizará será de observación y análisis documental, con instrumentos apoyados en registros y fichas textuales.

En base al diseño seleccionado, adicionalmente se establece que el primer capítulo será del tipo longitudinal, transversal, retrospectivo, descriptivo, documental, exploratorio y explicativo. El corte transversal se hará desde 2002 para los análisis y se harán referencias a siglos pasados en las descripciones históricas de los países analizados, incidiendo en la última década desde 2012 principalmente. El capítulo segundo, será documental, exploratorio, explicativo, con uso de síntesis. El tercer capítulo, será cualitativo, descriptivo, propositivo.

5. *ESTADO DE LA CUESTIÓN*

La Cooperación Internacional para que se articule efectivamente debe responder primordialmente a organizaciones que agrupen a sujetos reconocidos por el Derecho Internacional, denominados Estados. Estos últimos agremiados acorde a sus intereses o expectativas en correlación a las políticas que posean, las circunstancias que los rodeen o atraviesen, la necesidad de expansión que requieran, el fortalecimiento de sus relaciones con sus pares, la necesidad de actuación y negociación para obtener ciertos objetivos trazados, la preservación de su territorio y/o población y/o sistema político y/o económico, etc.

Las organizaciones internacionales (OI), poseen características y rasgos primordiales, que deben ser cumplidos por los Estados para poder constituirlas, al margen que deben derivar de instrumentos del Derecho Internacional para su conformación y reconocimiento con efectos jurídicos. Debiendo, analizar las OI, de forma previa para lograr, derivada de sus partes, entender el crucial rol que realiza la Cooperación Internacional como mecanismo o instrumento al que acuden los Estados para dar respuesta o solucionar alguna demanda o necesidad que poseen en su desarrollo.

Convirtiéndose, en esencia en uno de los principales fines para la constitución de una OI, pues los Estados no pueden aislarse ni convertirse en parias en un mundo globalizado, sometido a avances tecnológicos cada vez más disruptivos y paralelamente frente a una humanidad más conflictiva, siendo parte del desarrollo de las sociedades, que son las que al fin y al cabo se organizan para establecer su Estado, y a través de este lograr su OI que las represente con la robustez de la participación organizada y no asilada ante el mundo.

Por otro lado, los espacios de interrelación de las personas y sus propios Estados, hoy en día ya no sólo se circunscriben a los que hasta hace algunas décadas atrás, fueron las regulares o conocidas, como el terrestre, aéreo o marítimo, también el propio espacio extraterrestre

consecuencia de la carrera entre dos superpotencias en un mundo bipolar que subsistió hasta finales de 1991, con la desaparición de la antigua URSS.

Incluyéndose, desde algunas décadas atrás, de manera irremediable al espacio virtual o mejor conocido como ciberespacio, en el que de manera dinámica se actúa entre bits de computadora que viajan de un punto a otro en segundos llevando y trayendo datos, cuyas representaciones variaran acorde a lo que se requiera (texto, videos, imágenes, voz, documentos, etc.).

Espacio virtual, que es lugar donde ya no solo se interactúa para fines pacíficos, sino que los males de la propia humanidad y sus organizaciones se han transportado al mismo, generando ciberdelincuencia, ciberacoso, ciberataques, ciberguerras y la necesidad de desarrollas medidas de ciberseguridad, si el hombre quiere subsistir en la actual sociedad.

La tecnología, ha insertado la automatización que se viene utilizando desde hace ya muchos siglos atrás, desde el invento de la palanca o la rueda, para facilidad del hombre, quien no ha cejado en I+D+i para obtener mejores herramientas y maquinas a su favor y labor; siendo la cibernética uno de sus resultados.

Luego de la Segunda Guerra Mundial, la humanidad observó el repunte de la electrónica, cambiando diodos por transistores, para luego lograr su miniaturización derivado en chips y hoy en día ya devenidos en nanochips. Con aplicaciones tan diversas en el ámbito de las telecomunicaciones, salud, transporte, energía, robótica, sistemas de defensa y ataque militar y muchas más.

Sin embargo, el hombre para interoperar con los dispositivos debió desarrollar lenguajes de comunicación con las maquinas, a través de programas de computación conocidos como Software (SW) y para diferenciar los dispositivos físicos estos se conocen como Hardware (HW), formando el sistema cibernético o informático sobre el que hoy se apoyan la mayoría de infraestructuras críticas que poseen los Estados y las personas, sistemas cada vez más automatizados con ayuda de Inteligencia Artificial (IA) y desarrollo de computadoras cuánticas.

Si a ese sistema se le suma interconectividad a nivel global, a través de lo que hoy conocemos como la red de redes o Internet, resulta en accesos a sistemas cibernéticos de forma remota, sin la necesidad de estar en el lugar para interactuar con ellos y entre ellos.

Los efectos, del mal uso que la tecnología está generando conflictos, repercuten en el Sistema Internacional, que de por si es anárquico, caracterizado por Herz, Waltz y Gilpin, en la denominada escuela del realismo estructural, que provoca efectos descritos por el realismo defensivo y el realismo ofensivo según el caso que se trate, con visiones que procuran explicar lo que acontece en la realidad y de las cuales el presente trabajo tratara de apoyarse para su desarrollo y análisis.

5.1 CARACTERIZACIÓN Y CLASIFICACIÓN GENERAL DE LAS ORGANIZACIONES INTERNACIONALES

La referencia a Organizaciones Internacionales (OI) en el presente trabajo, debe entenderse a las del tipo compuesto por Estados interrelacionados y organizados, cuya estructura obedecerá a sus intereses y la generación de vínculos entre ellos, apoyados en actividades de cooperación para el logro de objetivos comunes.

Para autores como Virally (Calduch, 1991, págs. 1-3), nombrado por Calduch[1], reciben el denominativo de "Organizaciones Internacionales Gubernamentales", cuya definición de estas se orienta a destacar la parte asociativa de los Estados que contaran con un ente o aparato permanente compuesto por diferentes órganos en su estructura.

Dicha definición es relevante, pues permite de forma sencilla y clara diferenciar a dichas asociaciones u organizaciones de carácter estatal frente a las de otro tipo, últimos cuyos actores obedecerán a diversos orígenes con o sin aval estatal y objetivos diversos, que para el campo del análisis geopolítico y del conflicto podrán ser o no relevantes según su influencia y peso en temas de estudio de interés.

Para Calduch, apoyado en la caracterización realizada por Virally (Calduch, 1991, pág. 2), dichas organizaciones estatales o intergubernamentales, obedecen a cinco características que poseen y las diferencian de otras, siendo las siguientes:

i. **Interestatal.** Característica que describe la composición de la organización por parte de diferentes Estados, representado a través de sus respectivos gobiernos generalmente. Si bien la presencia de los Estados potencia la organización, esta característica NO IMPLICA que se constituya como tal sólo por esto. Debiendo observar que los intereses de cada uno de ellos primará, no siendo compatibles entre sus pares necesariamente, ni siquiera con los de la organización y viceversa en ciertos temas. El hecho de estar formada por Estados, le brinda el carácter internacional y relevante frente a organizaciones privadas o civiles.

ii. **Voluntarista.** Característica que denota la decisión volitiva de participación de los Estados en la OI, cuyo rasgo al no ser exclusiva de este tipo de agrupaciones, es relevante pues denota compromiso asumido por los Estados para integrar o no la misma. La voluntariedad genera dos consecuencias relevantes para la comunidad internacional, por un lado se generan efectos del tipo jurídico sobre la organización y miembros que la componen (Estados) y por el otro fortalece la COOPERACIÓN entre estos, que es de tipo internacional.

iii. **Órganos permanentes.** Característica que denota estabilidad y permanencia de las organizaciones internacionales en el tiempo, lo que le permite crear organismos en su interior o entidades, fortalecer la COOPERACIÓN entre sus Estados miembros o a favor de terceros, establecer y ejecutar decisiones colegiadas, objetivos, trazar metas, establecer planes, optimizar y organizar sus diversos recursos (humanos, económicos, jurídicos, etc.).

    Razón por la que las organizaciones, al ser estables, se diferencian de organizaciones temporales o coyunturales o para fines u objetivos específicos, muchas veces denominadas Movimientos o Conferencias de países o bloques regionales, que buscan

[1] *Calduch, R. (1991). Relaciones Internacionales. Capítulo 9. Edit. Ediciones Ciencias Sociales. Madrid, España. Página 1. El autor desarrolla la descripción de las organizaciones internacionales gubernamentales, apoyado en los criterios de Virally, razón por la que indica: "Partiendo de esta consideración preliminar podemos definir a las organizaciones internacionales gubernamentales, según VIRALLY, como: «Una asociación de estados, establecida por un acuerdo entre sus miembros y dotada de un aparato permanente de órganos, encargado de perseguir la realización de objetivos de interés común por medio de una cooperación entre ellos»". Guía utilizada también en el presente trabajo y utilizado como guía en base criterios expuestos en la referida obra y autor.*

generar cooperación entre ellas que no perdura en el tiempo o directamente no se produce. Debiendo observarse a los BRICS+, por ejemplo.

iv. **Autonomía decisional y funcional.** Característica que inserta el elemento diferenciador entre sus Estados miembros, pues de no poseerla se entenderían a las organizaciones como extensiones de los mismos. Si bien la OI se crea a partir de intereses y objetivos comunes, esta debe poseer relativa autonomía para adoptar decisiones en base a sus competencias recibidas de los propios Estados.

El elemento diferenciador, es que la OI como tal goza de reconocimiento del Derecho Internacional Público de forma independiente al de sus participantes, con capacidades jurídicas independientes, pero no por esto totalmente autónoma de los Estados que la componen. Pues tendrán influencia en mayor o menor grado de sus propios Estados participantes y viceversa, según sea el caso.

Las decisiones que adopte la OI, responderá a sus estatutos y normas internas, acorde a lo establecido por los propios Estados miembros, tipo de sistema de representación adoptado, votación, organización y competencias.

Si bien su funcionamiento dependerá de los Estados miembros, responderá a su propia estructura y organización interna, cuyo funcionamiento y operación será acorde a las mismas. Por lo que sus funcionarios actuaran en representación de la organización bajo tutela de sus Estados, con cierto grado de independencia también normada en su conformación.

Dependiendo la OI de la que se trate, será innegable observar que actuaran priorizando a algún Estado o grupo de estos, con mayor influencia en sus respectivos senos, frente al resto de sus miembros.

v. **COOPERACIÓN ENTRE ESTADOS.** Esta característica es factor común en las diferentes organizaciones internacionales, pues más allá de los objetos constitutivos por los que hayan emergido, es relevante que la cooperación entre sus Estados miembros se fortalezca producto de su integración.

En base al trabajo de Calduch (Calduch, 1991, pág. 3), es importante diferenciar la cooperación entre Estados miembros, sea interna o externa, de la integración o cooperación integradora, que se traduce en una forma particular de cooperación internacional.

La integración o "cooperación integradora" busca a la larga la conformación, según Calduch, de un ente del tipo supraestatal o supranacional que impacta en la soberanía de sus Estados miembros; mientras que en la "COOPERACIÓN INTERNACIONAL" se enfoca en respetar la soberanía de los Estados, fortalecerla y respetar su incidencia entre ellas evitando la conformación de entes supra entre sus Estados miembros.

Siguiendo al mismo autor Calduch, que se apoya en Virally (Calduch, 1991, págs. 4-6), este introduce además criterios de clasificación a los que responden dichos organismos, apoyándose en tres: espacial, funcional y jurídica.

a) **Espacial.** La clasificación desde el punto de vista espacial, responde a la ubicación geográfica del que provienen sus miembros de la OI. Están, también, las organizaciones internacionales que se agrupan a partir de ciertas características geográficas y/o geoestratégicas y/o económicas u otras como la OTAN cuya diversidad de procedencia de sus miembros las fortalece, siempre y cuando cumplan criterios de membresía a la que

respondan en la fundación de las respectivas organizaciones internacionales o su posterior integración.

b) Funcional. Su clasificación responde a dos vertientes, la primera del tipo político o general y la segunda del tipo técnico o especifico. Las primeras al ser del tipo general su ámbito de actuación o funcionamiento implica diversidad de áreas de interés, lo que fortalece la política de cooperación que poseen entre sus Estados miembros y a favor de terceros de ser necesario, respondiendo a las necesidades que surjan durante su existencia acorde a los intereses de sus participantes y realidades circundantes.

Las organizaciones del tipo técnico o especifico, responden a campos de especialidad en la que actúan, sea del tipo económico, comercial, salud, laboral, etc. Lo que brinda respuestas puntuales a problemas que atingen a sus Estados miembros.

c) **Jurídica (competencia y naturaleza).** Características a partir de la competencia jurídica que poseen las organizaciones internacionales de supremacía de sus ordenamientos jurídicos sobre la de sus Estados miembros, respondiendo a la esfera supra, conocidos precisamente como organizaciones supranacionales, siendo quizás el mejor exponente la Comunidad Económica de Europa (CEE), en base al Tratado de Roma de 1957, que luego de la formación de la Unión Europea en 1993 y su integración a esta, se llamó Comunidad Europea.

Por el otro lado, se encuentran las organizaciones con normas jurídicas que carecen de competencia para ser impuestas sobre el ordenamiento jurídico de los respectivos Estados, respondiendo al esquema de organizaciones internacionales entre Estados, siendo ejemplos de ese tipo el Fondo Monetario Internacional (FMI) o la Organización del Tratado del Atlántico Norte (OTAN), entre otras más.

Para Virally (Calduch, 1991, pág. 5), según Calduch, las organizaciones internacionales se pueden agrupar en dos, en función de su génesis, encontrándose las organizaciones de cooperación o agregación y las organizaciones de integración.

Las primeras, las de Cooperación, buscaran la armonía y el fortalecimiento de lazos de solidaridad, a través de la ejecución de programas, proyectos de ayuda o cooperación a favor de países que los requieran, utilizando fondos o aportes de sus miembros o recursos propios. Este tipo de organizaciones son más frecuentes.

Los segundos, los de integración como su nombre lo refiere buscan, a partir de la realización de diversas actuaciones, lograr alcanzar competencias en determinadas materias sobre los Estados miembros, buscando como fin la integración de estos dentro del área de influencia para la cual fue creada la organización, de manera tal de alcanzar tuición sobre el Estado, buscando su incorporación o fusión con el resto de Estados, de forma tal que se sustituya las competencias nacionales por las de la organización de integración. Este tipo de organizaciones son menos frecuentes.

La integración de Estados, será parte de la dinámica que buscan agruparlos en función de intereses de diversa naturaleza, adoleciendo de diversos factores a confrontar tales como el tipo de economía que posee cada Estado miembro, su soberanía, recursos naturales y geoestratégicos, soberanía, arraigo cultural, posición política imperante entre su población, ideología, religión, idiosincrasia, densidad poblacional, nivel de formación académica, sistemas de vivienda y salud, otros.

En correspondencia a lo descrito previamente, también deberán observarse las clasificaciones que inserta Virally (Calduch, 1991, pág. 6), entre organizaciones mundiales y las parciales, que encuentra intersecciones con las clasificaciones descritas. Las primeras, mundiales, son del tipo integradoras – no confundir con la de integración – buscando la incorporación de todos los Estados, promoviendo la cooperación entre sus miembros, así como no miembros.

Las del tipo parcial, a contrario sensu, buscan la exclusividad, agrupando a sus Estados miembros a partir de características o intereses específicas, razón por la que no buscan la incorporación de cualquier Estado, sino de aquellos que cumplan con criterios de admisibilidad previamente estatuidos en la conformación de este tipo de OI.

Otro criterio propuesto por Virally (Calduch, 1991, pág. 7), diferencia las organizaciones internacionales entre las de alcance general y las sectoriales, que coincide con descripciones previas caracterizadas por sus funciones que desarrolla. Arribando al criterio que observa la relación entre la cooperación desplegada por la OI y las que se generan con sus miembros a partir de la misma.

Derivado del último criterio, se diferencian las organizaciones internacionales del tipo normativo y las del tipo operativo, también desarrollados por Calduch sobre la clasificación de Virally (Calduch, 1991, pág. 7). Permitiendo entender que el aporte de las del tipo normativo son precisamente proponer códigos, desarrollar normas, actualizarlas, con el objetivo de que el Derecho Internacional se desarrolle, fortalezca y logre a través de la cooperación internacional encontrar consensos apoyados en normativas del tipo jurídico que regule el comportamiento de los actores internacionales, cuyo fin será el respeto, aplicación de mecanismos de solución de conflictos, equilibrio y en definitiva la paz que deberá primar entre sus miembros. Todo lo explicado, permite que dichas organizaciones posean autonomía normativa del tipo jurídico, principalmente.

Las del tipo operativo, son organizaciones gestoras y actoras en el ámbito internacional, realizando actividades de forma directa a partir de recursos propios o proporcionados por los Estados miembros a la cual pertenecen. Lo que les permite poseer autonomía funcional y el manejo de sus diversos recursos que posee.

A modo de resumen sobre la clasificación adicional de Virally de las organizaciones internacionales, se agrupan en: 1) las de integración y agregación; 2) las de alcance mundial y parcial; 3) las generales y sectoriales y 4) las del tipo normativas y operativas.

5.1.1 CONSTITUCIÓN Y CONFORMACIÓN GENERAL DE LAS ORGANIZACIONES INTERNACIONALES

El nacimiento de una OI es a través de Tratados Internacionales establecido entre Estados fundadores firmantes del mismo, instrumento que deberá ser aprobado y ratificado por cada uno de sus miembros acorde a sus propias legislaciones internas en sus respectivos países.

Al constituirse acorde al derecho consuetudinario internacional, los Tratados signados por sus miembros establecen derechos y obligaciones entre ellos, que en términos del derecho internacional se habla de que obligan entre sus pares y sobre terceros.

El Tratado o instrumento internacional más relevante del siglo pasado lo constituye, con muy alta probabilidad, la Carta de las Naciones Unidas de 1945, que se fundó en principios de igualdad soberana de los Estados, prohibición del uso de la fuerza en las relaciones internacionales (RRII) y otros principios de orden internacional aceptados.

Derivado de dicho instrumento, surgió el Estatuto de la Corte Internacional de Justicia (CIJ), que al margen de regular el funcionamiento de dicho organismo, forma parte integrante de la Carta de las Naciones Unidas (Carta NNUU), establecida en el Art. 92 del Capítulo XIV de la misma.

En líneas generales, los Tratados constitutivos al poseer especial solemnidad en su conformación, reciben la denominación de Cartas, constituyendo instrumentos de orden internacional relevante y vinculado a la conformación precisamente de organizaciones internacionales estatales.

Es así que a modo de ejemplo[2], se establecieron entes internacionales tales como la Organización de Estados Americanos de 1948, a través de Carta que lleva su nombre. Siguiendo a Calduch (Calduch, 1991, pág. 9), la conformación de OI se realiza ordinariamente a través de instrumentos o normas internacionales denominados Tratados o Cartas, lo que supone la vía ordinaria para la constitución, con las respectivas firmas y ratificaciones por parte de los Estados miembros.

Surgiendo alternativamente, la vía extraordinaria para la formación de un OI, como las Conferencias Internacionales con la participación de Estados miembros de la OI, que instruyen mandatos de conformación de una nueva OI vinculada directa o indirectamente a la OI matriz.

La tercera vía, que también es extraordinaria es a través de Resolución de constitución o transformación de una OI existente. Ejemplo, es la Organización Europea de Cooperación Económica (OECE), se transformó mediante Tratado firmado de 1960 en la Organización de Cooperación y Desarrollo Económico (OCDE)[3].

Obsérvese que al margen del camino de formación o constitución de la OI, un elemento que deberá relevarse y es factor común no sólo en su nacimiento, también en su estructura, caracterizaciones, agrupaciones, tipologías y descripciones que se realizaron en esta parte del trabajo, es la COOPERACIÓN INTERNACIONAL o INTERESTATAL existente o promovida entre sus diferentes miembros; ya sea a través de la misma OI u organismos derivados de esta, que de forma dependiente o independiente actuaran a favor de los requirentes, buscando brindar soluciones a necesidades o problemas que se presenten acorde a las realidades imperantes.

En el presente caso, dada la evolución tecnológica en la que está inmersa la humanidad, las diversas áreas de preocupación de organizaciones internacionales mundiales, sectoriales, parciales, especializadas, normativas, operativas, generales, de integración o cooperación; son sin duda los espacios virtuales o Ciberespacio, enfocando atención a la Ciberseguridad, debiendo atender diversas amenazas y ataques que se presentan denominados Ciberataques, con el objetivo de mitigar o procurar dentro de fines de mantenimiento de la paz, evitar la degeneración en

[2] Calduch, R. (1991). Relaciones Internacionales. Capítulo 9. Edit. Ediciones Ciencias Sociales. Madrid, España.

[3] Ídem 2.

posibles Ciberguerras, en la que ya no sólo los Estados son protagonistas sino pluralidad de actores, que confluyen a acentuar la multipolaridad de conflictos que van surgiendo.

La importancia de atender problemas que surgen en estos nuevos espacios son precisamente la dependencia cada vez más alta a la conectividad de diversos medios de comunicación e información, procesamiento y automatización de tareas, que son utilizados diariamente no sólo por la OI, sus funcionarios o sus Estados miembros, sino por casi toda la humanidad.

Cuando surgen ciberataques en contra de estructuras y sistemas automatizados que manejan sectores críticos de la sociedad, cuya organización superior es el Estado, generan que sus OI trabajen en dar solución a estos problemas en base a la Cooperación Internacional establecida.

5.2 LA CIBERGUERRA Y LOS CIBERATAQUES

En el Sistema Internacional, se hablan de cuatro o cinco dimensiones o espacios en el que interactúa el hombre, sus sociedades y principalmente sus Estados, previamente mencionado.

El ciberespacio, de interés para el presente trabajo, es la dimensión o espacio que posee disimiles características, la principal es su virtualidad e "inmaterialidad", vale decir que no responden a un espacio físico derivado de la naturaleza sino a la establecida o creada por el hombre, quien se conecta a través de Internet con ayuda de dispositivos físicos del tipo informático, interactuando para enviar y/o recibir datos con ayuda de programas que pueden también actuar de forma automatizada para facilitar la interacción entre máquina-hombre o máquina-maquina.

No poseyendo fronteras y por ende las derivadas limitaciones de desplazamiento de las personas físicas entre Estados, en la que la identidad y la verificación sobre todo de esa identidad del operador o navegante en el ciberespacio es compleja, permitiendo se genere el anonimato con o sin herramientas propias del sistema informático utilizado.

Descrito de esa manera, aparenta representar tierra de nadie y en este caso, espacio de nadie, donde todos acuden pero nadie tiene el derecho propietario sobre él. Sin embargo, la Cooperación Internacional ha interactuado para establecer reglas y limites sobre su uso, buscando precisamente precautelar la libertad, el derecho de uso irrestricto y sobre todo la seguridad de quienes participan en el ciberespacio.

Pero para quienes actúan sin reglas o las inobservan, aprovechan las limitaciones y ventajas que brindan las tecnologías, no hablando de simples individuos, también de los propios Estados que aprovechando la pluralidad de internautas y los recursos que manejan, utilizan el ciberespacio para sus fines y objetivos estratégicos. Por lo que no existe una relación univoca o lineal entre actor, acción y resultado o viceversa, sino abanicos de posibilidades y vinculaciones.

En un ensayo de 2012 sobre la ciberguerra y sus generaciones, el autor (Gaitán, 2012, págs. 1 - 14)[4], establece la interacción del hombre, las computadoras y el ciberespacio utilizados para realizar ataques en contra de los enemigos en los conflictos regulares.

[4] *Al momento de la publicación del ensayo en 2012, ya se habían producido los ciberataques a Estonia en 2007, Georgia en 2008, Irán en 2010 y la denominada Operación Titán Rain de China en 2002. Los casos fueron y siguen siendo referentes en diferentes trabajos, análisis y decisiones que toman las organizaciones y Estados, para fijar sus propias políticas de ciberseguridad y prevenir ciberataques. La relevancia de los mismos como ejemplos prácticos de posibles escenarios a confrontar en caso de ataques combinados o limitados a su soberanía en diversos espacios de dominio.*

Dicho autor, además, establece que el control con ayuda de la cibernética, genera tres elementos a subordinar a favor del atacante: a) el factor psicológico; b) la infraestructura crítica y c) armamento del enemigo.

El control sobre el factor psicológico, en base a lo expuesto, se desarrolla apoyado en Operaciones de Información (Gaitán, 2012, pág. 7), dentro de la Guerra de Información, en la que los tomadores de decisión ayudados por las tecnologías, procesaron datos y la emisión de directrices en campos de batalla.

Adicionalmente, las Operaciones de Información, se descomponen en operaciones: psicológicas, de engaño, seguridad, computadoras en red y electromagnéticas (Gaitán, 2012). La primera enfocada a generar sensaciones en la población o tropas enemigas, apoyados en herramientas psicológicas o de manipulación, complementadas con las de engaño. Buscando que el enemigo asuma decisiones erróneas a partir de información manipulada. Por otro lado, generar bloqueo o negación de acceso a la información, desarticulando la coordinación del enemigo, afectar la toma de decisiones y generar afectación psicológica ante el desconocimiento de lo que acontece realmente y la incertidumbre de lo debiera hacerse.

También, dentro la descripción, se habla de crear una realidad virtual (Gaitán, 2012, pág. 9), con ayuda de la manipulación de las informaciones usando tecnologías, pues crear o distorsionar imágenes o situaciones, para luego expandir información al enemigo en base a criterios manipulados, en redes y medios de comunicación masiva, "fake news", buscan generar desestabilidad en los gobiernos de los Estados a partir de reacciones de las poblaciones y sus propios funcionarios.

Adicionalmente, también dentro del control de factor psicológico, se encuentra el de brindar seguridad a las propias tropas de los atacantes, pues al utilizar tecnologías que les permitan acceder a datos precisos para flanquear y atacar con mayor efectividad al enemigo, brinda seguridad y confianza en el despliegue de las acciones realizadas, fortaleciendo no sólo su posición también la disposición de sus efectivos a continuar avanzando para obtener sus objetivos.

El control de la Infraestructura Crítica, para Gaitán se refiere (Gaitán, 2012, pág. 11) a la afectación al Centro de Gravedad, que en base al criterio de John Warden, también nombrado por él, estaría compuesto en caso de guerras, por cinco anillos o estratos, que van desde las fuerzas militares en combate, población, sistemas esenciales, liderazgo e infraestructura crítica.

Que hoy en día son afectadas transversalmente por las tecnologías de información y comunicación (TIC), existiendo antecedentes de ciberataques relevantes a nivel global registrados desde 2002, tal como lo menciona el autor (Gaitán, 2012, pág. 12), al describir los casos: Operación Titán Rain en el que China supuestamente hackeo infraestructuras públicas y privadas de USA; en 2007 el caso Estonia en el que supuestamente Rusia realizó ciberataques a infraestructuras gubernamentales y privadas durante tres semanas; en 2008 el caso Georgia en el que Rusia supuestamente tomo control de los sistemas de defensa e información de ese país antes de invadirlo; en 2010 el caso Stuxnet en el que supuestamente Israel afecto el desarrollo de armas nucleares llevadas adelante por Irán.

En ninguno de los casos se pudo establecer la autoría especifica de los hechos suscitados, se obtuvieron elementos de convicción que referían al país de origen o del cual se sospechaba provinieron los ataques, pero no la identificación puntual del o los autores, que al igual que

menciona Gaitán, se considera que la trazabilidad fue eliminada o distorsionada en base a las mismas herramientas cibernéticas.

La Tercera Generación, dirigida al control del armamento contrario, se concentra en la utilización de TIC en la intervención de los sistemas del enemigo y la captura del mando de los sistemas que posee a favor del ciberatacante.

Los ejemplos expuestos por Gaitán, son casos relevantes suscitados por Vehículos No Tripulados o UAV por sus siglas en inglés, que fueron capturados por Irán cuando naves de esas características pertenecientes a las fuerzas militares norteamericanas e israelitas, fueron obligadas a aterrizar en suelo iraní.

La práctica de ingeniería inversa y las limitaciones de ese país, involucraron a China y Rusia para que los tres Estados en conjunto se hagan con la tecnología de esos países, controlados remotamente a través de las TIC y los puedan replicar. Aplicando Cooperación Internacional para este caso.

Obsérvese, que a 2023 Irán cuenta con innovaciones en diferentes modelos de UAV que no sólo está utilizando en la conflagración Rusia – Ucrania, a favor de Rusia es claro, también ofertándolos comercialmente en el mercado mundial, en países aliados a su régimen.

Los vehículos no tripulados o remotos, hoy en día han proliferado en el área militar, abarcando usos para los diferentes espacios tradicionales, terrestres, aéreos y marítimos, lo que denota que las TIC y su ciberseguridad, son relevantes para la protección y utilización de dichos sistemas en conflagraciones, exploraciones, vigilancia, mitigaciones y asistencia a las tropas y fuerzas militares de los usuarios.

En el mismo sentido, Marín Martínez (Marin, 2023, págs. 71 - 86), desarrolló un trabajo sobre la relación entre armas autónomas letales y el Derecho Internacional Humanitario (DIH) en el conflicto Rusia - Ucrania, destacando el uso de control de dichas armas en base a IA y las limitaciones de la aplicación o uso por otro lado del Estatuto de Roma de 2016 por ambos Estados, en el que Ucrania no lo firmo y Rusia retiro su firma.

Algo que destaca, al inicio del trabajo, es parte del discurso de V. Putin el 21 de diciembre de 2017 reflejado en él, que describe la visión del líder ruso al afirmar que las armas más efectivas son las que operan automáticamente y de manera rápida, además de que en palabras del autor (Marin, 2023, pág. 73), Rusia pretende convertirse en líder en IA, aplicarla a la industria militar y dominar dicha tecnología para gobernar el mundo.

La realidad del actual Sistema Internacional, induce a observar que dicho criterio no es único del líder ruso, pues potencias como China, USA, Reino Unido, Australia, Canadá, Japón, Alemania; India, Emiratos Árabes Unidos, Irán, Corea del Norte o cualquier otro país que se lo proponga podría incluirse en la lista por alcanzar dichos objetivos.

Lo cierto es que la automatización cada vez es más relevante en diversos sectores de la vida humana, en el campo militar más aún, pues lo que se busca es maximizar recursos, conseguir objetivos y minimizar perdidas, buscando incrementar capacidades en todos los espacios de operación.

Para Marín, la preocupación es la liberación del uso de la fuerza de forma automática y su deshumanización en la guerra, cuyas implicancias obligan a plantear nuevas posturas sobre la eficacia del Derecho Internacional (DI) y específicamente del DIH.

Ius ad bellum o derecho a recurrir a la fuerza o la guerra, en la que debe cuidarse el uso proporcional de la fuerza y evitar afectar a poblaciones civiles, lo que en caso de sistemas automatizados con el uso del ciberespacio, parecería que es más controlado y eficaz en ataques a objetivos específicos, pero si fallan ya sea por error del hombre o la maquina o ambos, surgen interrogantes de cómo se aplicaría el DI y el DIH al respecto.

Si a esto se observa el Ius in bello, de qué forma se protege a las poblaciones no beligerantes y si en estas se mezclan combatientes que los usan como escudos humanos o tal vez quieren ser partícipes mostrándose como civiles no combatientes aprovechando el DIH para buscar sanciones contra el enemigo y el rechazo del Sistema Internacional, para aislarlos y debilitarlos.

Surgiendo interrogantes sobre el uso de las ciberarmas que basadas en su autonomía, sólo valoran pérdidas calculadas en base a algoritmos y representaciones de simples números en caso de cuantificar víctimas y daños a objetivos previamente trazados. ¿El DI y/o el DIH logrará procesar y sancionará a los Estados, fabricantes, programadores, usuarios o ciberpilotos y de qué forma?, ¿En base a que normas, reglas y criterios?.

El trabajo de Marín (Marin, 2023, págs. 74 - 75), plantea diversos desafíos a resolver, apoyado en tres escenarios en el uso de la ciberarmas o sistemas de armas autónomas letales, como él las denomina, destacando: a) el hombre es parte de la toma de decisiones de la ciberarma autónoma; b) la ciberarma autónoma procesa y asume la decisión final de ataque y el hombre puede cancelarla y c) la ciberarma autónoma actúa plenamente sin intervención humana acorde a criterios prestablecidos.

El problema que se plantea, no es menor, siendo de preocupación del Grupo de Expertos Gubernamentales (GEG) de NNUU sobre los Sistema de Armas Autónomas (SAA), cuya definición aún no es consensuada, si deben ser plenamente autónomas y actuar además de forma indiscriminada, excluyendo de las SAA a los UAV y sistemas militares altamente automatizados (ej. Misiles tierra-aire), en la que el DIH no se aplicaría en su uso en la guerra en Ucrania, como advertiría la Federación Rusa en cuanto a los alcances y limitaciones del DIH en su conflagración respecto a los SAA (Marin, 2023, pág. 75).

Entonces, si en informática, cualquier componente puede ser utilizado de forma dual, tanto para fines civiles como militares, la identificación de su utilización es acorde a lo que se entienda o quiera entenderse, pues de esa manera cualquier objetivo civil en base a dicha dualidad podría pasar a convertirse en un objetivo militar, si además están contenidas en infraestructuras civiles, derivado de la dualidad en sus capacidades de uso podrían pasar a ser militares y por tanto a devenir en objetivos de ataque militar.

Aunque en apariencia la dualidad[5] brinda enfoques acorde a la visión del atacante, sería justificativo para realizar ataques por su parte, en este caso de Rusia en contra de instalaciones de

[5] *Marín M., A. (2023). "Los Sistema de Armas Autónomas Letales y el Derecho Internacional Humanitario en la Guerra de Ucrania". En el principio de distinción el autor establece: "Dicha computarización a gran escala (sistemas de armamentos, infraestructuras críticas, sistemas de comunicación, etcétera) establecen una nebulosa entre los objetivos militar y civil. Los investigadores R. Geib y H. Lahmann argumentan que, en el mundo cibernético, cualquier componente podría ser un objeto de uso dual y ser utilizado en la actualidad o en un futuro como objetivo militar legítimo, con amplias repercusiones hacia la población civil. Así, potencialmente, cualquier infraestructura cibernética (computadoras, redes y cables) o incluso el propio ciberespacio podrían ser calificados como un objetivo militar. A ellos se añadirían otras*

Ucrania, por ende de no aplicación del DIH al haber sido posiblemente utilizados en la conflagración militar. Lo que contradictoriamente, por el otro lado, se entendería como ataques indiscriminados que violentarían más bien los principios de distinción, precaución y proporcionalidad del DIH.

La necesidad de instrumentalización jurídica para el establecimiento de normas y reglas que diluciden responsabilidades y limitaciones en cuanto al uso del ciberespacio, las armas que se utilizan acorde al avance tecnológico y la cada vez más desarrollada automatización, provocan que las respuestas se sigan construyendo, con avances como el Manual de Tallin 2.0 que aporta guías a observarse[6].

Los Estados, no pueden desligarse de sus responsabilidades en el uso del ciberespacio, los ciberataques y el uso de los SAA, no pudiendo evadir el responder por los daños causados a personas que no participan de la conflagración armada, menos al tratar de justificar que los SAA no pueden generar responsabilidad por sus funciones autónomas que poseen, pues no se las puede procesar y mucho menos enjuiciar.

Una regla auxiliar, derivada del Manual de Tallin 2.0, es la número 20 que indican que las operaciones cibernéticas en un conflicto armado están sujetas al Derecho Internacional de los Conflictos Armados, que complementado con el inciso a) de la regla 24 hace responsables criminalmente a los comandantes, sus superiores por ordenar operaciones cibernéticas que constituyan crímenes de guerra, incluyendo algoritmos que se utilicen para el ataque de infraestructuras críticas. Que junto a la regla 14 fortalecen la responsabilidad contra Estados atacantes y sus hackers o ciberguerreros.

Al respecto, Andrea Cochini (Cocchini, Real instituto ELCANO, 2021), plantea que los Estados sean responsables por sus actos y los vinculados a estos dentro del ciberespacio, haciendo un símil entre la "diligencia debida" y su traslado al ciberespacio con la ciberdiligencia debida.

---

infraestructuras civiles que pudiesen ser utilizadas como infraestructuras militares en caso de conflicto armado como: centrales eléctricas, instalaciones de telecomunicaciones, puentes, etcétera. Por lo tanto, si cualquier elemento de uso dual puede ser considerado un objetivo, sería muy difícil establecer por un SAAL cómo discernir lo militar de lo civil y por tanto ser capaz de cumplir con el DIH. Dicha premisa podría resultar una potente excusa para la Federación Rusa argumentando que sus ataques sobre infraestructuras críticas ucranianas o edificios civiles habría sido porque dichas infraestructuras o edificios habrían sido utilizados en el ámbito militar como provisión de electricidad a estamentos militares o el uso de edificios civiles como puestos de observación militar o de comunicaciones (Geib y Lahmann, 2012, pp. 382-383; Kelsey, 2008, p. 1437).". Revista Relaciones Internacionales. Número 53, Junio a Septiembre 2023, Grupo de Estudios de Relaciones Internacionales. Universidad Autónoma de Madrid. Pag. 76..

[6] *Ídem 5. El autor destaca la responsabilidad atribuible a los Estados derivados del uso del ciberespacio y las operaciones cibernéticas realizadas en el, manifestando lo siguiente: "Un concepto extremadamente importante sería el de la responsabilidad. Con relación al Manual de Tallinn 2.0, la regla 14 establece que un "estado tiene responsabilidad internacional sobre cualquier acto cibernético atribuible a dicho estado que constituya una violación de una obligación legal internacional". En cuanto a la regla 17, que trata de los actos "por delegación" (proxy), especialmente de aplicación para los hackers, de acuerdo con las leyes internacionales, las operaciones cibernéticas llevadas a cabo por actores no estatales, pero que estén bajo un control efectivo de un estado, entonces dichos actos serían atribuibles a dicho estado. En cuanto al aspecto de las contramedidas, los expertos estuvieron de acuerdo que dichas contramedidas no podían violar una norma perentoria y que deberían ser proporcionales al daño recibido, aunque no existiría la necesidad de que dichas contramedidas cibernéticas o analógicas (pudiendo ser a través de los SAAL) tuviesen como objetivo el mismo órgano estatal que hubiese violado la ley internacional (Jensen, 2017, pp. 750-751, p. 754; Schmitt, 2017).". Pag. 82.*

Dicho planteamiento, es destacable pues dentro del ámbito del derecho y mandatos, tanto la personalidad jurídica, como sus representantes deben actuar de forma congruente en el ámbito internacional y nacional de sus propios Estados, cuya responsabilidad precisamente deriva del principio de confianza que se otorga para el respeto a las normas del DI y en caso de combates al cumplimiento del DIH, lo que conlleva a actuar tomando las medidas y cuidados, asumir investigaciones en contra los infractores, actuar de oficio, sin dilaciones, de forma imparcial y sobre todo efectiva en contra de ciberataques, ciberguerras, ciberterrorismo y ciberdelincuencia como mínimo dentro su territorio.

En general, las actuaciones dentro del ciberespacio por sus características e implicancias en diferentes ámbitos, incluyendo el de la geopolítica, representan desafíos no sólo para los Estados, sobre todo para la humanidad, la regulación del mismo aún incipiente es necesaria sobre todo para establecer condiciones que garanticen la libertad de uso pero en contraste de forma que no repercuta en daños o afectaciones a los demás.

5.3 TIPOS DE CIBERATAQUES

Cuando se habla de ciberataques debe entenderse como las actividades planificadas y sistematizadas llevadas adelante con el propósito de afectar a los sistemas informáticos de las victimas u objetivos, ayudados del uso de herramientas de la misma naturaleza, cuyos fines serán diversos y por ende las variedad de mecanismos a utilizar serán acorde al tipo de ciberataque que se pretenda.

Esto quiere decir, que para la realización de ciberataques se utilizaran una o varias herramientas informáticas, pudiendo combinarlas para atacar tanto los programas o SW como el HW, así como las infraestructuras vinculadas a los sistemas que están siendo afectados.

Para comprender la magnitud del problema a nivel global, se listaran las siguientes estadísticas, tomadas de la página de Techopedia, elaboradas por Nicole Kolesnikov (Kolesnikov, 2023), en el que tomaron cincuenta estadísticas de ciberseguridad, brindando un panorama aproximado al respecto:

a) Según las estadísticas publicadas (Kolesnikov, 2023), se producen alrededor de 3,400,000,000 ó 3,400 millones de ataques DIARIAMENTE de pishing incrustados en correos electrónicos o redes sociales, para su distribución. Lo que se busca con el pishing es capturar datos sensibles de las víctimas. Para entender la magnitud del problema, si en el mundo habitan 8 mil millones de personas aproximadamente en un mes el tamaño de los ataques de pishing superan en 12 veces el tamaño de la población mundial.
b) El segundo problema en ser listado son los ataques DDoS, precisamente utilizados en los ciberataques a Estonia en 2007. En 2022, sólo la empresa informática Microsoft evitó más de 520 mil ataques en el año. Google, por otro lado, en 2020 dio a conocer que posiblemente China lo ataco en 2017, al identificar, según la fuente (Kolesnikov, 2023), servidores ubicados en dicho país, constituyendo el ciberataque de DDoS más grande registrado.
   En 2023, en publicación de telegram atacantes rusos manifestaron que atacaron la Asamblea legislativa de Francia en represaría al apoyo de este último a Ucrania, afectando su página web mediante DDoS.
c) El malware en 2023, apareció con más de 300 mil nuevas variantes por día, según la misma fuente consultada (Kolesnikov, 2023). Utilizando para su distribución también

correo electrónico en porcentajes que superan el 90%, con permanencia hasta su detección de 49 días. Vale decir, que no son detectados inmediatamente y durante el periodo de tiempo hasta que se los neutralice, actúan no sólo robando datos o ingresando al sistema atacado, también busca dañar e interrumpir el sistema. Para su difusión utilizan pluggins o pequeños programas complementarios que se instalan en los sistemas.

Son utilizados para capturar dispositivos para minar criptoactivos, o aprovechar el IoT o internet de las cosas. El malware alcanzo la friolera cifra de más de 5.500 millones de ataques, superando a los provocados por rasonware.

d) El rasonware, es una variante del malware, pero que ocupa un rasgo independiente de ciberataque, porque captura o retiene al sistema informático atacado, buscando principalmente se paguen rescates. Es el ciberataque que busca monetizar sus actividades a través del secuestro de sistemas e infraestructuras críticas, como las suscitadas en USA en sus oleoductos, que provocaron se paguen millonarios rescates. Según Comparitech, utilizada por la autora (Kolesnikov, 2023), los rescates generaron más de 115 millones de dólares en afectaciones.
e) Los ciberataques para descifrar contraseñas o "password" son frecuentes y bastante agiles con las capacidades computacionales de los dispositivos que utilizan los atacantes hoy en día. Según la fuente Security.org, utilizada por la autora (Kolesnikov, 2023), si la contraseña de ocho caracteres solo utiliza letras, se puede descifrar instantáneamente, si usa adicionalmente una letra mayúscula en la clave se demora 22 minutos en descubrirla, si además al último se usa un número se demora una hora y si además se usa un carácter o símbolo adicionalmente demora ocho horas en ser descifrada. Pero si la clave consta de doce caracteres y está compuesta por número, símbolo, letra mayúscula y letras, se demoraría más de treinta y cuatro mil años en descifrarla. La pregunta es ¿Qué pasará con las capacidades de procesamiento de las computadoras cuánticas? Según la misma fuente, un hacker puede intentar más de 2 billones de combinaciones para descifrar una contraseña en veinte dos segundos.
f) Ciberataque a los dispositivos conectados a Internet, conocidos como IoT o Internet de las cosas, es el que está generando crecimiento en sus estadísticas, pues no sólo se habla de electrodomésticos, también de dispositivos sensibles como los de uso médico, vehículos u otros de uso no comercial, ni civil, como los militares y de defensa nacional. Siendo una de las preocupaciones que se está tratando de prever sobre todo con el uso de las redes 5G.

La ciberseguridad, para la autora (Kolesnikov, 2023), según fuentes consultadas está en aumento, constituyendo una gran oportunidad comercial, mientras que por el otro lado la media de las pérdidas sufridas por violaciones a la ciberseguridad, representaban para 2021, según IBM utilizada en el estudio, 4.35 millones de dólares en pérdidas promedio. Incluyendo en el análisis de perdidas lo que representa el trabajo remoto y las filtraciones que generan en relación al trabajo presencial, cuya diferencia según IBM, es de un millón de dólares entre ambas modalidades.

También, para reducir brechas de ciberseguridad, las empresas que invirtieron en IA y automatizaron plenamente su seguridad, lograron no sólo disminuir en promedio sus costos, también optimizar las detecciones con diferencias de más de cien días en promedio con las empresas que no invirtieron en tales medidas. Esto es relevante, pues lo que se busca tanto para las empresas como para los Estados es optimizar recursos, lo cual también implica que la plena

automatización de su seguridad estaría delegada y susceptible a que el sistema apoyado o basado en IA funcione correctamente, generando en caso de fallas o cese de funcionamiento riesgos a su propia seguridad.

Desde el punto de vista de los países que sufren más ataques de malware se encuentran USA, UK y la India en 2022. En caso de la propagación de malware, según las fuentes utilizadas por la autora (Kolesnikov, 2023), en 2021 los países asiáticos como Vietnam o Filipinas estaban en puestos de mayor foco, incluyendo a seis países dentro del top diez provenientes de Europa.

Los datos de ciberguerra, que presenta la fuente (Kolesnikov, 2023), da cuenta que Rusia y China lideran los ciberataques maliciosos, con el 35% a nivel mundial, cada uno con más de 75 ataques confirmados.

En los que usan malware y otras herramientas de ataque, para prácticas de espionaje, afectación a infraestructuras críticas, apoderarse de propiedad intelectual, afectar actividades en redes sociales y de carácter político. Inclusive, según la fuente, el 74% de los ingresos por rasonware tienen como destino Rusia, apoyada en un reportaje de la BBC news.

Para USA, Mi5 y el FBI, China utiliza diferentes tipos de ciberataques con propósitos de obtener no sólo información, con actores pertenecientes al Ministerio de Seguridad del Estado de ese país, que estuvieron participando en extorsión, criptojacking, robo de identidades y otras actividades ilícitas para obtener dineros.

El rasonware, también afecto a infraestructuras críticas, en las que las de salud fueron las más afectadas, seguida por la industria, gobierno, TIC, servicios financieros y otros más. Recordando que este tipo de ciberataque busca monetizar sus acciones de secuestro o control.

De lo descrito en base al artículo de consulta y sus diversas fuentes citadas, se observa que la ciberseguridad es prioritaria a nivel global, debido a que los ciberataques no discriminan las víctimas, pero si las seleccionan según intereses que se busquen, por lo que a nivel Estados tanto China como Rusia están clasificados como países promotores de prácticas de ciberataques con fines de conflagración o afectación a sus objetivos, en ciberguerras.

El uso de la Inteligencia Artificial o IA, representa ventajas y desventajas, pues de ser capturada o intervenida por potencias extranjeras, cuando esta debe supervisar la seguridad de las diversas capacidades de un Estado, genera susceptibilidad sobre la delegación de poder en base al funcionamiento apoyada en la plena autonomía de manejo que podrían tener los sistemas basados en dicha tecnología.

El incremento en los ciberataques, que van expandiendo sus capacidades a la par que avanza la tecnología, generan riesgos cada vez más complejos a resolver por parte de los Estados, las Organizaciones Internacionales y la Cooperación Internacional como medio que coadyuve al mejoramiento de la ciberseguridad de cada país, región y Sistema Internacional en general, en la que son los propios Estados que están inmersos en prácticas que buscan afectar a otra potencias y al propio Sistema, contradictoriamente en los que actúan. Elevando así aún más los desafíos a resolver para controlarlos y potenciar la ciberseguridad mundial.

6. *MARCO CONCEPTUAL*

Por la diversidad de términos utilizados en el presente trabajo, cuya extensión trasciende el título del trabajo de investigación, se conceptualizaran los siguientes y más relevantes:

i. CIBERACTIVISMO: son actos de personas que utilizan TIC para generar, participar, promover y buscar masificar movimientos en las redes informáticas, con propósitos del tipo político y/o ideológico.
ii. CIBERAMENAZAS: son actividades maliciosas realizadas con ayuda de las TIC que buscan violentar o agredir la seguridad de un sistema informático o cibernético de una o varias personas, organizaciones u entes de diversa naturaleza (militar, político, económico, salud, energético, etc.), para inutilizarlos, capturarlos, secuestrarlos u obtener ventajas como las del tipo económico o de otra índole.
iii. CIBERARMA: son programas informáticos utilizados para atacar objetivos preestablecidos con el propósito de capturarlos, alterar su normal funcionamiento y/o destruirlos, afectando tanto su sistema de SW como sus infraestructuras físicas conectadas a él.
iv. CIBERACOSO: uso del ciberespacio y sus aplicaciones para acosar a las personas mediante el uso de Internet, redes sociales, mensajes u otros accesos que brindan las TIC.
v. CIBERATAQUE: es un ataque planificado y sistematizado aprovechando las TIC que busca intervenir, interceptar, controlar, afectar funcionamiento, destruir o inutilizar el sistema informático o cibernético del o los objetivos, utilizando herramientas cibernéticas que interactúen tanto en el SW como en el HW de las víctimas o afectados.
vi. CIBERDILIGENCIA: estándar que pretende responsabilizar a los Estados sobre las ciberamenazas, ciberataques u otras actuaciones similares, debiendo estos actuar de forma obligada para monitorear, prevenir, mitigar o detener a individuos que actúen dentro su Estado realizando actividades cibernéticas observadas. Debiendo además realizar investigaciones, procesos y aplicar sanciones a los sujetos responsables de actos realizados en el ciberespacio que sean prohibidos por el derecho y/o leyes.
vii. CIBERDIPLOMACIA: es el conjunto de actividades realizadas por los Estados principalmente, que apoyados en la Cooperación Internacional trabajan en temas y objetivos relacionados a temas informáticos o cibernéticos, que les permita interactuar en el ciberespacio de manera segura, libre, sin restricciones pero con responsabilidad para evitar daños a terceros.
viii. CIBERDEFENSA: es el conjunto de actividades y operaciones asumidas, principalmente por los Estados, empresas y/o personas, para proteger y establecer la seguridad del o los sistemas informáticos tanto de los programas como de las estructuras físicas que las componen, utilizando protocolos, herramientas y personal capacitado en temas de ciberseguridad.
ix. CIBERDELINCUENCIA: conjunto de actividades antijurídicas, típicas, culpables y dolosas realizadas en el ciberespacio por parte de sujetos individuales u organizados, que buscan la obtención de algún tipo de ventaja, siendo el económico el principal móvil, para cometer ilícitos con la ayuda de las TIC, afectando cuentas bancarias, tarjetas de crédito, secuestro de identidades en redes sociales o páginas web o correos electrónicos o los propios dispositivos utilizados por sus víctimas. Pudiendo, también degenerar en actividades de ciberacoso del tipo sexual o búsqueda de victimas en redes sociales con diversos fines delictivos y sancionados por las normas legales del tipo penal y/o civil, entre otros más.

x. CIBERDELITO: conjunto de tipos penales sancionados por normas legales acorde a jurisdicciones de cada Estado. Debiendo observarse que su establecimiento en el entorno internacional, responde a Cooperación Internacional de diversas OI y Estados, que trabajan para establecer los tipos a ser observados y sancionados.

xi. CIBERESPACIO: espacio virtual creado a partir de infraestructuras físicas en combinación con programas informáticos que interactúan para generar comunicación en la red cibernética e intercambiar datos, que representan la forma de interacción de los usuarios que a través de las TIC y la extensión de las redes interactúan, accediendo a diversas páginas y programas instalados, navegando en Internet.

xii. CIBERGUERRA: son las operaciones de ataque y defensa que se producen entre diferentes actores, que trasladan su conflicto al ciberespacio, buscando afectar y/o dañar tanto infraestructuras criticas así como programas informáticos del o los enemigos, para anular sus capacidades de confrontación en base al ataque a sus sistemas interconectados a través de redes informáticas que las controlan.

xiii. CIBERNÉTICA: es la ciencia cuyo objeto de estudio son los sistemas de comunicación y automatización, que en base a características del humano tratan de emularse con ayuda de la electrónica y la mecánica. Sin embargo, para efectos del trabajo serán entendidos como sistemas informáticos, utilizando dicho termino de forma similar e indiferente entre ambos.

xiv. CIBERRESILIENCIA: capacidad que posee una organización, Estado, empresa o persona que afectada por algún tipo de amenaza, ataque o incidente del tipo informático es capaz de resistir o reestablecer sus capacidades de TIC.

xv. CIBERSEGURIDAD: es el conjunto de medidas y recursos humanos, físicos, de infraestructura, económicos y de conocimiento que son utilizados para proteger y hacer frente a cualquier tipo de incidente, ataque, crisis o daño generado o que amenace a los sistemas informáticos, infraestructuras críticas conectadas a estos y a la vida de las personas o el normal desenvolvimiento de su sociedad que las utiliza.

xvi. CIBERTERRORISMO: son los actos realizados a través del uso de las TIC que buscan generar caos, terror, desconfianza, destrucción, afectación y/o cualquier tipo de daño a las personas, su sociedad, sus infraestructuras críticas, su economía, telecomunicaciones, sistemas de defensa, de seguridad y cuanto sistema este interconectado a través de las redes informáticas. También, son los actos perpetrados con ayuda de las TIC que tienden a captar, adiestrar, difundir, transferir, coordinar y promover actos con fines terroristas, incluidos sus movimientos o agrupaciones que se apoyan en el uso de Internet y las TIC en general.

CAPITULO II

1. *ORGANIZACIONES INTERNACIONALES Y SU POSTURA FRENTE A LOS CIBERATAQUES*

Las OI son sujetos internacionales de derecho, constituidos legalmente por los Estados acorde a instrumentos del DI como son los Tratados Internacionales, su existencia como se analizó responde a un conjunto de características y decisiones que responderán a los intereses, posiciones y necesidades de los Estados.

Debido a la actuación de los Estados acorde a sus intereses, impulsa que las OI existan para mejorar su propio desarrollo a partir de Cooperación Internacional, que coadyuve a resolver problemas transversales que los afecten y apoye a mantener el equilibrio en la convivencia dentro del Sistema Internacional.

Uno de los problemas actuales que afectan a la mayoría de los países, es precisamente el uso abusivo que se hacen de las TIC, que afectan a la seguridad de todos incluyendo a las propias OI, en la que un solo Estado no podrá resolver todos los requerimientos o problemas, menos aislarse del resto de países, debiendo acudir en base a experiencias y conocimientos adquiridos por otros Estados, mediante la Cooperación Internacional, puedan acceder a las mismas y fortalecer capacidades que deben desarrollar para beneficio propio y del resto de Estados, por lo que es válido cuando se dice que una cadena es tan fuerte como su eslabón más débil.

Por lo que, la defensa de intereses comunes de los Estados en una OI, también implica que sean propios individualmente, aunque estos últimos no siempre responderán a los del resto colectivo; de esta forma las OI deberán adaptarse a los requerimientos de sus Estados en diferentes momentos y estos a los de la mayoría. Por lo que las OI adquieren un carácter mixto entre su autonomía y la dependencia respecto a sus miembros, en la que sus labores y decisiones deben buscar beneficiar a todos y mantener estándares lo más neutrales posibles, pero relevantes acorde a las problemáticas que se traten.

La ciberseguridad y sus diversas expresiones, dentro del ciberespacio, en un Sistema Internacional cada vez más volátil y conflictivo, ha obligado a que los Estados a través de sus diversas OI, trabajen para responder de forma dinámica a lo que cada día es más difícil de controlar, donde no sólo la asimetría del problema constituye de por si dolores de cabeza para los Estados, sino que dicha asimetría también se refleja en las capacidades que poseen cada uno de estos, donde los más aventajados buscaran fortalecer su poder individualmente o como bloque, para incidir sobre el resto de Estados en desventaja.

Para los países miembros de movimientos o grupos de países, como los BRICS+, que no han constituido aún una OI, esta última que como se observó posee características específicas que deben cumplirse, confronta intereses diversos a las que poseen las mismas y sus Estados miembros, asumiendo una posición revisionista del statu quo que se ha llegado a denominar del Nuevo Orden Internacional o Mundial, apoyados en la multipolaridad y por ende en el enfrentamiento con el que hoy es reconocido aún como el hegemon y sus aliados.

La lucha no sólo estriba en expandir fronteras, territorios y RRNN a poseer, también el dominio del ciberespacio y el desarrollo de herramientas cada vez más autónomas que las controlen, como es la Inteligencia Artificial.

Derivando en ciberguerras cuyo fin es el de afectar la infraestructuras críticas del enemigo y preservar las propias. Por lo que las guerras cada vez son más sofisticadas, pero no por eso menos mortales y violentas, en la que las OI a pesar de pretender mantener neutralidad, están llamadas a actuar de forma cada vez más dinámica utilizando la Cooperación Internacional para procurar mantener la paz y la seguridad mundial, apoyadas en el DI, DIH y DDHH.

En este capítulo, se describirán las OI más relevantes dentro del sector de la ciberseguridad y sus acciones que están asumiendo contra los ciberataques, ciberdelincuencia, ciberguerras principalmente.

2. *ORGANIZACIÓN DE NACIONES UNIDAS (ONU)*

Creada en 1945, a través del Tratado constitutivo o Carta de las Naciones Unidas[7], ha establecido como propósitos y principios, mantener la paz y la seguridad internacionales, asumiendo medidas colegiadas que prevengan y eliminen amenazas a la paz, agresiones o quebrantamiento a esta última. Apoyados en la producción de Cooperación Internacional que brinde soluciones a los problemas internacionales que se presenten en diversas áreas, siendo la humanitaria la que implicara a todo lo relacionado con esta, incluyendo los medios tecnológicos que desarrolla.

Adicionalmente, dentro de la lista de principios enunciados, se destaca el numeral 4 del Art. 2 de la misa Carta, que establece que sus Estados miembros deben abstenerse de amenazas, uso de la fuerza contra la independencia de sus pares, territorio o cualquier forma incompatible con los propósitos de las Naciones Unidas (NNUU). Esto representa que la ONU buscara mecanismos de solución a diversas amenazas o ataques que se presenten y atenten a la seguridad y la paz.

Los ciberataques se entienden como ciberterrorismo para la OI, por lo que para la ONU, debe atenderse por un organismo especializado que posee, denominado "Oficina de Lucha contra el Terrorismo" (OLCT)[8], la que fue creada el 15 de junio de 2017, por mandato de la Asamblea General de las Naciones Unidas vía Resolución 71/219, nombrando al Sr. Vladimir Voronkov[9] como el primer Secretario General Adjunto.

---

[7] *Organización de las Naciones Unidas (ONU, 2023). Carta de las Naciones Unidas (texto completo). Naciones Unidas. Acceso web 2023, https://www.un.org/es/about-us/un-charter/full-text*

[8] *ONU (2023). Oficina de Lucha contra el Terrorismo. Acceso web 2023, https://www.un.org/counterterrorism/es/cybersecurity*

[9] *ONU (2023). El Sr. Voronkov en discurso emitido en Bielorrusia, el 26 de septiembre de 2019, en ocasión de celebrarse evento Contra el Terrorismo con Tecnologías nuevas y emergentes (Side-Event on Countering Terrorism with New and Emerging Technologies), dijo: "Debemos unirnos ahora, y debemos hacerlo rápido, para mitigar esta amenaza y garantizar que las nuevas tecnologías siguen siendo una fuerza para el bien y no para el mal", denotando así la urgencia con el que deben encararse estos desafíos. Acceso web 2023,*

https://www.un.org/sites/www.un.org.counterterrorism/files/20190926_usgvoronkov_statement_belarusside-event.pdf

Según la página oficial de la ONU, dicha Oficina se creó con el objetivo de que la "Estrategia Global de las Naciones Unidas contra el Terrorismo" (EGCT) pueda implementarse en los diferentes Estados miembros de la OI. Además, dicha Oficina agrupa en su seno a dos organismos preexistentes, como el "Pacto Mundial de Coordinación de la Lucha contra el Terrorismo de las Naciones Unidas" (PMCLCT), que anteriormente era el denominado "Equipo Especial sobre la Ejecución de Lucha contra el Terrorismo"; y el segundo, conformado por el "Centro de las Naciones Unidas de Lucha Contra el Terrorismo".

Las funciones encargadas a la OLCT, son: 1) liderar los mandatos de Lucha contra el Terrorismo encargados al Secretario General provenientes de diversas entidades de NNUU; 2) coordinar con las entidades que conforman el PMCLCT y la aplicación de los cuatro pilares que forman parte de la estrategia EGCT; 3) mejorar la prestación de asistencia de la OI a los Estados para generar capacidad contra el terrorismo; 4) incrementar la visibilidad y promoción de la ONU en su lucha contra el terrorismo y 5) buscar se priorice oportunamente en el sistema de NNUU la lucha contra el terrorismo y adicionalmente se fortalezca dentro la EGCT la prevención del extremismo violento.

Las prioridades de la OLCT son establecidas por la Asamblea General de las NNUU, son de carácter bienal en base a examen a la EGCT, por lo que la OLCT genera alianzas con diversos actores de diversa procedencia tanto de la academia, OI, interesados, sociedad civil, etc.

La OCLT para brindar asistencia para la creación de capacidad de sus Estados miembros, cuenta con un ente especializado en estas tareas, que fue creado en 2011, denominado "Centro de la Naciones Unidas de Lucha contra el Terrorismo" (CNULCT), actuando a través de proyectos y programas que fortalezca los pilares de la EGCT.

Además, la OLCT trabaja de manera coordinada con el Consejo de Seguridad de la NNUU (CSNU), a través de los organismos pertenecientes a este último, tales como: "Comité Contra el Terrorismo", "Comité de Sanciones contra el EIIL (Dáesh) y Al-Qaida" y el "Comité del Consejo de Seguridad" creado en 2004 para la no proliferación de armas nucleares, químicas y biológicas. Dicha coordinación busca por un lado prevenir y responder frente a ataques terroristas y por el otro apoyarse en las capacidades de los diversos Comités que posee el CSNU.

2.1 LA OCLT Y LA CIBERSEGURIDAD

Existe el reconocimiento de que los ciberataques son perpetrados con fines terroristas, estableciendo que las actuaciones se realizan tanto a través de las denominadas Tecnologías de Información y Comunicación (TIC), así como el Internet, utilizadas para fortalecer las capacidades de los grupos terroristas que a través de dichos medios buscan no sólo provocar afectaciones a infraestructuras críticas, economía, política, democracia, sociedad y estabilidad de sus objetivos; también las propias a través de la búsqueda y movimiento de recursos financieros, reclutamiento de miembros, difusión de mensajes, planeación de ataques, comunicación e intercambio de información entre sus miembros, adquisición de material bélico y otros más.

La OLCT cuenta con el "Programa de Ciberseguridad y Nuevas Tecnologías" (PCNT), esto con el objetivo de fortalecer a través de la cooperación medios y capacidades que logren confrontar, mitigar, evitar ataques y daños a los bienes críticos de los Estados miembros.

La OLCT fomenta concursos o desafíos enfocados al campo de la Ciberseguridad, a los que denomina "Cyber Challenge", buscando que la sociedad civil a través de jóvenes expertos en el campo de interés participen en diferentes ejes de interés que define la OLCT, para que brinden soluciones novedosas. Las categorías en 2019 eran: a) ciberataques a infraestructuras críticas, IoT y dispositivos interconectados; 2) propagación en línea de contenidos terroristas; 3) comunicaciones terroristas en internet y 4) financiación digital del terrorismo.

Más allá de los desafíos, se desprende de los mismos, que las afectaciones a infraestructuras y medios físicos es una preocupación para la ONU y por ende para sus Estados miembros, siendo quizás uno de los puntos más críticos que genera preocupación en el mundo, pues es relevante destacar que los sistemas informáticos han manejado, desde hace décadas, centros de energía nuclear, plantas de provisión de energía eléctrica, distribución de gas domiciliario e industrial, redes de provisión de agua potable, redes de transporte, sistemas de navegación aérea, sistemas de datos e información de ciudadanos, sistemas de bolsa de valores y mercados, sistemas financieros, etc.

La ONU, a través de su OLCT, ha emitido diferentes instrumentos o resoluciones que brindan lineamientos y recomendaciones enfocadas no sólo a la LCT, también a su vinculación con la necesidad de fortalecer la Ciberseguridad de la OI y sobre todo de sus Estados miembros.

Los documentos que destaca la OLCT son cuatro: 1) Sexto examen a la EGCT; 2) Resolución 2341 (2017) del Consejo de Seguridad; 3) Resolución 2370 (2017); 4) Texto del Consejo de Seguridad S/2015/939 denominados Principios rectores de Madrid.

Como se explicó previamente, las evaluaciones bienales a las que se somete la OLCT son llevadas a cabo por la Asamblea General, en dicha evaluación se observa el cumplimiento y desarrollo de las EGLT, la sexta evaluación o examen[10] en el que también se insertan resoluciones que buscan fortalecer y mejorar las acciones que se vienen desarrollando, se reflejó en el documento A/RES/72/284 de 26 de junio de 2018[11], denominado "Examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo", que refleja avances alcanzados, aplicación y posibles actualizaciones a la EGLT.

En dicho documento se expresa la preocupación de atentados terroristas contra infraestructuras críticas, con afectaciones no sólo a los gobiernos de los Estados miembros, también al sector

---

[10] *ONU (2023). Página web de la Oficina de Lucha contra el Terrorismo, CIBERSEGURIDAD. Destaca uno de los puntos emitidos en el documento correspondiente al Sexto examen de la Estrategia Global de la Naciones Unidas contra el Terrorismo (EGLT), indicando: "Los Estados Miembros expresaron "preocupación ante el creciente uso, en una sociedad globalizada, por los terroristas y quienes los apoyan, de las tecnologías de la información y las comunicaciones, en particular Internet y otros medios, y ante el uso de esas tecnologías para cometer actos terroristas y en actividades de incitación, reclutamiento, financiación o planificación para actos de terrorismo". Sexto examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo".*

[11] *Declaración que describe de manera importante no sólo la preocupación sino las actividades que deben asumir para encarar los problemas que se derivan del uso tecnológico explotado por los terroristas, siendo un eje sobre el que se elaboró el respectivo examen por parte de la Asamblea General. Acceso web 2023, https://www.un.org/counterterrorism/es/cct/programme-projects/cybersecurity*

privado, instando a que se busquen alianzas público-privado tendientes a fortalecer integralmente medidas precautorias que eviten afectaciones.

Para esto, impulsa a que entidades de la ONU como el Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, parte del Pacto Mundial PMCLCT, deban coordinar de manera más cercana con las organizaciones regionales y subregionales en dicha lucha. Esto es relevante, pues muchos Estados a través de sus gobiernos de turno carecen de experiencia o recursos para confrontar de forma especializada la LCT, sin dejar de observar la disponibilidad de recursos en diversas esferas.

De hecho todo el mundo sabe del peligro latente que representan los ataques terroristas, pero al no poseer objetivos específicos y ser aleatoriamente seleccionados por los atacantes en base a sus propios objetivos, genera que pocos Estados estén preparados para la confrontación y hasta que no les suceda muchas veces no prestan la necesaria atención al mismo, pese a suscribir y ratificar instrumentos internacionales contra dicho flagelo.

La ONU, alerta y manifiesta su preocupación por el incremento de los ataques terroristas, el incremento de la violencia extremista, así como la migración aprovechada por sujetos para trasladarse entre diferentes Estados con el propósito de cometer actos terroristas, repercutiendo en la observación del fenómeno mundial que representa el desplazamiento de personas entre diferentes países y regiones en el mundo.

Destacando la Cooperación Internacional, ya no sólo como mecanismo de fortalecimiento de LCT, también como la herramienta a ser utilizada entre los Estados para combatir de forma coordinada y fortalecida, con el intercambio de información y experiencias entre los miembros de la ONU, para prevenir, confrontar y evitar diversas actuaciones que cometen los grupos terroristas y sus miembros contra las diversas sociedades, que derivaran en delincuencia organizada transnacional y el tráfico ilícito ya no sólo de objetos, también de personas con diversos fines, siendo el principal el de tipo económico para financiar sus actividades.

Resultado del examen, también se destaca el reconocimiento del uso que hacen los terroristas de las denominadas TIC e Internet, no sólo para difundir sus mensajes, también para reclutar nuevos miembros aprovechando las Redes Sociales que se utilizan en línea, recomendando que se eviten tales prácticas al interior de los Estados, debiendo estos observar y actuar para que no se lleven a cabo.

Lo último es relevante, pues más allá de los grupos terroristas, también son los propios Estados los que al contar con los recursos, cometen actos de ciberataques contra objetivos específicos, que podrán entenderse como ciberataques del tipo terrorista o político, según el caso.

Para dicho propósito la ONU recomienda a que los Estados asuman medidas legales en contra de los infractores en el uso de las TIC con fines terroristas. Recomendando además que si bien estos medios tecnológicos TIC e Internet son aprovechados por los terroristas, también representan una oportunidad para que los Estados los utilicen a su favor en su LCT.

De esa forma, se pueda lograr impedir que los terroristas adquieran armas, materiales y tecnologías para su fabricación y prácticas en contra las sociedades. Instando además a que las respectivas autoridades llamadas por ley de los respectivos Estados actúen de forma coordinada y

dinámica para reprimir a los terroristas, con articulaciones entre sus diversos órganos o poderes, sus fuerzas de seguridad, sus jueces y autoridades.

En el punto 81 del examen[12] acá en revisión, se destaca la importancia del multilateralismo en la LCT, pero al mismo tiempo condiciona a que dicha lucha debe realizarse en base al respeto de la Carta de las NNUU y el respeto al Derecho Internacional (DI).

Lo que representa que las acciones que deban asumir los diversos Estados en su LCT deben enmarcarse en los límites establecidos por las normas internacionales, aspecto no menor a ser observado e importante recalcarlo, por la coherencia que debe existir con respecto a las propias normas jurídicas de los Estados, debiendo ser claras, evitando ambigüedades y enfocarse a la LCT y evitando el "lawfare", por ejemplo.

Muchas de las resoluciones de NNUU, se construyen de forma sucesiva e integral, de manera tal que sirvan de apoyo para futuras decisiones y orientaciones para sus miembros, no representan soluciones absolutas, pero si lineamientos orientadores no sólo para las entidades de la ONU, sobre todo para sus Estados miembros.

De esta manera, se observan los Principios Rectores de Madrid[13], establecidos en 2015, en franca respuesta a la LCT, cuyo flagelo cada vez demuestra incremento en la violencia y expansión de redes en el mundo.

El documento nace del Comité contra el Terrorismo, quienes ante la urgencia de los acontecimiento en ese año, buscan frenar las migraciones o flujos de terroristas foráneos entre los Estados, emitiendo conclusiones emergentes de sus grupos de trabajo y sobre todo un conjunto de Principios Rectores sobre combatientes terroristas extranjeros; principios presentados en una especie de deberes a ser realizados por los Estados y presentados en formato de recomendaciones.

En la introducción al Anexo II que lista los Principios Rectores, se observa el uso de la TIC por parte de terroristas para reclutar, incitar y facilitar sus actividades. Destacan que el perfil del combatiente terrorista ha evolucionado, en la que se busca la captación de ingenieros, profesionales y empresarios en vez del soldado tradicional. Lo que representa una nueva amenaza a la seguridad y paz internacional.

La observación realizada por el Comité y sus miembros identificó de forma pertinente que el terrorismo ya no sólo busca actuar en campos de batalla tradicionales, también en otros

---

[12] *ONU (2018). A/RES/72/284. ´Examen de la Estrategia Global de las Naciones Unidas contra el Terrorismo´. Página 19, en su punto 81. "Subraya la importancia de las iniciativas multilaterales para combatir el terrorismo y de abstenerse de adoptar prácticas o medidas que sean incompatibles con el derecho internacional y los principios de la Carta". Acceso web 2023, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/198/84/PDF/N1819884.pdf?OpenElement*

[13] *ONU (2023). Reunión especial del Comité contra el Terrorismo sobre el tema Frenar el flujo de combatientes terroristas extranjeros. Madrid, 27 y 28 de julio de 2015. S/2015/939. Consejo de Seguridad. El documento elaborado constaba de tres anexos, los dos primeros dirigidos a las Conclusiones del Comité y sus grupos de trabajo, el segundo anexo desarrolla los principios y el tercer anexo dirigido a la declaración realizada por los Ministros de Relaciones Exteriores y del Interior quienes se reunieron en el mismo evento. Acceso web 2023, https://undocs.org/es/S/2015/939*

escenarios, en los que se destaca precisamente a raíz de las TIC, el ciberespacio a través de Internet.

El principio rector 10, recomienda que los Estados presten la debida atención a las comunicaciones y usos de las TIC por parte de los terroristas, en base a la observación y respeto a la ley y la privacidad, normas internacionales reflejadas en pactos, con restricciones a que este reguladas legalmente.

Si bien el respeto al Derecho Internacional y su normativa por parte de los Estados como garantes de Tratados y Convenios Internacionales, sobre todo en temas de DDHH son importantes, también lo es la necesidad de respuestas rápidas a los ataques terroristas, por lo que las legislaciones nacionales deben observar procedimientos que equilibren el derecho con la necesidad de prevención o confrontación de ser necesario contra terroristas y sus actividades.

En el mismo sentido, tanto el principio rector 13 como 14, reconocen la necesidad del uso de Internet y las TIC, recomendando que las restricciones a su utilización por parte de terroristas, responda a marcos normativos de respeto a derechos humanos (DDHH) e internacionales. Para lo cual invita a que se produzcan y fortalezcan alianzas con sectores privados en la LCT y el uso de los medios de TIC.

Para el enjuiciamiento penal, destacan la producción probatoria del tipo digital y su admisibilidad en procesos penales, incluidas las obtenidas en redes sociales, no sólo por parte de grupos de inteligencia, también autoridades,

Para esto el principio rector 25, recomienda a los Estados miembros hagan revisión de sus legislaciones para la admisibilidad de las pruebas digitales en su ordenamiento, con restricciones a la libertad de expresión cuyo límite se estableció en el artículo 19, párrafo 3 del Pacto Internacional de Derechos Civiles y Políticos[14], sin incurrir en arbitrariedades e ilegalidades contra la privacidad de las personas.

Las intervenciones a las comunicaciones tanto por parte de los Estados como por grupos o actores que actúan al margen de la ley, no sólo terroristas, ha degenerado en abusos y arbitrariedades, cuya deformación se observa en la persecución con fines políticos y económicos, cuyas regulaciones a favor de la Protección de la Privacidad se van fortaleciendo y actualizando frente a nuevas formas y variantes que infringen dichos derechos. Sin embargo, a los terroristas lo que menos les importa es el respeto a las normas de carácter internacional, nacional, local y sobre todo a los DDHH, por lo que también en ese entorno los Estados están en desventaja.

---

[14] *ONU (2023). Pacto Internacional de Derechos Civiles y Políticos. Artículo 19. párrafo 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas. Acceso web 2023, https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights#:~:text=Art%C3%ADculo%2019,-1.&text=Toda%20persona%20tiene%20derecho%20a,otro%20procedimiento%20de%20su%20elecci%C3%B3n.*

El principio rector 26, establece que los Estados miembros cuenten con personal capacitado en técnicas forenses y de vigilancia en redes sociales así como en TIC, dirigidas a prevenir que terroristas realicen actividades no sólo de reclutamiento, también de incitación hacia el terrorismo, todo enmarcado en el respeto a los DDHH.

Con respecto a los Ministros de Relaciones Exteriores y del Interior declararon en su punto 8, que debe buscarse evitar propagación del extremismo violento, apoyado en diálogos entre religiones y culturas, pero al mismo tiempo en franca confrontación contra la violencia y el extremismo violento practicado por grupos terroristas conocidos como el EIIL/Daesh, Al-Qaida, Boko Haram, Ansar al-Sharia, que utilizan las TIC para la difusión de ideología violenta y prácticas que realizan.

De los instrumentos observados, se extrae el factor común que las TIC e Internet han ido siendo ocupados por grupos terroristas y sus adeptos para fines diversos vinculados a sus prácticas, no sólo ya para coordinar migraciones de sus miembros, financiarse, también para reclutar personal, difundir mensajes de violencia extrema, fomentar la violencia y realizar ataques a distancia aprovechando las tecnologías que cada vez evolucionan y se desarrollan de forma vertiginosa.

Las resoluciones 2370 y 2341 ambas de 2017, emitidas también por el Consejo de Seguridad de la ONU, se apoyan en lo relevado anteriormente, el uso de las TIC por parte de terroristas, prácticas ya descritas, destacando que adicionalmente la resolución 2341 se enfoca en las recomendaciones de 2001 en base a resolución 1373 que insta a que los intercambios de información operacional se concentren en áreas como el tráfico y posesión de armas de destrucción masiva, uso de las TIC y otras más, con el fortalecimiento de acuerdos de diverso tipo enfocados a la represión y combate en la LCT.

Instando, además, a que los recursos humanos de Estados con formación presten asistencia al resto de Estados que lo requieran, enfocando esfuerzos a la protección de infraestructura crítica contra posibles ataques terroristas, de manera tal de fortalecer las capacidades de LCT, en base a transferencia de tecnología y programas utilizados para tal fin.

Para la ONU, la experiencia de INTERPOL en la vigilancia de redes sociales, es valiosa y a través de la propia página de la OLCT se establece un link que describe un protocolo general para dicho fin. El mismo se apoya en dos pilares: 1) identificación y 2) formación.

El primero dirigido a identificar a sospechosos y también testigos en base a análisis antiterrorista; el segundo, orientado a potenciar las capacidades de los investigadores en la detección de actividades terroristas, recopilación de pruebas electrónicas y registros, solicitudes de pruebas a partir de cooperación con otros cuerpos policiales fronterizos y la interacción y colaboración con el sector privado.

La interacción de INTERPOL y la ONU, se apoya en el proyecto conjunto con el Centro de la Naciones Unidas contra el Terrorismo (CCT), producción que dio como resultado talleres realizados entre 2018 y 2019, el manual titulado “Uso de Internet y las redes sociales para investigaciones antiterroristas”, obtener pistas de investigación y preservación de registros y cadena de custodia de pruebas.

Dichas labores son relevantes para los Estados pues permite interactuar con instituciones expertas en labores de campo que tienden precisamente potenciar las capacidades de respuesta e

interacción entre el personal de los países en el objetivo común que es la LCT, de manera tal que se logre no sólo detectar y procesar a los posibles terroristas, también interactuar en base a Cooperación Internacional e intercambio de información, tanto para mitigar o eliminar amenazas también preservar y custodiar pruebas.

Todo esto muestra que la LCT no es una labor solitaria, que es y debe ser confrontada por los diversos Estados de manera coordinada apoyados en la Cooperación Internacional, que la presencia de personal y grupos terroristas no es de localización fija y aislada, que sus miembros interactúan en diversas ubicaciones en todo el globo terráqueo, con ayuda o colaboración de Estados cuyos gobiernos apoyan sus prácticas o ideologías, e inclusive sin apoyarlas por el respeto a los DDHH y la solidaridad y práctica del Derecho Internacional Humanitario (DIH) apertura sus fronteras que son aprovechadas por miembros de organizaciones terroristas para migrar a esos territorios.

La evolución de TIC han reprimido las fronteras físicas, la ONU y sus miembros, junto a OI trabajan de forma conjunta para detectar e identificar actividades terroristas, no siempre pudiendo identificar a sus miembros, quienes aprovechando el anonimato que otorga Internet esconden su rostro, facilitando su traslación por toda la red entorpeciendo dar con su paradero.

Al hablar de terrorismo y terroristas, en sentido tradicional se los ubicaba en zonas o regiones de acción del tipo territorial geográfico donde operaban; con la evolución de las TIC e Internet los espacios físicos o geográficos se fueron extendiendo y alcanzaron el ciberespacio, por lo que los ataques y actividades que realizan se traslapan al espacio o territorio virtual. Si esto es así, no existen fronteras virtuales y de existirlas son traspasadas por atacantes, denominados ciberterroristas o ciberatacantes.

La evidencia en la práctica, para los terroristas y los ciberterroristas, es que no existe respeto a los límites impuestos por organizaciones internacionales como la ONU, que trabajan con sus Estados miembros en estrategias de LCT, apoyados en normativas internacionales de necesaria observancia, como el respeto a los DDHH por parte de sus Estados miembros.

Para los terroristas, como en algún lugar se mencionó, lo menos relevante es el respeto a los Pactos, derechos fundamentales de los Estados, Convenciones y Tratados Internacionales y mucho menos los DDHH de los enemigos a sus movimientos, ni siquiera los de sus propios adeptos; por lo que todo es un objetivo y la ONU no es la excepción.

A pesar de las iniciativas y trabajo que desarrolla de LCT, la ONU por su relevancia también es blanco y susceptible de recibir ciberataques, no estando exenta de dichos problemas, por lo que a pesar de la experticia que va desarrollando apoyado en diversas iniciativas y entidades, lo cierto es que ya sucedió y recibió ciberataques, generando preocupación al ser una OI líder en la lucha desplegada también en esta área.

2.2 CIBERATAQUES SOBRE LA ONU

Abril de 2021[15], fue crítico para la ONU, la infraestructura de su red de comunicación había sido atacada, no siendo el único ataque que recibió, afectación que se tradujo en el robo de datos de la OI con posibles repercusiones sobre entidades pertenecientes a esta.

Sin embargo, el ataque fue detectado luego de labores desarrolladas por una empresa de ciberseguridad que detecto la falla critica o fuga de información por parte de ciberatacantes. La ONU, a través de su portavoz, reconoció que la OI recibe constantemente ciberataques, incluyendo campañas de desprestigio; sin embargo, lo sucedido fue de mayor preocupación por las características y forma que asumió el ataque.

Para el portavoz, la detección del ataque se realizó al interior de la OI antes de la voz de alarma de la empresa de ciberseguridad, por lo que supuestamente ya habían tomado las medidas de atención al respecto. Seguimiento que se realizaba antes de abril y cuyas consecuencias se detectaron continuaban en agosto, con acciones por parte de los atacantes que seguían operando en el sistema afectando la integridad de la infraestructura[16] de la ONU.

La forma de generar el ataque, según reportes de medios de comunicación, se realizó a través de la web obscura o "dark web" en la que se adquirió o compró credenciales de un funcionario de la ONU, de manera tal de acceder al sistema y obtener información sobre la infraestructura informática de la OI.

Los ciberataques están relacionados con la ciberdelincuencia, pero sobre todo con el ciberterrorismo y la ciberguerra, participando en dichas prácticas también los denominados "hacktivistas"[17]; por lo que para IBM[18] las motivaciones por los que se producen los ciberataques, al margen de que son variadas, pueden agruparse en: motivaciones con fines delictivos (principalmente económicos), motivaciones con fines políticos (ideológicos o políticos, traducido en "hacktivismo" principalmente) y motivaciones personales (diversas, como la venganza, afectación a la imagen de la víctima, económicos, violencia, etc.).

---

[15] *SWI (2021). Swissinfo.ch. La ONU confirma que su infraestructura recibió un ciberataque en abril. Según declaraciones de la portavoz de la ONU, el Sr. Stéphane Dujarric, mencionó: "Podemos confirmar que unos atacantes desconocidos fueron capaces de violar partes de la infraestructura de Naciones Unidas en abril de 2021". Acceso web 2023, https://www.swissinfo.ch/spa/onu-ciberataque_la-onu-confirma-que-su-infraestructura-recibi%C3%B3-un-ciberataque-en-abril/46936214.*

[16] *Rodriguez, S. (2021). Cybersecurity news. La ONU, víctima de un ciberataque que ha afectado su infraestructura. Acceso web 2023, https://cybersecuritynews.es/la-onu-victima-de-un-ciberataque-que-ha-afectado-a-su-infraestructura/*

[17] *LISA Institute. (2023). Hacktivismo: definición, tipos, modus operandi y motivaciones. "Un hacktivista es un hacker que usa sus conocimientos informáticos para llevar a cabo acciones en el ciberespacio con una finalidad y una motivación políticas o ideológicas.". Acceso web 2023, https://www.lisainstitute.com/blogs/blog/hacktivismo-definicion-tipos-modus-operandi-motivaciones.*

[18] *IBM. (2023). Por qué ocurren los ciberataques. Para IBM al preguntarse "¿Qué es un ciberataque?", responde "Los ciberataques son intentos no deseados de robar, exponer, alterar, inhabilitar o destruir información mediante el acceso no autorizado a los sistemas." Acceso web 2023, https://www.ibm.com/es-es/topics/cyber-attack*

Esto representa que los ciberataques que recibió y recibe la ONU, tendrán fines diversos, desde la identidad de sus funcionarios, de sus funciones, de los niveles de tareas que desempeñan al interior de la OI, los programas y proyectos existentes, recursos económicos con los que cuentan, identificación de las fuentes de recursos, países y servidores que están a cargo o son enlaces con las labores de la ONU, bases de datos de documentos, información confidencial, etc.

Información variada que vinculada a la relevancia que posee la ONU es crítica no sólo para ella misma como OI, también para sus países o Estados miembros, pues dentro de las tareas que despliega esta la prevención y el mantenimiento de la paz, con tareas delicadas que realizan sus organismos como el Consejo de Seguridad, sus comités, sus oficinas, sus grupos expertos y diversas entidades, incluyendo sus grupos protocolares a cargo de recibir a líderes mundiales, etc.

Representa lo sucedido, un ejemplo de la vorágine y peligrosidad que significan los ciberataques en el mundo, más aún si los ataques se realizan sobre infraestructuras críticas, como plantas nucleares o redes de hidrocarburos[19], por mencionar ejemplos.

2.3 ONU Y EL GRUPO DE TRABAJO DE COMPOSICIÓN ABIERTA

La Asamblea General de la ONU, en 2021 establece un grupo enfocado a atender temas de seguridad en el uso de las TIC, para lo cual bajo su auspicio y mediante Resolución 75/240, establece grupo de composición abierta para el periodo 2021 a 2025, cuya base es que sus actuados sean por consenso.

Dicho grupo, tiene como tareas principales la elaboración de normas, principios y reglas de comportamiento de los Estados, este último con el énfasis de responsabilidad por parte de los mismos. Debiendo el grupo conformado, observar la aplicación de dichos instrumentos por parte de los Estados miembros, con la potestad de ser necesario de elaborar reglas de comportamiento adicionales para su aplicación.

En esencia el enfoque es el de trabajar de forma coordinada entre los diversos actores involucrados en el sector, que garanticen la seguridad en la utilización de las TIC, utilizando diversas herramientas tales como diálogos regulares con el involucramiento de los Estados, que los temas de seguridad, amenazas y peligros sean debidamente comprendidos, para asumir a través de la cooperación mecanismos que prevengan y mitiguen las mismas.

---

19 EXPANSIÓN. (2021). Ataque al oleoducto Colonial: el peligro de la industria conectada. EXPANSIÓN explica: "La compañía finalmente ha pagado el rescate a los hackers, lo que supone casi 5 millones de dólares. El pasado viernes 7 de mayo, Colonial, la mayor red de oleoductos de Estados Unidos, sufrió un ataque de ransomware. Este secuestro de información desembocó en la paralización de todas las operaciones de la compañía, encargada del transporte de 2,5 millones de barriles al día y 8.850 kilómetros de oleoductos gestionados, principalmente para abastecer a los grandes núcleos de población del este y el sur del país. El resultado fue una subida del precio del crudo del 4% el domingo, y un 1,5% el lunes por la mañana. (...)DarkSide, uno de los principales grupos de ransomware actuales, ha recibido finalmente 75 bitcoin, lo que equivale a aproximadamente 5 millones de dólares. "Somos apolíticos", aseguran los asaltantes en un comunicado. "Nuestro objetivo es ganar dinero y no crear problemas para la sociedad"." Acceso web 2023, https://www.expansion.com/economia-digital/innovacion/2021/05/14/609d58bbe5fdea3d448b461e.html

Debiendo apoyar su trabajo en el Derecho Internacional, fortaleciendo confianza y capacidades dentro los Estados para el uso seguro de las TIC y bases de datos. Por lo que el grupo de composición abierta, en 2023 ha realizado por lo menos cinco sesiones y ha presentado en julio/2023 su segundo informe anual[20].

Lo relevante de la iniciativa, según reporte de Microsoft[21], fue la presentación en abril 2021 del grupo formado a partir de consensos abiertos a los 193 Estados miembros. Se destaca que las reglas cibernéticas de la ONU se manejaron en círculos reducidos, con acuerdos alcanzados luego de más de cinco años con reglas de comportamiento responsables en Internet, a pesar de que los ataques se fueron incrementando, son más sofisticados y genera conflicto entre la población y sus Estados.

Algo valioso para las organizaciones no gubernamentales y empresas, es la apertura del grupo de composición abierta, a que las primeras participen de las iniciativas y labores encomendadas para la construcción de reglas y normas enfocadas a fortalecer la ciberseguridad, expandiendo a que actores de la sociedad civil y empresarial, sean relevantes en la construcción de las mismas y ya no sólo los respectivos Estados a través de sus gobiernos de turno.

Los conflictos en el espacio cibernético no están sujetos a los del tipo físico, por lo que involucran a diversidad de sectores y es responsabilidad de toda su protección, siendo la mayoría actores pertenecientes al sector no gubernamental.

Además, el grupo de trabajo de composición abierta para las TIC, al margen de inclusivo, impulsa la utilización del Derecho Internacional como herramienta normativa en el uso del ciberespacio, junto al diseño e implementación de reglas de comportamiento responsable, con base en principios y acuerdos asumidos en 2015[22], a partir de los trabajos realizados por el "Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el contexto de la Seguridad Internacional", publicado mediante Resolución de Asamblea General A/70/174, que emitieron las denominadas "Normas, reglas y principios de comportamiento responsable de los Estados".

Esto significa, que los Estados cuentan con normativa internacional sobre el uso del ciberespacio de forma responsable, las prohibiciones y observaciones a ciberataques sobre infraestructura

---

[20] *ONU. (2023). A/AC.292/2023/L.1. Proyecto del segundo informe anual sobre los progresos realizados del grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso (2021-2025). Siendo un proyecto de informe, se hizo punteo de su posible contenido, relevando resultados sostenidos con la Academia de los Estados, grupos civiles y diversos actores como empresas y organizaciones no gubernamentales, con resultados de los debates que se fueron llevando a cabo a la cabeza de su presidenta. Acceso web 2023, https://digitallibrary.un.org/nanna/record/4015764/files/A_AC.292_2023_L.1-ES.pdf?withWatermark=0&withMetadata=0&version=1&registerDownload=1*

[21] *O´Sullivan, K. (2021). MICROSOFT. La ONU logra avances importantes en ciberseguridad. Acceso web 2023, https://news.microsoft.com/es-xl/la-onu-logra-avances-importantes-en-ciberseguridad/*

[22] *ONU. (2015). Resolución A/70/174. Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional. Acceso web 2023, https://undocs.org/A/70/174*

critica, la cooperación que deberá existir entre equipos de respuesta de incidentes informáticos, así como entre los Estados para afrontar los ataques o emergencias resultantes de las TIC.

Se promueve la utilización del Derecho Internacional sobre las TIC, en base a la Carta de Naciones Unidas, observando la soberanía e independencia de los Estados, con reconocimiento a la jurisdicción que poseen estos sobre las infraestructuras de las TIC en el interior de su territorio, el respeto a la soberanía de los demás Estados y la no intervención en asuntos internos de sus pares, respeto a los DDHH y libertades fundamentales, así como el cumplimiento al Derecho Internacional e inmanente para el bien común de la humanidad, así como el uso pacífico de las TIC.

Adicionalmente, se reconocen Principios Internacionales que son jurídicos, tales como: Principio de humanidad, Principio de necesidad, Principio de proporcionalidad y el Principio de distinción. Estos últimos también parte del Derecho Internacional Humanitario.

Lo relevante de la resolución A/70/174, introduce la prohibición de tercerías utilizadas para cometer ilícitos vinculados a las TIC, pues los Estados deben establecer prohibiciones para que terceros no estatales y por ende tampoco gubernamentales, actúen al interior del territorio del Estado receptor. Siendo susceptibles de imputaciones en base al propio Derecho Internacional, con la observación que la dificultad estará en la comprobación y debida fundamentación de las acusaciones a tratarse contra el supuesto Estado infractor. Generándose el problema de la carga probatoria y su respectiva valoración y verificación.

Lo que si queda fortalecido es que las TIC y los espacios donde se desarrollan deben ser abiertos, pacíficos, estables, accesibles, seguros y debe promoverse su uso de forma responsable.

Dentro las conclusiones del documento, observa el aumento de la Cooperación Internacional como base para promover entendimientos sobre los riesgos y amenazas que implican el uso de las TIC con fines ilícitos, con posibles afectaciones a la paz y seguridad, así como afectaciones a las infraestructuras críticas de los Estados. En el grupo de expertos participaron alrededor de veinte Estados con sus respectivas delegaciones de especialistas.

Retornando, al grupo de trabajo de composición abierta, si bien se apoya en la resolución arriba descrita, dentro sus avances se destaca también: 1) la necesidad de proteger infraestructura crítica como la hospitalaria, frente a ataques producidos durante la pandemia[23]; 2) protección a las cadenas de suministros de las TIC, como actualizaciones de SW a componentes de los propios sistemas TIC; 3) la necesidad que los Estados cumplan con los compromisos y realicen inversiones en ciberseguridad, con atención de los países emergentes.

---

[23] *O´Sullivan, K. (2021). MICROSOFT. La ONU logra avances importantes en ciberseguridad. Sullivan dice: "Segundo, reconoce una necesidad de proteger la atención médica de los ciberataques, incluidos los servicios y las instalaciones médicas. En medio de la pandemia global en curso, estos ataques se han dirigido a hospitales y organizaciones de atención médica en los Estados Unidos y organizaciones en todo el mundo, incluido el Hospital Universitario de Brno en la República Checa, el sistema hospitalario de París, los sistemas informáticos de los hospitales en España, hospitales en Tailandia, e incluso organismos internacionales como la Organización Mundial de la Salud."Acceso web 2023, https://news.microsoft.com/es-xl/la-onu-logra-avances-importantes-en-ciberseguridad/*

Todo lo que está desarrollando la ONU, servirá para analizar lo que acontece con respecto a los ciberataques y variantes, observando hechos suscitados de relevancia internacional y lo que transcurre a partir de los conflictos armados en progreso.

3. *ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE (OTAN)*

La OTAN, según se describen[24], es una OI establecida entre Norteamérica y países europeos, con el propósito de fortalecer cooperación entre los países integrantes dentro del campo de la seguridad y defensa, así como la realización de actividades conjuntas dirigidas a gestionar crisis.

Su operación se apoya en la doctrina de la DEFENSA COLECTIVA, lo que significa que actúan bajo el principio de que un ataque contra uno o varios de sus miembros es considerado como un ataque contra todos. Establecido en el Art. 5 de su Tratado fundacional, denominado "Tratado del Atlántico Norte[25]", constituyendo el eje con el que la OTAN interactúa con sus miembros y se presenta ante el mundo para confrontar posibles amenazas.

Si bien el instrumento internacional, cuenta con 14 artículos, reconociendo la Carta de Naciones Unidas y su aplicación en caso de posibles conflictos, donde su resolución se realizará utilizando mecanismos de solución de conflictos pacíficos y de esa forma evitar que seguridad, paz y justicia internacionales, sean comprometidas, no pudiendo utilizar la amenaza ni el empleo de la fuerza en sus relaciones internacionales.

El Tratado se revisa cada diez años, para efectos de actualización de los objetivos estratégicos de la OI; posterior a los veinte años dentro del Tratado, cualquiera de los países que haya sobrepasado ese tiempo podrá interponer denuncia al Tratado de la OTAN luego de pasado un año más a dicho espacio de tiempo.

El Tratado de la OTAN, entró en vigencia el 24 de agosto de 1949 y se remitió copia legalizada a los países miembros del mismo.

De lo descrito, la OTAN, es un OI enfocada en la seguridad, defensa y atención de crisis, constituyendo una del tipo militar principalmente, creada bajo la Alianza de dos continentes y la necesidad de defensa ante posibles ataques armados. Emergiendo a través del instrumento internacional constitutivo, sobre la base de la Carta de Naciones Unidas y dentro de este el Art. 51, derecho inmanente a la legítima defensa individual o colectiva, frente a ataques armados.

Norma que se adoptó y se adaptó a las características de su norma de nacimiento. La cual representa la piedra angular sobre la que se desarrolla y se expande dicha OI, nacimiento que tuvo inicialmente a diez (10) Estados y para 2023 a treinta y un (31), en el que Macedonia del Norte en 2020 y Finlandia en 2023 fueron los últimos en integrarse a dicha organización.

La adhesión a la OTAN, se apertura a cualquier Estado europeo comprometido con la seguridad y principios establecidos por la organización. Apoyados en capacidades políticas y militares, que defiendan la libertad de sus miembros, su interacción entre los mismos apoyados en la

---

[24] *OTAN. (2023). El vínculo trasatlántico. Acceso web 2023, https://www.nato.int/nato-welcome/index_es.html*

[25] *OTAN. (2023). Tratado del Atlántico Norte. Washington DC – 4 de abril de 1949. Acceso web 2023, https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es*

cooperación y la consulta en temas de seguridad y defensa, mitigar problemas o conflictos, apoyados en la construcción de confianza.

En lo militar, la OTAN observa que deben agotarse los mecanismo de solución pacífica de conflictos, buscando y promoviendo la paz, siendo la participación bélica ultimo ratio cuando falla la diplomacia, actuaciones militares que se desarrollaran cumpliendo el Art. 5 de defensa colectiva de su Tratado, con la opción de recibir mandato de NNUU, pudiendo ser sus actuaciones individuales o de forma coordinada con otros Estados y OI.

OTAN, sólo ejecuto el Art. 5 de defensa colectiva en 2001 frente a los ataques terroristas contra Estados Unidos, por lo que siguen estrictamente protocolos de seguridad y actuación en casos debidamente justificados.

Para eso, la OTAN, establece los denominados "Conceptos Estratégicos", que son lineamientos sobre los que realizaran actuaciones como organización, fijando objetivos estratégicos y políticas de seguridad que den respuesta a los desafíos que confronta la Alianza, ante los cambios y evoluciones que se produzcan en el entorno. Razón por la que cada década se fijan estos y durante ese periodo se van fortaleciendo y adaptando acorde a sus necesidades de protección y seguridad, en base a experiencias alcanzadas y acumuladas.

Los "Conceptos Estratégicos", se dividen en tres grupos: 1) disuasión y defensa; 2) prevención y gestión de crisis; 3) seguridad cooperativa.

Cuando se habla de gestión de crisis[26], deberá entenderse que bajo el concepto de la OTAN podrá comprender la asunción de medidas del tipo militar y no militar, durante todo el ciclo de atención que se pueda producir, vale decir, antes de la crisis (prevención), durante la crisis (atención) y después de la crisis (posconflicto). Todo esto llevado adelante por el Mando Militar Integrado y experticia acumulada por la OI.

Para la OTAN, cualquier atención o gestión de crisis, debe realizarse a partir de tres ejes, participación política, civil y militar; pues, en base a experiencia de la propia Alianza las fuerzas armadas o ejército por sí sólo no podrán resolver el conflicto o la crisis, requiriéndose la participación de diversos actores de forma coordinada en la solución.

La gestión de crisis de la OTAN, no sólo se enfoca a la atención de conflictos apoyado en el Art. 5 de defensa colectiva, también actúa a favor de socios y otros Estados en situación de crisis por fenómenos naturales, crisis tecnológica y crisis humanitaria.

El enfoque del Concepto Estratégico 2022 de la OTAN, se dirige a la prevención de la crisis, fortaleciendo capacidades en base a experiencias acumuladas en las últimas tres décadas, no sólo militares, también de coordinación militar-civil; además, dentro la doctrina del ultimo Concepto se enfocará en la preparación para crisis alimentarias, sanitarias, derivadas del cambio climático y

---

[26] *OTAN. (2023). Gestión de crisis. Actualizado al 07 de julio de 2022, en su presentación se destaca: "Las sólidas capacidades de gestión de crisis de la OTAN le permiten hacer frente a una amplia gama de crisis, que podrían representar una amenaza para la seguridad del territorio y las poblaciones de la Alianza. Estas crisis pueden ser políticas, militares o humanitarias, y también pueden surgir de un desastre natural o como consecuencia de disrupciones tecnológicas." Acceso web 2023, https://www.nato.int/cps/en/natohq/topics_49192.htm*

seguridad humana, no hablando sólo de atención humanitaria, sino de enfocar esfuerzo en el humano como tal, tanto en la prevención como en la atención o gestión de crisis.

La OTAN utiliza para la toma de decisiones de gestión de crisis organismos de decisión apoyados en diferentes Comités y un Consejo, siendo el Consejo del Atlántico Norte (NAC, por sus siglas en inglés), el de toma de decisiones política, intercambiando información, inteligencia, datos, percepciones y apoyándose en el consenso de sus miembros.

El NAC, interactúa con diversos Comités para asumir decisiones: Comité de Política Operativa, Comité Político, Comité Militar, Comité de Resiliencia, Sistemas de Comunicaciones de la OTAN, Centro de Situación (SITCEN). Todos ellos actúan de forma dinámica, recibiendo información e inteligencia 24/7/365.

Respecto a la operatividad de la gestión de crisis, se apoya en el Sistema de Respuesta a Crisis (NCRS), que consiste en el proceso interno de la OTAN para coordinar con diversos actores la gestión de crisis en función de la fase o etapa que corresponda, realizando tareas adicionales de planificación antes de la intervención. El protocolo se revisa de forma anual.

En el sistema NCRS, se debe identificar la fase correspondiente antes de atender la crisis, para esto utiliza el Proceso de Gestión de Crisis de la OTAN. Se usan procedimientos de estandarización y logístico, para que los recursos destinados a la gestión de crisis sean debidamente utilizados y asignados. Tanto la coordinación con diferentes actores internacionales, como la preparación del personal civil, son tareas focales para las gestiones de crisis de forma eficiente.

La Gestión de Crisis de la OTAN, se realizará en base a dos enfoques, la primera actuar apoyados en el Art. 5 de Defensa Colectiva y la segunda, las no previstas en dicha norma. Esta última se dividirá en diversas acciones tales como: mantenimiento, establecimiento, consolidación, imposición de la paz, operaciones humanitarias y prevención de crisis. Acciones que se realizarán como apoyo a la ONU o a Estados soberanos que lo soliciten.

Denotando de esta manera, que OTAN, cuenta con diversidad de organismos, sistemas, protocolos de actuación, objetivos, políticas de acción no sólo para gestionar crisis, también conflictos armados y no armados, así como de cooperación y ayuda humana.

3.1 OTAN Y CIBERDEFENSA

Para la OTAN, la ciberdefensa[27] es prioritaria, definiendo que las guerras y conflictos hoy en día no se desarrollan solamente en los tres espacios tradicionales mar, aire y tierra, insertándose uno nuevo el ciberespacio.

La relevancia de esta concepción es la identificación hace muchos años de una realidad que fue demostrando a lo largo del tiempo que va de la mano de la revolución industrial 4.0 o digital, con avances significativos en el campo de las TIC, como la Inteligencia Artificial (IA), las

[27] *REAL INSTITUTO EL CANO. (2014). La OTAN y la ciberdefensa. Acceso web 2023,* https://www.realinstitutoelcano.org/blog/la-otan-y-la-ciberdefensa/

computadoras cuánticas, las conectividad satelital de tipo comercial y muchos otros como la cibernética.

Como se explicó, para la OTAN, las actuaciones que asume se apoyan en sus Conceptos Estratégicos, que fijan objetivos dentro de la década y estos se van potenciando con medidas tendientes a fortalecerlas a favor de sus Estados miembros y la propia OI.

La ciberdefensa para la OTAN, no es reciente y tiene experiencia en el área, incorporándola dentro de sus políticas a partir de 2002 en la Cumbre de Praga[28], con un hito relevante suscitado en 2007 en Estonia, que generó atención para la OI y profundizo en sus acciones en esta área.

En 2008, se presentó la primera Política de Ciberdefensa de la OTAN. Luego en la Cumbre de Lisboa de 2010 se incorporó la ciberdefensa dentro del Concepto Estratégico de la OI, realizando actualizaciones en 2011 y en 2012 la implementación de un Plan de acción complementario.

2011, fue también importante para el área de estudio para la OTAN, pues se estableció la iniciativa "Smart Defence" o Defensa Inteligente, presentado por el Secretario General de OTAN en febrero de 2011, el Sr. Anders Fogh Rasmussen[29]; incorporando la ciberdefensa en la cumbre de Chicago de 2012 dentro la mencionada iniciativa.

Concepto que busca la cooperación entre los Estados para construir seguridad, sin redundar en esfuerzos o solapamientos de manera tal que los alcances estén coordinados y se optimicen recursos y labores realizadas entre ellos.

Francia, como parte de la OTAN, decidió invertir alrededor de 1,500 MM de euros en actualizar sus sistemas TIC, priorizando sus capacidades de ciberseguridad y ciberdefensa. Hecho que reafirmaba la decisión asumida por los Ministro de Defensa de la OTAN para que los Estados mejoren su defensa en esta área.

Para 2014, en la Cumbre de Gales, se actualizo la política y mejoró. Lo relevante fue la extensión de la aplicación del Art. 5 al campo de la ciberdefensa, pues establece que un ataque digital relevante a uno de los Estados miembros podría entenderse como extensión de la referida norma.

En 2016, la OTAN, durante la Cumbre de Varsovia establece que el ciberespacio es un área de operaciones, con compromisos orientados a potenciar la cooperación en el campo de la ciberdefensa, reforzando el trabajo y coordinación OTAN-UE.

Para 2014, el Comité de Planificación y Política de Defensa para la ciberdefensa, se convierte en el Comité de Defensa Cibernética (CDC), convirtiéndose en asesor superior del Consejo del Atlántico Norte en temas de ciberseguridad, constituido en consultor para Estados aliados y responsable de la ciberdefensa de la OTAN.

---

[28] *CCDCOE-OTAN. (2023). Organización del tratado del atlántico norte. Acceso web 2023, https://ccdcoe.org/organisations/nato/*

[29] *OTAN. (2023). Discurso sobre la Iniciativa de Defensa Inteligente de la OTAN por el Secretario General Adjunto de la OTAN, Embajador Claudio Bisogniero, en Tallin, Estonia. Actualizado en 2012. Acceso web 2023, https://www.nato.int/cps/en/natolive/opinions_83096.htm?selectedLocale=en*

Para 2018, ministros de los Estados de la OTAN, acuerdan el establecimiento de un Centro de Operaciones Cibernéticas, debiendo integrarse de manera transversal a la planificación y operaciones de la OI.

Siguiendo sus políticas, OTAN, el Consejo del Atlántico Norte, ejerce tuición y autoridad en caso de ataques importantes, siendo la cabeza en gestión de crisis vinculadas a la ciberdefensa.

Luego, existe la Junta de Gestión de Ciberdefensa (CDMB), supeditada a la División de Desafíos de Seguridad Emergentes, que a su vez está integrado por representantes de entidades OTAN, relacionadas con la ciberseguridad: Mando Aliado de Transformación, agencias OTAN, Mando aliado de Operaciones.

La Junta CDMB, coordina con los Estados miembros para el intercambio de información, los asiste técnicamente, elabora los planes estratégicos y está a cargo de la redes de la OTAN.

Además, existe una Junta de Consulta, Control y Comando de la OTAN (NC3), que es relevante para la OI, pues es el ente de consulta para la implementación y observación de temas técnicos relacionados con la ciberdefensa de la OTAN.

Con respecto a la Capacidad de Respuesta de Incidentes Informáticos de la OTAN (NCIRC), es parte de la CIA, está a cargo de la protección técnica de los denominados ciberactivos de la OTAN, operando de forma centralizada y operando completamente desde 2014.

También, la OTAN, cuenta con un Centro de Excelencia Cooperativa de Ciberdefensa (CCDCOE), dedicado a la investigación y capacitación, cuya operación es académica e investigación en el campo de la ciberseguridad, recibiendo apoyo de más de 22 Estados. Brindando soporte a requerimiento de la OTAN y no formando parte de su estructura.

El Centro CCDCOE, es reconocido por el sector, goza de alto prestigio, habiendo publicado en 2009 el Manual de Tallin con la participación de juristas o abogados de más de 50 países. En 2017 publicaron la actualización de otra publicación de 2013, denominado: “Manual de Tallin 2.0 sobre el derecho internacional aplicables a las operaciones cibernéticas”. Para 2020 el CCDCOE fortaleció vínculos con más de 28 Estados de la OTAN y aliados.

Observando la organización de la OTAN en cuanto a la ciberseguridad, ciberdefensa y ciberataques, ha desplegado varios entes internos y externos vinculados a las áreas de interés con el objetivo de fortalecer sus propias capacidades y las de sus Estados miembros, dentro de un campo de operaciones que ha trascendido a la virtualidad pero que tiene repercusión sobre infraestructuras y sistemas altamente críticos, muchos de ellos del tipo militar.

Al igual que en la ONU, para la OTAN, la cooperación, la coordinación, el intercambio y trabajo conjunto de sus Estados miembros, en la atención a la ciberdefensa como parte de su política de seguridad, incorporada dentro de su objetivos a través de sus Conceptos Estratégicos, demuestran que para dicha OI, el tema es extremadamente relevante.

Dentro sus prácticas y ejercicios militares, también la OTAN ha desarrollado desafíos y simulaciones que convocan a especialistas de sus países miembros y aliados, dirigidos a comprobar sus capacidades y detectar nuevos desafíos que deben asumirse en búsqueda de la

mejora de sus sistemas. "Locked Shield"[30], es ejemplo de los mismos, en el que en 2023, participaron más de 2600 personas de 38 países, en acciones destinadas a dar respuesta a ataques y reaccionar en tiempo real frente a estos en diferentes niveles y rubros, enfocados a la gestión de crisis de la ciberdefensa.

Para 2023 la OTAN a través de su Secretario General, el Sr. Jens Stoltenberg[31], en la reunión de políticos, militares y técnicos de aliados, durante la Conferencia anual de ciberdefensa, emitió su discurso haciendo un diagnóstico de lo que acontece en el mundo[32]. Lo más destacable y a manera de resumen en base al discurso leído, fue:

a) El posicionamiento de la OTAN como experto para la defensa en el ciberespacio, contando con experiencia, innovación, información y capacidades de coordinación colectiva.
b) El desafío contra la OTAN de Estados autoritarios, incluidos China y Rusia, que desafían la seguridad de la OI, incluyendo sus valores e intereses; promoviendo la competencia estratégica, según se entiende del discurso del autor. Países autoritarios, que además, actúan con el propósito de transformar el ciberespacio como extensión de sus Estados, basados en la falta de transparencia e irrespeto por los DDHH, también expresado por el autor.
c) Independencia que debe existir sobre la adquisición de suministros de equipamiento proveniente de países autoritarios, con el objetivo de construir su propia estructura digital para el futuro. Buscando proteger mejor a su población y redes tecnológicas.
d) OTAN debe trabajar y coordinar con la industria y sector privado, sin los cuales no habrá defensa, ni disuasión, ni seguridad.
e) La guerra Rusia contra Ucrania, ha relevado el uso del ciberespacio en los conflictos modernos.
f) OTAN, cuenta con equipos de reacción rápida, así como Centros de operaciones en el ciberespacio. Enfocados a prestar soporte y ayuda a sus Aliados.
g) Se debe persuadir de mejor forma los ciberataques y asumir defensa cuando surjan. Con el mensaje que si la OTAN es atacado habrán consecuencias.
h) Militarmente defender el ciberespacio propio de la OTAN, poseer capacidades operativas cibernéticas defensivas y ofensivas.
i) La necesidad de desarrollar sistemas de comunicación segura, incluidas la redes 5G.
j) Dada la experiencia de la dependencia de Rusia en cuanto a la energía, en base a esa experiencia se debe evitar depender de China para la provisión de redes críticas.

---

[30] *CCDCOE. (2023). En la página de descripción del Locked Shield, se lee: "Se trata de un ejercicio de Equipo Rojo vs. Equipo azul, donde estos últimos están formados por naciones miembros del CCDCOE. En 2021 participaron 22 Equipos Azules con un promedio de 40 expertos en cada equipo. Los equipos asumen el papel de equipos nacionales de reacción rápida cibernética que se despliegan para ayudar a un país ficticio a manejar un incidente cibernético a gran escala con todas sus implicaciones.". Acceso web 2023, https://ccdcoe.org/exercises/locked-shields/*

[31] *OTAN. (2023). Secretario General: A través de la OTAN, podemos construir un ciberespacio seguro para todos. Acceso web 2023, https://www.nato.int/cps/en/natohq/news_219850.htm?selectedLocale=en*

[32] *OTAN. (2023). Discurso por el Secretario General de la OTAN, Jens Stoltenberg, en la primera Conferencia anual de Ciberdefensa de la OTAN. Acceso web 2023, https://www.nato.int/cps/en/natohq/opinions_219806.htm?selectedLocale=en*

k) El sector privado ha demostrado su valía y ser actores relevantes, volviéndose críticos en el conflicto de Ucrania, con apoyo de empresas como Microsoft, Starlink y Amazon. Por lo que para la OTAN la alianza con el sector privado es de alta prioridad.
l) El objetivo es que entre todos los países de la OTAN, se construya una ciberseguridad propia y se proteja a los más de 1000 millones de habitantes que pertenecen a sus Estados miembros.

Reflejando, con el punteo superior, no sólo el discurso brindado por el Sr. Stoltenberg, a través del mismo también la visión y postura de la OTAN frente a los ciberataques, la ciberseguridad y sobre todo la ciberdefensa en la actualidad. Lo que denota la búsqueda de independencia tecnológica de países conflictivos o que representan amenaza, que pese a mantener posturas contrarias a las de la propia organización, poseen recursos que son utilizados comercialmente y recaudan fondos de los países que no comulgan con sus posturas ni ideologías; lo que genera tensión entre la OTAN y los países observados por esta y sus Estados miembros.

4. *UNIÓN EUROPEA (UE)*

Regionalmente la Unión Europea (UE) ha establecido diversas políticas que logró establecerlas en normas de orden jurídico, apoyados en el Derecho Internacional y la fortaleza que poseen a partir de su composición interestatal. Son sin duda guías y bases para muchos países en diferentes continentes, que sin ser parte de la Unión, adaptan las mismas acorde a sus necesidades o las utilizan como marcos de referencia en la construcción de sus propias normas.

En el campo de ciberseguridad, la UE fue liderando la regulación legal del sector, en 2001 generó el Tratado de Budapest, conocido como el Convenio sobre la Ciberdelincuencia de Budapest[33] de 23 de noviembre de 2001. Instrumento internacional para la protección a la sociedad en general contra delitos cometidos en Internet e informáticos, tipificando delitos y estén armonizados a las normas sustantivas penales de los respectivos Estados, de manera tal de que los ilícitos sean investigados, procesados, sancionados y sirvan para determinar vínculo con otros delitos en el que se haya utilizado medios informáticos para su comisión.

La base de dicho convenio es la cooperación internacional, pues sin esta se dificulta la labor de los respectivos Estados y la búsqueda de lucha efectiva contra nuevas variantes de actos delictivos que se cometen en espacios virtuales, que no cuentan con fronteras y la comisión de los mismos por los medios utilizados dificulta repetitivamente la identificación de autores, cómplices, encubridores, instigadores y ubicación de los mismos.

Es importante comprender que los delitos informáticos o sus afectaciones a intrusiones a partir del uso de las TIC no son recientes; lo relevante, es el incremento y masificación de los medios tecnológicos por los que miles de millones de usuarios en todo el mundo acceden a estos de forma cotidiana, lo que proporcionalmente repercute en el incremento de los delitos.

Se considera importante del referido Convenio de Budapest de 2001, el énfasis que aporta a la protección y manejo de datos personales, que junto a la observación al Derecho Internacional,

[33] *Organización de Estados Americanos. (OEA, 2001). Convenio sobre la ciberdelincuencia. Budapest, 23.XI.2001. Ed. Council of Europe. Serie de Tratados Europeos No. 185. Acceso web 2023, https://www.oas.org/juridico/english/cyb_pry_convenio.pdf*

derechos fundamentales y DDHH, encuadran la norma en directrices guías a ser asumidas por los diferentes Estados.

Si bien, como toda norma, será siempre perfectible, el hito de dicho instrumento fue no sólo el reconocimiento creciente de las actividades en el ciberespacio con fines ilícitos, también la decisión de los Estados de encarar el problema y brindar directrices en la armonización para que las actividades observadas estén reguladas y así buscar la forma de restringirlas.

Los problemas generados por el uso de las TIC, no sólo es a partir de usuarios civiles, también corporativos e incluso los propios Estados que cuentan con los recursos necesarios para realizar tales fines. Al ser un espacio cuya generación probatoria requiere también de especialistas, la aplicación de normas no siempre responderá a la realidad, constituyendo otra situación a valorar.

4.1 UNIÓN EUROPEA Y CIBERDEFENSA

Para la UE la defensa es una preocupación constante, luego de la segunda guerra mundial y las repercusiones que produjo, han impulsado a que los Estados de la Unión reconstruyan y desarrollen sus capacidades enfocadas más en el desarrollo país antes que en incidir en la defensa, apoyándose además en la OTAN, los países que accedieron a la misma.

Los recientes acontecimientos que se van produciendo en el mundo, ha impulsado que la UE establezca un plan enfocada en la política de seguridad y defensa hasta 2030, a través de la iniciativa denominada "Brújula Estratégica"[34], buscando en esencia reforzar e incrementar sus capacidades defensivas y de ataque ante posibles conflictos en su territorio, a partir del desarrollo de autonomía por parte de la Unión para asumir políticas y medidas estratégicas que tiendan a dotarle de seguridad y defensa estable a favor de su población y respectivos Estados.

La iniciativa decenal, se apoya en cuatro ejes[35]: actuar, trabajar de manera asociativa, invertir, garantizar la seguridad.

Actuar[36], representa el eje de respuesta rápida de la UE en caso de conflictos, gestionando la crisis con el despliegue de hasta cinco mil (5000) efectivos militares, que actuaran para diversos tipos de crisis y la Unión deberá crear y contar con dicha capacidad.

Además, tendrá capacidad de despliegue de una misión civil compuesta por doscientos (200) expertos en un lapso de treinta (30) días, equipados plenamente y que respondan a su política

---

[34] *Unión Europea. (UE, 2022). Consejo De la UE, resolución 7371/22 de Bruselas, 21 de marzo de 2022. "A Strategic Compass for Security and Defence For a European Union that protects its citizens, values and interests and contributes to international peace and security". Acceso web 2023, https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf*

[35] *REAL INSTITUTO EL CANO. (2022). NOVEDADES EN LA RED, Nº 853: LA BRÚJULA ESTRATÉGICA DE LA UE. Acceso web 2023, https://www.realinstitutoelcano.org/novedades-en-la-red/novedades-en-la-red-no-853-la-brujula-estrategica-de-la-ue/*

[36] *Consejo de la UE. (2022). Una Brújula Estratégica para reforzar la seguridad y la defensa de la UE en el próximo decenio. Acceso web 2023, https://www.consilium.europa.eu/es/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/*

común de seguridad y defensa (PSCD). Deberá desarrollarse el eje, además, con la realización de ejercicios reales en mar y tierra. Observando que deberá incrementarse su movilidad militar, protocolos de respuesta agiles y flexibles, con participación de misiones militares y civiles a cargo del PSCD, todo con apoyo de su Fondo Europeo de Apoyo a la paz.

El eje Trabajar de manera asociativa, busca de manera coordinada en base a cooperación con OTAN, ONU y socios regionales como ASEAN, OSCE o la Unión Africana, confrontar amenazas y desafíos comunes que les atinjan.

Para fortalecer dicho eje, se buscaran también alianzas bilaterales con países como USA, Japón, Reino Unidos, Canadá y Noruega. Buscando sociedades a partir de sus ejes y objetivos con Estados de diferentes regiones, cuyas bases serán el dialogo y la cooperación.

El eje Invertir, como su nombre lo indica se enfoca en incrementar la inversión en el campo de la defensa de la Unión, de esa forma se eleven las capacidades militares y civiles, fortalezcan su base industrial y tecnológica de la Unión en sector defensa, buscando optimizar recursos económicos, desarrollando proyectos colaborativos entre los Estados con inversiones enfocadas a desarrollar capacidades de nueva generación y apoyo estratégico en escenarios terrestres, marítimos, aéreo y cibernético.

Impulsando además la innovación tecnológica en el sector seguridad y defensa de la propia Unión, con el objetivo de desarrollar su propia industria y disminuir dependencias de medios tecnológicos de terceros.

El eje, Garantizar la seguridad, se enfoca en la anticipación o prevención, disuasión y respuesta frente a amenazas, desafíos latentes y conflictos súbitos que busquen afectar a la Unión. Para lo cual se recomienda incrementar las capacidades de análisis de inteligencia, desarrollo de equipos e instrumentos de respuesta contra amenazas hibridas.

Además, dentro del eje, se establece el desarrollo de instrumentos dirigidos a la ciberdiplomacia y la política de ciberdefensa de la Unión, para contar con capacidades mejoradas de confrontación ante posibles ciberataques. De esa forma contar con herramientas que eviten la injerencia y manejo de información por parte de agentes extranjeros.

También, el desarrollo de la estrategia espacial de la UE destinadas a la seguridad y defensa, así como el reforzamiento de las capacidades de seguridad de la propia Unión en el sector marítimo.

De manera similar a las otras OI descritas, la UE dentro del marco de la seguridad y defensa reconoce y establece la existencia ya no de tres espacios tradicionales solamente, incluye el cuarto referido al ciberespacio.

La necesidad de enfrentar los problemas que surgen en el ciberespacio, han sido trasladados al desarrollo de la Unión vinculados tanto a suministro de infraestructura física y virtual, siendo fundamental si se busca en compatibilidad con la OTAN, desvincularse de suministros asiáticos principalmente; siendo China muy probablemente líder en provisión de componentes y partes que integran los sistemas informatizados que usan dentro la Unión, sin obviar la dependencia casi mundial que existe de Taiwán referente a microprocesadores y otras componentes, país amenazado y asediado estos últimos años de manera más intensa por parte de China, generando tensión en el área geográfica y la preocupación sobre suministros a nivel global.

La iniciativa estudiada, Brújula Estratégica de la UE, no está cerrada, se irá actualizando luego de que pase por diferentes discusiones entre los Estados de la Unión, por lo que se espera que en los próximos años siga evolucionando y adaptándose a las demandas de los Estados miembros y lo que acontece en el entorno.

Entonces, para la UE se habla de trabajar en su defensa orientada a cinco escenarios o espacios de posibles amenazas y conflictos, debiendo desarrollar sus capacidades de reacción inmediata para actuar en caso de crisis, en la práctica los espacios no son cuatro para UE sino cinco: tierra, aire, marítimo, espacio y ciberespacio.

4.2 UNIÓN EUROPEA Y CIBERSEGURIDAD

Para la UE es fundamental actuar de manera multidimensional en el campo de la ciberseguridad, por lo que actúa en cuatro esferas[37]: 1) ciberresiliencia; 2) ciberdelincuencia; 3) ciberdiplomacia y 4) ciberdefensa.

Si bien, como lo reconoce el Consejo de la UE, la tecnología representa una herramienta valiosa para trabajar de forma conjunta en situaciones de crisis como la pandemia del coronavirus, la informatización de muchos recursos se han convertido por otro lado en amenazas, que deben ser atendidas de forma pertinente, estando inmersa la propia sociedad susceptible de sus posibles consecuencias, con posibles repercusiones en los sectores energéticos, financieros, sanitarios, políticos, socioeconómicos, seguridad y defensa en general.

El trabajo de la UE está orientado al fortalecimiento de su Unión y el bienestar de su población, por lo que si bien muchas políticas que adopta, no siempre responden de manera ágil a los acontecimientos que se suscitan, es innegable que la labor que realizan es primordial para sus sociedades, por lo que de forma activa sus órganos políticos trabajan en diferentes sectores, no estando exenta el de la ciberseguridad.

Proyecciones de la UE, dan cuenta que para el año 2025 existe la expectativa de conectividad de más de 41 mil millones de dispositivos a través de la IoT o Internet de las cosas, si observamos que la población mundial supera los 8 mil millones de habitantes, aproximadamente, representa que en promedio general cada persona llegará a contar con por lo menos 5 equipos conectados a través de la IoT. Representa y no de manera exagerada cinco posibilidades por persona a sufrir algún tipo de ciberataque en los próximos años de no asumir medidas al respecto.

Por otro lado, por lo visto hasta acá, las diferentes OI buscan equilibrar la seguridad con el uso, incidiendo en el uso del derecho internacional, en base a la cooperación internacional, para evitar restringir espacios y garantizar de forma libre el acceso de manera segura las TIC.

Si bien parece un juego de equilibristas, lo cierto es que el mundo observa más los derechos, pero al mismo tiempo no siempre los ejerce o ante la vorágine de información, no se presta atención a ellos, desde el acceso a páginas en línea con aprobaciones de cookies vinculadas a comunicaciones publicitarias, estudios de comportamiento, preferencias, ubicación y muchos otros versus derechos a la privacidad de sus datos, por establecer algún contraste contextual.

---

[37] *Consejo de la Unión Europea. (2023). Ciberseguridad: cómo combate la UE las amenazas cibernéticas. Acceso web 2023, https://www.consilium.europa.eu/es/policies/cybersecurity/#defence*

Para esto la UE, en octubre 2020, requirió a través de sus líderes que se prioricen políticas encaminadas a: la protección frente a las ciberamenazas, insertar encriptación cuántica para la protección de datos y navegación segura en Internet y por otro lado que las fuerzas de seguridad y judiciales tengan las garantías requeridas para poder acceder a los datos en casos de investigación.

En apariencia, si observamos lo requerido en párrafo anterior, sería algo coherente, pero desde el momento que se quiere asegurar datos y estos estén disponibles para las autoridades, representa que las restricciones son sólo para la mayoría de usuarios excepto las autoridades, generando la cuestionante de quién controlará las actividades de las mismas en caso de cometer posibles abusos y violentar la privacidad de las personas. Paralelamente, se habla de seguridad y vinculada a esta aparece también la defensa, lo que establece en apariencia un entorno complicado de regular.

La UE asumiendo su liderazgo, ya sea por necesidad o por presión de la propia realidad y su población comunitaria, a través de sus líderes, trabaja de forma activa al respecto, por lo que se observará descriptivamente las diversas acciones que realiza.

4.2.1 ACCIONES DE LA UE RESPECTO A LA CIBERRESILIENCIA

La UE cuenta con la denominada Estrategia de Ciberseguridad, iniciativa liderada por el Servicio Europeo de Acción Exterior (SEAE) y la Comisión Europea, con la misma se busca insertar normas encaminadas a la inversión y actuación, fortaleciendo la resiliencia de la Unión contra las nuevas amenazas, de forma que sectores productivos y civiles se beneficien con instrumentos digitales más seguros, confiables y acceso a servicios de igual forma.

Para la UE, según conclusiones de 2021 la Europa resiliente, ecológica y digital podrá lograrse a partir del fortalecimiento de la ciberseguridad en la región. Enfoque que busca por parte de líderes[38] la denominada autonomía estratégica, apoyada en la conservación de la economía abierta y la fortificación de los respectivos liderazgos y capacidades de la Unión en el entorno digital.

La UE cuenta actualmente con un Reglamento de Ciberresiliencia, tomando en cuenta la ciberseguridad, por lo que la adquisición y utilización de dispositivos informáticos, así como programas o aplicaciones (SW), están estandarizados a normas de ciberseguridad que deben cumplir, de esa forma se busca proteger y garantizar a su población en el uso de productos certificados por la UE que cumplan con sus regulaciones sobre el sector.

Dentro del reglamento, también se observan los dispositivos de uso común tradicionales como televisores inteligentes, equipos denominados de línea blanca o de uso doméstico, consolas de juego y video, cámara de seguridad, juguetes, etc.

De esa forma, se promueve la producción de la Unión, el cumplimiento de normas establecidas de ciberseguridad, el consumo de productos certificados con estándar único y uniforme de la

[38] *Consejo de la UE. (2023). Acceso web 2023, https://www.consilium.europa.eu/es/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/*

propia Unión, se garantiza cumplan con medidas de ciberseguridad y el acceso de forma libre al ciberespacio resguardando la seguridad de su población.

4.2.2 ACCIONES DE LA UE RESPECTO A LA CIBERDELINCUENCIA

Para luchar contra la ciberdelincuencia, se debe hablar necesariamente de ciberseguridad[39], la UE cuenta con su respectivo Reglamento sobre la Ciberseguridad de la UE, vigente desde 2019, ordenando un sistema de certificación para toda la Unión y nuevo mandato de la Agencia de la UE para la ciberseguridad.

La certificación única, busca establecer regular normativamente que servicios, productos y procesos vinculados a las TIC, cuenten con reglamentos uniformes, estándares mínimos a ser cumplidos por los países miembros y se logre fortalecer la ciberseguridad de la Unión, evitando las incompatibilidades entre normas y certificaciones asumidas por cada Estado.

El resultado de dichos esfuerzos se reflejan en el incremento de la ciberseguridad de la Unión, el comercio, la confianza y la expansión de mercado de la seguridad apoyado en estándares uniformes para todos los Estados miembros. Resultando en el denominado "Sistema europeo de certificación de ciberseguridad de la Comisión Europea[40]", que parametriza requisitos técnicos, reglas, procedimientos y normas relacionadas a la certificación.

También dicha iniciativa ha contribuido al incremento del mercado de la ciberseguridad, la expansión y crecimiento de sociedades mercantiles o empresas especialistas en el rubro, ingresos económicos a favor de los Estados miembros, mejoras en sus capacidades de respuesta, así como en la cooperación internacional entre países miembros y otros, estandarización de productos y procedimientos, así como de servicios y experticia a favor no sólo de su propia sociedad civil, también de sus capacidades de defensa.

Dentro la ciberseguridad europea, la "Agencia de la UE para la Ciberseguridad[41]", cumple un rol importante en el desarrollo de las políticas del Unión, pues habiendo heredado la estructura de la "Agencia de Seguridad de las Redes y de la Información de la UE", cuenta con un mandato permanente para asistir a sus Estados en temas de su esfera, confrontar ciberataques y apoyar a terceros interesados en el sector bajo demanda.

Con respecto a la legislación, en 2016 generó mandato de cooperación entre los Estados miembros de la Unión, destinadas a fortalecer capacidades en el campo de la ciberseguridad.

---

[39] *Ídem33. Para la UE, según su reglamento de sobre la ciberseguridad de la UE, define ciberseguridad de la siguiente forma: "¿Qué es la ciberseguridad? La ciberseguridad incluye las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de dichos sistemas y de otras personas afectadas por las ciberamenazas.- Reglamento sobre la Ciberseguridad de la UE".*

[40] *Idem33. El Sistema europeo de certificación de la ciberseguridad de la Comisión Europea, ha logrado el incremento de mercado de la ciberseguridad, por lo que declara: "El mercado de la ciberseguridad en la Unión. Entre los veinte primeros puestos del Índice Mundial de Ciberseguridad figuran dieciocho países europeos. El valor del mercado de la ciberseguridad en la Unión se estima en más de 130 000 millones de euros y está creciendo a un ritmo del 17 % anual. La UE cuenta con más de 60 000 empresas de ciberseguridad y más de 660 centros especializados en ciberseguridad."*

[41] *Ídem33. Acceso web 2023, https://www.enisa.europa.eu/*

Dicha legislación se destacó por insertar obligaciones de cumplimiento de seguridad a sectores críticos para la Unión, tales como: energía, sanidad, transporte, finanzas, proveedores de servicios digitales compuestos por mercados en línea, motores de búsqueda y servicios en la nube.

La legislación referida, recibió el nombre de "Directiva sobre la seguridad de redes y sistemas de información" (SRI), recibiendo actualización en 2022, denominada por sus siglas SRI2, abrogando la de 2016 y fortaleciendo los niveles de ciberseguridad al interior de la Unión. Se destaca en la actual legislación: el marco regulador establece nuevas normas mínimas a ser cumplidas en el sector, mejora las normas que impulsan la cooperación entre los Estados miembros, establece nuevo listado de actividades y sectores obligados a cumplir con regulaciones sobre ciberseguridad. Las SRI2[42] entró en vigencia en enero de 2023.

Con las herramientas normativas, entidades de la Unión y la estandarización exigida que cumpla con parámetros de ciberseguridad, descritas arriba, se ingresa a describir el fenómeno de la ciberdelincuencia, que busca cualquier resquicio de la seguridad para acometer sus actos, por lo que las normas estarán constantemente detrás de actos perpetrados por sujetos y organizaciones dedicadas a lo ilícito.

Según reporta la propia UE, el daño generado por la ciberdelincuencia, alcanza a nivel global la suma de más de 5,5 billones de euros anualmente, cuya generación de actividades es principalmente del tipo económico. El monto estimado no es un dato menor, pues no se refiere a cifras acumuladas en periodos de varios años, sino en doce meses, lo cual no sólo es alarmante, también denota la necesidad de fortalecer medidas dirigidas a su mitigación y de ser posible eliminación, aunque este último suene más a utopía y deseo que practicidad.

Es conocido que los delitos del mundo físico, se transportaron al mundo virtual, incurriendo en robo de recursos económicos, identidades, estafas, falsificaciones, apropiación de derechos de todo tipo sobre bienes materiales e inmateriales, con la innovación de haber establecido en mercados ilícitos en las denominada redes obscuras, cuyo comercio con fines netamente económicos no tiene límites para comercializar cualquier cosa – ejemplo, en el caso del ciberataque a la ONU se comercializó credenciales de un funcionario de dicha OI que repercutió en el acceso a su infraestructura informática y datos contenidos en ellas, explicado anteriormente -, el uso de redes sociales para la distribución de contenidos prohibidos o incitaciones con consecuencias dañosas, etc.

Sin mencionar, delitos del tipo sexual, venta de órganos, personas, tráfico ilegal de todo tipo, venta de datos y muchos más, que dan muestra que se debe confrontar con problemas que para la mayoría de la población es inimaginable, complicando aún más la actuación de los servicios estatales de seguridad y justicia.

La UE, para enfrentar el flagelo de la ciberdelincuencia creó el "Centro Europeo de la Ciberdelincuencia[43]", perteneciente a la EUROPOL. Además, la propia UE, por iniciativa de sus Estados miembros ha creado la "Plataforma multidisciplinar europea contra las amenazas

[42] *Ídem33.* https://www.consilium.europa.eu/es/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/

[43] *Ídem33.* https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

delictivas", denominada EMPACT, encargada de la detección y combate contra la delincuencia internacional organizada, priorizando los ciberataques.

Dentro de la lucha contra los ciberdelitos, aparece uno relacionado al fraude de pagos en línea, lo que representa que el crimen organizado obtiene recursos económicos derivados de dichos ilícitos, fortaleciendo no sólo sus recursos económicos, también su acceso a bienes de diversa naturaleza y expansión en territorios de su interés al contar con los medios para hacerlo.

El fenómeno es global, por lo que para la eurozona se adoptaron desde 2019 medidas encaminadas a endurecer las normas legales[44] que sanciones el fraude de pagos en línea, con aplicación de las mismas desde 2021.

Por otro lado, con respecto a la explotación sexual de menores en Internet y abuso sexual, la UE aún debate las normas al respecto, asumiendo de manera provisional autorizaciones para que los proveedores de servicios de email y mensajería en línea o web, detecten abusos sexuales contra menores, aprovechando para esto la Directiva sobre privacidad y las comunicaciones electrónicas, en los apartados 1 de los artículos 5 y 6 de la misma. La temporalidad de dicha medida está vigente desde 2021 y concluirá en 2024, o hasta que las nueva normativa específica sea aprobada en el Consejo.

Si bien aparentemente, los ciberdelitos descritos en esta sección suponen son aislados a los ciberataques y ciberterrorismo, la realidad denota que no es así, no debe soslayarse que para que los terroristas y sus organizaciones cuenten con recursos económicos, deben buscar formas de financiación a sus movimientos, no estando exentos de cometer los mismos para monetizar recursos económicos, así como obtener bienes de interés para su lucha, lo que genera círculos bastantes conflictivos de interoperación en el ciberespacio.

En este sector, si se busca sancionar la ciberdelincuencia y dado el respeto a los DDHH y Derechos Internacionales, la justicia y la policía, deben actuar en base a pruebas y evidencias, inclusive indicios que les remitan a las anteriores, lo que en el ciberespacio representa gran desafío para la obtención, procesamiento y custodia de los datos obtenidos.

Para el mundo físico, es un gran problema las cadenas de custodia, la pruebas y los medios probatorios utilizados en procesos jurisdiccionales, si se traslada al ciberespacio se transforma en desafíos pues deben recurrir a la cooperación internacional, generando acciones entre Estados para la obtención legal de las pruebas.

El uso de estas, se enfoca en la mensajería, contenido de imágenes y video, correos electrónicos, navegación por Internet, rastros digitales de acceso a lugares específicos en el ciberespacio y fuentes de emisión de transmisión, recepción de comunicación, etc. Lo cual es utilizado en los procesos judiciales y de investigación policial.

De esta forma la UE, está trabajando de forma estrecha con USA[45], para la elaboración de la segunda versión del Convenio de Budapest de 2001, establecimiento de acuerdos para el acceso a

[44] *Ídem33.* https://www.consilium.europa.eu/es/press/press-releases/2019/04/09/eu-puts-in-place-tighter-rules-to-fight-non-cash-payment-fraud/

pruebas electrónicas de proveedores norteamericanos y viceversa, buscando de esa manera el acceso de forma más expedita a la obtención probatoria requerida.

La conservación de datos y el cifrado, también constituyen interés para la comunidad mundial, no sólo europea, pues lo que se busca es establecer el equilibrio entre la seguridad de las comunicaciones de las personas y por el otro lado el acceso de cuerpos de seguridad de los Estados enfocados a la lucha contra el ciberdelito, ciberataque, ciberterrorismo, ciberactivismo y cualquier modalidad utilizada mediante las TIC para cometer actos que afecten la seguridad y la paz de sus sociedades; además, también genera un alto desafío el tema pues a veces son los propios Estados que contando con todos los recursos se convierten en los primeros agresores a las comunicaciones en contra de sus propias sociedades, con fines diversos, principalmente políticos.

De manera similar, la conservación de datos[46], genera otro conflicto para los Estados, no sólo los de la UE, pues los proveedores deberían conservar determinados datos para fines legales, surgiendo por lo menos dos problemas, el primero desde el punto de vista técnico referente a los medios y capacidades de almacenamiento, pues los datos se guardan en componentes físicos así se diga que se trabaja con servidores virtuales, que en la práctica son servidores físicos con acceso a Internet; el segundo problema, es de orden legal dado que dentro los DDHH y fundamentales de muchos Estados el derecho a la privacidad e intimidad son inalienables, generando otro problema de equilibrio y discusión entre sociedad, Estado y proveedores.

Surgiendo nuevamente la cuestionamiento sobre la relación con los ciberataques, ciberterrorismo, ciberguerra y ciberseguridad; respuesta que es obvia, pues lo que busca el terrorista es exigir que se respeten sus DDHH a la privacidad e intimidad, para sumergirse y ocultarse en el ciberespacio para cometer sus actos, obtener recursos para financiar su movimiento, captar nuevos seguidores o adeptos a su lucha, coordinar ataques en el mundo físico, ocultar su identidad, actuar aprovechando que no requiere estar en el lugar de objetivo para interactuar, cometer ilícitos en la web obscura, adquirir materiales de destrucción, comercializar moneda falsificada, traficar con sustancias y materiales ilícitos, obtener datos e información de relevancia para sus ataques y muchas actividades que son absoluta y definitivamente delictivas, que al ser cometidas en el ciberespacio se denominan ciberdelitos y al final el perpetrador busca la forma de eludir las justicia, las fuerzas de seguridad y continuar en el anonimato cometiendo sus actuados.

4.2.3 ACCIONES DE LA UE RESPECTO A LA CIBERDIPLOMACIA

Para la mayoría de los países firmantes de la Carta de las Naciones Unidas, siendo que es obligatorio para todos, el respeto a los DDHH es primordial para sus diversas actuaciones, en la que la UE es líder al respecto.

El ciberespacio para la UE debe ser libre, estable, seguro y abierto, con respeto del Estado de Derecho, derechos fundamentales, DDHH, en correlación a la protección, desarrollo, estabilidad de sus sociedades y economías que se apoyan en la libertad y la democracia.

---

[45] *Ídem33.* https://www.consilium.europa.eu/es/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

[46] *Ídem33.* https://www.consilium.europa.eu/es/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/

Para lograr armonía y evitar ciberataques de terceros países, la UE activo su diplomacia, insertando instrumentos en su labor, denominada "conjunto de instrumentos de ciberdiplomacia", que se apoya en la cooperación internacional y la diplomacia para la resolución de conflictos.

La labor diplomática europea, encuentra su respaldo en la denominada Estrategia de Ciberseguridad de la UE, explicada en apartados anteriores. Además, previniendo ciberataques la UE ha establecido sanciones[47] orientadas a evitar ciberataques, dirigida a infractores naturales o personas como a entes que intenten y/o consuman ciberataques, incluyendo a los que brinden recursos materiales para su comisión. Las sanciones están enfocadas a la prohibición de ingreso a la UE en caso de personas y la retención de bienes para estas últimas y/o los entes involucrados.

Para fortalecer sus programas de ciberseguridad, la UE realizó en 2020 una inversión de 49 millones de euros, destinados a la actualización y mejoramiento de sus sistemas de protección de datos y ciberseguridad. Para 2027, se invertirá alrededor de 1,600 millones de euros para fortalecer las capacidades de las administraciones públicas de los Estados, sus empresas y población.

Si se observa la suma y se compara con la cantidad de objetivos a cubrir, aparentemente se trata de un monto dinerario muy reducido, más aún, por la composición poblacional y empresarial que posee la UE; sin embargo, se trata de una inversión sustancial para una región que posee avances en ciberseguridad y TIC.

La UE está impulsando centros de I+D+i en el campo de la ciberseguridad, con la implementación de un Centro de Competencia en Ciberseguridad[48] en 2021, a cargo de fortalecer la ciberresiliencia, impulsar la adopción de tecnologías de última generación, prestar asistencia a las pymes y empresas emergentes, fortalecer las capacidades de ciberseguridad; estableciendo, su sede en Bucarest.

Con respecto a la conectividad, también relacionada de forma primordial a lo observado hasta aquí, la UE ha establecido que el IoT[49] al margen de los riesgos que representan para la ciberseguridad, conectividad y privacidad de las personas, también representa una oportunidad para la Unión, decidiendo liderar el sector enfocado a la resiliencia, protección y ciberseguridad.

Para que el IoT funcione, debe contar con conectividad, por lo que la tecnología 5G es la que liderará su integración, constituyendo la ciberseguridad de sus redes fundamental para la UE, al margen también de constituir una gran oportunidad para la generación de recursos a partir de la expansión que alcanzaran estas hasta 2025. En 2020 la UE ha fijado reglas[50] enfocadas a la mitigación de los riesgos que representa 5G para la ciberseguridad, y aprovechando sus estándares enfocadas a la ciberseguridad también la UE quiere aprovechar el mercado.

---

[47] *Ídem33.* https://www.consilium.europa.eu/es/policies/sanctions/

[48] *Ídem33.* https://www.consilium.europa.eu/es/policies/cybersecurity/seat-selection-cybersecurity-centre/

[49] *Ídem33.* https://www.consilium.europa.eu/es/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/

[50] *Ídem33.* https://www.consilium.europa.eu/es/press/press-releases/2019/12/03/significance-and-security-risks-of-5g-technology-council-adopts-conclusions/

Para la UE, es extremadamente urgente actuar en las diversas áreas relacionadas al ciberespacio, la cercanía con los conflictos armados de 2022 y los que acontecen en 2023, exigen que la base normativa y de acciones que fueron asumiendo se aceleren, se fortalezcan y sobre todo se expandan a los aliados de la Unión, pues de esa forma podrá armonizar y optimizar recursos, apoyados en la cooperación internacional en ciberseguridad.

5. *GRUPO BRICS*

En 2001, el economista Jim O´Neill, para describir a cuatro países con economías emergentes, compuestas por Brasil, Rusia, India y China, usa como acrónimo las primeras letras de los mismos, constituyendo el término BRIC, que luego se convirtió en un bloque de países "emergentes" en 2008, siendo Sudáfrica el que se unió para formar lo que conocemos como BRICS en 2010.

La población de los cinco países, agrupa al 40% aproximadamente de la población mundial, su PIB anual alcanza 27,7 billones de euros y su PIB per cápita es de 7,627 euros por habitante, su deuda con relación a su PIB es del 71%, por lo que su déficit en relación a su PIB, según datos de la página datosmacro.com[51] es negativo a excepción de Rusia que es del 0,77% de su PIB

Sin embargo, a diferencia de las OI descritas anteriormente, los BRICS es la alianza de países emergentes, como aceptan llamarse, que agrupan la tercera parte del territorio global, son ricos en RRNN, concentran el 15% del comercio mundial, su PIB representa aproximadamente el 25% respecto del global y aportan el 20% de inversión mundial.

Por tanto, no cuentan con ningún Tratado fundacional o Carta constitutiva – requisito primordial observado y que caracteriza a las OI -, no poseen estructura, ni una representación permanente, llámese secretaria o lo que fuese, no tienen criterios de admisión, más que el interés de adherirse al grupo, sus Estados fundadores tampoco compatibilizan muchos criterios, pues en el caso de la India y China, existe un nivel de desconfianza mutua, tomando en cuenta que entre ambos se concentra aproximadamente el 35% de la población mundial y el 90% de lo que concentra el BRICS como grupo.

De la descripción y análisis de lo que se entienden por OI en apartados superiores, los BRICS y actualmente BRICS+, por sus adhesiones adicionales de otros Estados, se estaría hablando no de una organización, sino de un Movimiento de Estados "emergentes", liderados por China, Rusia y la India, principalmente, sin demeritar a Brasil y Sudáfrica, que poseen posturas menos hegemónicas que los otros tres.

Sudáfrica, tampoco es un referente de unión en el grupo, pues según los propios BRICS comercia más con la UE y USA, que con los países BRICS, cuya pertenencia al grupo es por conveniencia sin que denote un horizonte claro hacia dónde quiere ir o que quiere hacer.

En el caso de China, la India y Rusia, cada uno de ellos tienen intereses en liderar un bloque alternativo de países del Sur o el Sur Global, la multipolaridad y la rivalidad por convertirse en hegemónicos es constante. China ha avanzado más al respecto, en base a su plan de expansión en

---

[51] EXPANSIÓN. (2023). Datosmacro.com, BRICS. Acceso web 2023, *https://datosmacro.expansion.com/paises/grupos/brics*

base la nueva Ruta de la Seda y la Franja china, ha logrado establecer relaciones con diversos países en todos los continentes, cuyo posicionamiento territorial en muchos de ellos ha generado alarmas en todas las regiones, sea a nombre de inversiones, desarrollos conjuntos, explotación con "transferencia" tecnológica de recursos, zonas "diplomáticas" territoriales o bases militares.

Desde el punto de vista económico, China posee alrededor del 70% del PIB que representa el grupo, India, Rusia y Brasil están aún lejos, Sudáfrica más todavía. Para el 1º de enero de 2024, ingresarán a los BRICS, que se denominan ahora BRICS+, países como Argentina, Egipto, Etiopia, Irán, Arabia Saudita y Emiratos Árabes Unidos; que representaran, ya unidos, poblacionalmente alrededor del 46% de la totalidad mundial aproximadamente.

Llama la atención, que los últimos tres miembros poseen respetables recursos energéticos del tipo fósil principalmente; Argentina, con su proyecto de "Vaca Muerta" en progreso se está convirtiendo en un proveedor relevante en Sudamérica de gas natural y otros energéticos, siendo parte junto a Chile y Bolivia del denominado triángulo del Litio, en la que China participa activamente en su explotación, principalmente en Bolivia.

Muchos de sus países miembros, tienen regímenes autoritarios, aunque buscan simular que practican la democracia, cada uno tiene relaciones con USA de diversa forma, con y sin restricciones de este último, con posturas a favor o en contra acorde al régimen gobernante de turno; pero al final todos buscan de una u otra manera comercializar con él.

Venezuela, también con régimen autoritario, que también comercia con USA a través del gobierno de Biden, a pesar de las denuncias que pesan sobre el líder venezolano y personeros de su gobierno; ha pedido a China que interceda para que logre ingresar la BRICS+.

La expansión del Grupo o Movimiento, obedece a razones geopolíticas y geoestratégicas, principalmente a partir de los recursos que posee cada uno, adicional a su falta de representatividad o preferencia que tiene a favor de USA. Por lo que buscan agruparse por lo que representan en porcentajes, en territorio, en población, en RRNN, en economía y en su confrontación con USA, que será relativa según les convenga para el discurso político o para el comercio.

Por lo que, dada las características del BRICS+, al no poseer estructura, sus propósitos de seguridad y defensa obedecen a políticas lideradas principalmente por China, Rusia y la India constituyendo un foco de atención por su regímenes, relacionados algunos de ellos como China con países como Corea del Norte y otros regímenes autoritarios.

Genera para la ciberseguridad mundial, más bien una preocupación, agrupando además en su seno a países que han desplegado ataques extremos en el ciberespacio, usando inclusive en el interior de muchos de ellos las TIC para la persecución, seguimiento, aplicación del "lawfare" en contra de sus opositores, restringiendo la libertad de expresión, pretendiendo normar el acceso y uso libre de las TIC, generando medidas de control sobre sus poblaciones.

Por lo que sin lugar a dudas, habrá que monitorear posibles ciberataques proveniente de sus Estados contra los que denominan los países del occidente y viceversa, en una estrategia de expansión y búsqueda de hegemonía de dicho bloque a la cabeza de China, que no escatimaran en usar recursos para usar el ciberespacio como un escenario de confrontación y lucha por su dominio.

Desde el punto de vista del Índice Global de Ciberseguridad[52], que considera las medidas: legales, técnicas, organizativas, desarrollo de capacidades y cooperación. Coloca a sus países en posiciones expectantes en el caso de sus nuevos miembros a partir de 2024, Arabia Saudita ocupa el puesto número 2 a nivel global, Emiratos Árabes Unidos el puesto 5 a nivel global, Argentina el puesto 99 globalmente, Egipto el puesto 23 global, Etiopia el puesto 115 global, Irán el puesto 54, Sudáfrica el puesto 59, Rusia el puesto 5 global, Brasil el puesto 18 global, China el puesto 33 global y Venezuela el puesto 116.

Deberá observarse que los cuestionarios de la UIT son remitidos a los Estados, algunos no responden a los mismos, como es el caso de Israel que la clasifican en el puesto 36 a nivel global; sin embargo, es conocido que es un Estado polo de desarrollo y celoso de la información que proporciona sobre sus capacidades, por lo que son estimadas.

En el caso de los países miembros del BRICS+, todos respondieron el cuestionario para la publicación de 2020, ubicando a los países árabes y Rusia como altamente comprometidos con la ciberseguridad, los tres son potencias en recursos energéticos, cuentan con recursos económicos derivados del comercio de los mismos, en la que Rusia despliega desarrollo de software y cibercapacidades enfocadas no sólo a la defensa, también al ataque y no siendo la única, pues las potencias mundiales del occidente también están ubicadas en índices de seguridad y ataque en el ciberespacio.

La ubicación de China, debe observarse con cautela, pues es uno de los principales proveedores de desarrollo tecnológico, tanto de SW como en HW, ubicándolo en un lugar que aparentemente es respetable pero no llamaría la atención en relación a los primeros y últimos.

En el caso de Brasil y Egipto, se destacan como altamente comprometidos en su región y también a nivel global, dentro de los primero 25 puestos, mientras que Argentina, Venezuela y Etiopia se ubican con porcentajes que tienden a ir hacia el otro lado, vale decir, poco compromiso en ciberseguridad.

Sudáfrica e Irán, están en el 26% aproximadamente de los países más comprometidos con la ciberseguridad y su regulación. Siendo observables en su comportamiento a partir de los regímenes políticos que poseen, sobre todo el segundo y la calidad de información proporcionada, lo cual ubica a los países en relación a lo respondido en ubicaciones indiciarias.

Sirviendo el Índice Global de Ciberseguridad, como indicios sobre el sector, pero no necesariamente el reflejo de los verdaderos compromisos que poseen los Estados, constituyendo una herramienta muy útil y que deberá analizarse en detalle en función del país que se trate.

En resumen, los BRICS+ buscan, con influencia de la visión rusa, la construcción de un Nuevo Orden Internacional Multipolar, Plural cultural y políticamente, como también del tipo Poshegemónico, a ser construido estratégicamente con los países "emergentes", a través de un movimiento que busca confrontar al hegemon, en la que tres potencias del grupo buscan liderar y

[52] UIT. (2020). "Global Cibersecurity Index". El índice se construye analizando el compromiso a la ciberseguridad de 193 Estados, incluyendo el de Palestina, según la UIT, ya se enviaron las notas en 2023, por lo que está en construcción Acceso web 2023, *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx*

establecerse como tal y con el ingreso de nuevos miembros, las posiciones serán más difusas y confrontacionales, pese a que China tiene un peso relativo mayor en relación al resto de Estados miembros.

No es una organización, podría llegar a serlo, pero por ahora agrupa a diversos países potencias en RRNN, principalmente, cuya "pluralidad" política antagoniza la unidad acorde a sus intereses particulares de cada quien.

La ciberseguridad y los ciberataques en espacios virtuales y físicos generan posibilidades para países "emergentes", que podrán invertir recursos en expandir sus potencialidades para confrontar a diferentes actores en el mundo, sin tener que enfocarse sólo en desarrollar capacidades armamentísticas militares que son más costosas. Muchos de ellos con regímenes del corte autoritario, susceptible de observarlos en el nuevo espacio de actuación, el virtual.

6. *ANÁLISIS DE CASOS DE CIBERATAQUES RELEVANTES SUSCITADOS EN EL MUNDO APLICANDO TRIPLE ENFOQUE*

Los ejemplos de ciberataques suscitados dentro del Sistema Internacional, fueron seleccionados como los más representativos acorde a lo expuesto en el presente trabajo, dejando de lado el ataque Stuxnet suscitado entre Israel e Irán o el WannaCry que afecto a diversos Estados.

Los últimos, son relevantes también y han gozado de análisis diversos tanto en la academia, como en publicaciones especializadas, a través de papers, reportes, noticias o trabajos de tesis. Por lo que serán mencionados en esta sección cuando corresponda, para concentrar el análisis en dos grupos.

El primero, en el que el factor común es Rusia y los Estados ciberatacados, son los que en algún momento integraron la antigua URSS, tratando desde Moscú seguir poseyendo dominio sobre dichos territorios y naciones, para fortalecer su posición como hegemon o Estado influyente en el Sistema Internacional con una posición de poder más consolidada y fuerte. Actuando en la denominada Zona Gris, con propósitos bien establecidos de interés geopolítico, razón por la que se agrupan los ciberataques ocurridos, para su mejor comprensión, en sus años ocurridos.

El segundo, emergente de los sucesos recientes de 7 de octubre de 2023, en los que efectivos del grupo islámico Hammas invadieron Israel en ataques sincronizados, con afectación a la población civil que fue secuestrada y masacrada, con respuesta por parte israelí que generó la destrucción de gran parte de la franja de Gaza, con victimas también civiles en una guerra que está en curso.

Dado que el ciberespacio, es la quinta dimensión o espacio, en el que se desarrollan también los combates o la denominada ciberguerra, los ciberataques que se suscitan en la virtualidad buscan afecta el mundo físico, a través de afectaciones no sólo a infraestructuras críticas, también la obtención de datos e información que dé cuenta de objetivos que buscan los bandos en conflicto, cuya participación se extiende a otras potencias como Yemen, Irán, Líbano y de forma más discreta Egipto, Emiratos Árabes Unidos, China, Rusia, India, USA y otros.

Por otro lado, la Cooperación Internacional está jugando un rol importante, no sólo desde el punto de vista del cuidado y exigencia al cumplimiento del Derecho Internacional Humanitario,

el respeto a los DDHH y al propio DI, también observa que la ciberguerra no afecte infraestructuras críticas que al final atenten contra la propia vida de las personas.

6.1 CASO ESTONIA DE 2007, GEORGIA DE 2008 Y UCRANIA 2022

6.1.1 ESTONIA

Estonia[53] es una nación que estuvo durante más de dos siglos bajo el dominio de diferentes potencias, tales como Noruega, Suecia, Alemania y Rusia, alcanzando su independencia en 1918. En 1939 a 1940 el país es adherido a la comunidad o unión de países soviéticos, ahora conocida como Rusia aunque con fragmentaciones después de la Perestroika.

Es precisamente a raíz de la última, que Estonia en 1991 se independiza nuevamente, ingresando de forma activa y oficial a la Unión Europea y a la OTAN en 2004, ingresando a la OCDE en 2010 como país con estabilidad y potencia económica, adoptando oficialmente el Euro como moneda oficial en 2011.

Geográficamente, es parte de Europa, ubicada en Europa del Este y fronteras con el Golfo de Finlandia y el Mar Báltico, fronteras con Letonia y Rusia. Su superficie total es de más de 45 mil kilómetros cuadrados, de los cuales su territorio terrestre ocupa 42 mil kilómetros cuadrados, poseyendo territorio marítimo de 2.8 mil kilómetros cuadrados que contienen alrededor de 1500 islas; lo que le permite tener por el Derecho Internacional, mar territorial y su zona económica exclusiva, reconocidas por Letonia, Finlandia, Rusia y Suecia.

Sus RRNN, se componen de tierras principalmente, estando ocupada por bosque en casi el 60% de su territorio, tierras agrícolas y para pasteo se ocupan en el 30% de su territorio.

Su población es de alrededor de 1.2 MM de habitantes, el idioma oficial es el estonio en 68%, el ruso en un 29%, ucraniano el 0,6% y otros idiomas. En cuanto a la religión más del 54% no especifica su preferencia, por lo que el 16% aproximadamente es ortodoxo, 9,9 alguna fe cristiana – incluida la católica y metodista -. Su población, concentra la mayor parte en edades medias entre 15 a 64 años, en un 62% aproximadamente, el 22% es de la tercera edad y el 15% es menor de 15 años.

Su gobierno es del tipo parlamentario, su capital se encuentra en Tallin, su división política territorial interna se compone por municipios urbanos y municipios rurales. Desde el punto de vista económico su fortaleza está orientada a los servicios financieros, comercio y telecomunicaciones, siendo un país estable y apto para las inversiones. Su industria se enfoca en la electrónica, alimentación, ingeniería, madera y derivados, textiles, tecnología de la información y telecomunicaciones.

Si se observa su industria, los años en los que Estonia se adhirió a la UE, OTAN y OCDE, da cuenta que luego de sucesos de 2007, en los que recibió ciberataque masivo durante semanas, marcaron la posición de su actual Estado, por lo que en base a todo lo acontecido se podría

[53] *CIA. (2023). Información actualizada a noviembre de 2023 en el Libro Mundial de datos. Acceso web 2023,* https://www.cia.gov/the-world-factbook/countries/estonia/

afirmar que cuenta con una industria dedicada a las TIC de forma robusta. Marcando un antes y un después en su desarrollo. Por lo que se pasará a describir lo que aconteció más abajo.

6.1.2 GEORGIA

Georgia[54], remonta su historia antes del Imperio romano, encontrándose bajo influencia y dominio diverso, con asimilación por parte del Imperio rusa a finales del siglo XIX, luego de la denominada revolución rusa, fue adherida por la fuerza por la antigua unión soviética en 1921; permaneciendo en la última hasta 1991, en la que se independiza.

En 2003, se produjo la denominada "Revolución Rosa" ante los descontentos del gobierno dirigido desde 1995 por Shevardnadze, con elecciones en 2004, debiendo enfrentar el nuevo presidente Saakashvili no sólo denuncias en su contra, también reacciones por parte de regiones separatistas prorusas en su país, que derivo en agosto de 2008 en conflictos entre Rusia y Georgia durante cinco días, sufriendo además la invasión a vastos territorios del país por parte de las fuerzas rusas.

Si bien Rusia se comprometió a retirarse de los territorios ocupados, a finales de agosto de 2008, reconoció unilateralmente la independencia de las dos regiones de Georgia separatistas en conflicto, Abjasia y Osetia del Sur, en la que las fuerzas rusas se quedaron allí hasta la fecha.

En los años siguiente la inestabilidad de gobernanza se ha producido en el país georgiano; sin embargo, su población exige la adhesión de Georgia a la UE y a la OTAN, habiendo presentado oficialmente su petición de adhesión a la Unión en marzo de 2022, lo que permitió que a partir del Acuerdo de Asociación firmado entre la Unión y Georgia en junio 2014 y vigencia desde julio 2016, posean un Acuerdo de libre comercio completo y profundo, lo que favoreció luego a que los ciudadanos georgianos puedan viajar al espacio Schengen sin necesidad de obtener visa.

Fue durante los conflictos de 2008 en los que se produjeron ciberataques al Estado georgiano, lo que ayudaron a que se consoliden las consecuencias descritas previamente y que se pasa a analizar a continuación más abajo.

6.1.3 UCRANIA

Ucrania[55], llamado en un inicio Kyivan Rus, posee historia proveniente desde el siglo X, en el que logró ser el Estado más poderoso de Europa, pasando a llamarse Hetmanate en el siglo XVII con influencia cosaca, para posteriormente a finales del siglo XVIII, pasar a formar parte del Imperio ruso, este último que colapso en 1917.

Ucrania, ya como tal, llegó a ser independiente desde 1917 hasta 1920, para ser absorbido por el régimen soviético, durante el cual su población se vio mermada primero por la hambruna a principios de la década de 1920, denominada holodomor, en el que perecieron aproximadamente más de 6 millones de personas bajo el régimen soviético y luego durante la Segunda Guerra Mundial, en el que también perecieron más de 8 millones de ucranianos aproximadamente.

---

[54] *Idem48. Acceso web 2023, https://www.cia.gov/the-world-factbook/countries/georgia/*

[55] *Idem48. Acceso web 2023, https://www.cia.gov/the-world-factbook/countries/ukraine/*

Para 1991, ante el colapso de la URSS, Ucrania voto por su independencia, pero no pudo arrancar el desarrollo del país, debido a la subsistencia de problemas endémicos heredados del antiguo régimen, primando la corrupción, clientelismo y evitando que reformas a favor de su desarrollo se realicen, estando todavía unida a la influencia de Moscú.

Entre 2004 y 2005, se produjo la denominada "revolución naranja", derivada de protestas frente a elecciones presidenciales viciadas, por lo que se exigió presencia internacional y asumió la presidencia Yushchenko, quien cedió el poder en 2010 al opositor Yanukovich, quien con marcada subordinación a Rusia, cuando la población de Ucrania apoyaba acuerdos comerciales y de Cooperación con la UE, en 2013 dio paso atrás en la firma del mismo.

La negativa que produjo el 21 de noviembre de 2013, a la firma del Acuerdo de Asociación con la Unión Europea, generó fuertes presiones, pues Yanukovich, pretendía que Ucrania actúe como puente entre la UE y Rusia, este último que le impuso un Acuerdo de Unión Aduanera, por lo que el mandatario ucraniano favoreció a los rusos, provocando rechazos en la población que derivaron a finales de febrero de 2014 protestas, enfrentamientos principalmente en Kiev, con la posterior destitución de Yanukovich en 2014, quien se refugió en Rusia.

En junio 2014, asume la presidencia Petro Poroshenko, pero el presidente ruso Putin, ordena luego de la salida de Yanukovich, que el ejército ruso invada la península de Crimea en Ucrania, con el pretexto de proteger a las poblaciones rusas habitantes en esa región. Impulsando, además, un referéndum a las dos semanas de la invasión, para que se decida si Crimea se integraría a la Federación Rusa, por lo que dicho acto fue acusado de ilegal por parte de la ONU, USA, UE y sobre todo el gobierno ucraniano.

La Asamblea General de la ONU, emitió la Resolución 68/262, que reivindicaba la unidad e integridad territorial de Ucrania, rechazando el supuesto referéndum, reconociendo la independencia política y soberanía de Ucrania.

Sin embargo, Rusia apoyo a regiones orientales en Ucrania, lo que desencadeno en conflictos armados, procurando establecer un alto a los mismos se firmaron el Protocolo y Memorándum de Minsk en septiembre 2014, por parte de representantes de Ucrania, Rusia, las provincias involucradas de Ucrania devenidas en repúblicas independientes prorusas (Dombás), cuyo efecto fue negativo, continuando los enfrentamientos. En 2015, se repitió el esfuerzo, esta vez, con participación de Alemania, Francia, junto a Ucrania y Rusia, también sucumbiendo al fracaso.

Por lo que los combates, continuaron desde 2015 hasta inicios de 2020. Resultando en más de 1.5 millones de desplazados, 14 mil muertos en los combates[56]. El 2019, asumió la presidencia de Ucrania Volodymyr Zelensky. Para finales de 2021, Rusia agrupo a sus tropas en la frontera con Ucrania, concentrando sus labores en establecer infraestructuras preparando la invasión a dicho país, aunque declaraciones rusas daban cuenta que sólo se trataba de ejercicios militares.

Rusia, comunico a los países del occidente y a la OTAN principalmente, que exigían garantías escritas de que la OTAN no se expandiría hacia los países del Este, restricciones sobre tipos de armas instaladas en los países que se unieron a la OI desde 1997, cese de cualquier tipo de cooperación de la OTAN con Estados postsoviéticos, particularmente Ucrania y Georgia.

[56] *BBC news mundo. 2023. Rusia – Ucrania 9 hitos en la historia que explican la amenaza de invasión actual. Acceso web 2023, https://www.bbc.com/mundo/noticias-internacional-60237751*

Poniendo, Rusia, en movimiento su aparato propagandístico en redes sociales e Internet, alertando a su población de un posible ataque de la OTAN y de Ucrania al Dombás.

El 24 de febrero de 2022, Rusia realiza la mayor invasión convencional contra un Estado luego de la Segunda Guerra Mundial, logrando inicialmente avanzar y tomar muchas regiones de Ucrania, pero para finales de 2022 la población de este país, con ayuda logística de diversos países, logro recuperar gran parte de su territorio en el norte y noroeste, algunos avances al este y sur, cuya determinación y resistencia del pueblo ucraniano es un elemento no calculado por Rusia.

A finales de septiembre de 2022, Rusia anexo unilateralmente cuatro provincias de Ucrania, Donestk, Kherson, Zaporizhzhia y Luhansk, ocupadas parcialmente por ambos bandos. Las cuales carecen de reconocimiento internacional.

Derivado de la guerra, en el mundo se estima que existen más de 6.3 millones de refugiados ucranianos en el mundo, siendo además una de las dos mayores crisis de desplazamiento y refugiados en el mundo, siendo la otra Siria.

La guerra actualmente se combate no sólo con el uso de armamento sofisticado, como misiles, armas supersónicas, tanques y aviones modernos; también, se están utilizando los denominados drones o UAV por parte de ambos bandos, en el caso de Rusia algunos de ellos de fabricación iraní modelo Shahed. Debiendo recordar que en el presente trabajo se mencionó como ejemplo la captura de drones israelíes y norteamericano, que derivó en una relación de cooperación entre Irán, Rusia y China para replicar mediante ingeniería inversa dicha tecnología obtenida en la década anterior, aproximadamente, cuyos resultados se observan ahora en la actual guerra.

La ciberguerra[57], en la que Rusia tiene experiencia de aplicación, tampoco está ausente en loa actuales conflictos, por lo que son analizados también como parte del despliegue militar que forman parte de los combates tanto en el mundo físico así como en el virtual o ciberespacio.

6.1.4 RUSIA

Rusia[58], su historia deviene desde el siglo XII en progresión de acontecimientos que la fueron configurando en diferentes épocas, iniciando con el Principado de Moscovia, fortalecida en base a su expansión, la cual fue continuada en el siglo XVII por la dinastía Romanov, que llegó a Siberia, pacífico y el Mar Báltico, luego de lo cual el país paso a llamarse Imperio Ruso, siguiendo su expansión por Europa y Asia.

El imperio ruso, fue afectado con revueltas en 1905 principalmente, luego de la derrota sufrida frente a Japón, confluyendo en inestabilidad en su interior, hasta que en 1917 con consecuencias de la primera guerra mundial reflejadas en falta de alimento y carencias generalizadas, resultaron en el derrocamiento de la dinastía Romanov y la toma del poder por parte de revolucionarios de

---

[57] *Tidy, J. BBC news. (2023). La otra guerra inclemente que libran Ucrania y Rusia. Acceso web 2023, https://www.bbc.com/mundo/noticias-internacional-65266795*

[58] *CIA. (2023). Información actualizada a noviembre de 2023 en el Libro Mundial de datos. Acceso web 2023, https://www.cia.gov/the-world-factbook/countries/russia/*

corte comunista, a la cabeza de Lenin. Pasando a llamarse URSS o Unión de Repúblicas Socialistas Soviéticos.

En 1928 asume el poder Stalin, cuya brutalidad fortaleza la posición comunista dentro del país, quien aprovechando la alianza con USA luego de la Segunda Guerra Mundial, expande territorio y zona de influencia en la denominada Europa del Este, consolidándose luego como potencia mundial.

Entre 1947 y 1991, la URSS mantuvo su posición de confrontación con USA, en la denominada "guerra fría", en la que los regímenes comunistas desarrollaron potencial nuclear y capacidades bélicas, incluyendo expansión al espacio.

La apertura de Rusia, denominada "glasnost" en base a una reestructuración del país, denominada "perestroika", fueron llevadas adelante por Mikhail Gorbachev, entre 1985 a 1991; buscando que el régimen comunista se modernice y brinde soluciones a las demandas del país que se vio sumergida en el estancamiento económico principalmente.

El resultado de las reformas, derivó en que la URSS se desintegre, con la independencia de 14 Estados y en diciembre de 1991 desaparezca la Unión de Repúblicas como tal.

Ya como Rusia, entre 1991 a 1999, asume la conducción del país Yeltsin, generándose dentro del país demandas e inestabilidad económica, que provoco demandas políticas insatisfechas. Asumiendo el poder, en 2000 Vladimir Putin, cuyo régimen ser caracterizó por ser centralizado y autoritario.

Mapas del Mundo. (2023). La URSS grande mapa político con socorro, ferrocarriles y grandes ciudades – 1986. Tamaño 980 kb. URSS: Mapas del Mundo. https://www.mapas-del-mundo.net/mapas/europa/urss/grande-mapa-politico-de-la-urss-con-socorro-ferrocarriles-y-grandes-ciudades-1986.jpg

Putin, estuvo al frente de Rusia en un primer periodo, entre 2000 a 2008, para luego retomar la conducción del país en 2012 y actualmente sigue al frente desde ese año, habiendo construido toda una estructura de poder que le permita liderar el país supeditado a su poder, con reformas que buscan que permanezcan al frente hasta posiblemente 2030.

Su postura frente al Sistema Internacional, es el de fortalecer su influencia geopolítica a nivel global, apoyado en recursos derivados de la comercialización de materias primas energéticas y la expansión de su influencia en Europa del Este principalmente.

En 2014, anexa a Crimea y dos regiones de pertenencia ucraniana, para en 2022, 24 de febrero, invadir Ucrania, luego de la pandemia del Covid-19, lo que provocó el rechazo mayoritario por parte de los Estados en el mundo, salvo excepciones que tienen afinidad con el régimen de Moscú.

La invasión fue diseñada para que durara pocas semanas, encontrándose con una nación aguerrida, con combates en una guerra que dura hasta la actualidad, en la que el régimen ruso anexo a cuatro regiones de Ucrania de manera unilateral en septiembre de 2022, el cual es rechazado por la mayoría de Estados de la comunidad internacional.

La ubicación de Rusia, es significativa, esta al norte de Asía y a nivel país limita al norte con el Océano Ártico, extendiendo su territorio desde el occidente europeo, denominada Europa del Este (occidente de los Urales), hasta el Océano Pacifico de la zona norte. Poseyendo una superficie de más de 17 millones de kilómetros cuadrados, haciéndolo el país más grande, seguido por la Antártida, Canadá, USA, China, Brasil y Australia en extensión, superándolas en casi el 80 al 100% de superficie, a excepción de la Antártida que es menor en un 20% aproximadamente.

Sus fronteras alcanzan 22,407 kilómetros y tiene fronteras con catorce países: Ucrania, Polonia, Noruega, Mongolia, Lituania, Letonia, Kazajstán, Georgia, Corea del Norte, Finlandia, Estonia, Bielorrusia, Azerbaiyán y China.

Sus mayores fronteras las comparte con Kazajistán con casi 7,6 miles de kilómetros de frontera, seguido por China en dos puntos uno de 4.1 y otro de 0.046 miles de kilómetros en el sur, Mongolia con 3.4 miles de kilómetros, Ucrania con 1.9 miles de kilómetros, Bielorrusia y Finlandia cada una con 1.3 miles de kilómetros y Georgia con 0.89 miles de kilómetros. Es decir, siete países.

Su frontera más pequeña de apenas 18 kilómetros de longitud, la comparte con Corea del Norte y no menos importante por la connotación geoestratégica que representan ambos. No siendo el análisis objeto del presente trabajo. Su frontera o línea costera, tiene una longitud de 37,653 kilómetros, siendo la mayor terrestre.

Sus RRNN se concentran en gas, petróleo, carbón, minerales estratégicos, madera y otros. La explotación de muchos de sus recursos naturales, por su tipo de geografía es difícil. Sus tierras cultivables ocupan el 7,3% de su territorio y el 5.7% se utiliza para pastos, el 50% aproximadamente de su territorio consiste en bosques, el resto de 37% de sus tierras se ocupan para fines diversos. De allí que su potencial está enfocado a los energéticos fósiles.

Geográficamente, su extensión es la mayor del mundo, su ubicación dificulta su conectividad con las principales rutas marítimas mundiales, constituyendo en desventaja, como se observó la agricultura en relación a su extensión es reducida, por los tipos de suelos y clima imperante que puede llegar a ser extremadamente frio o seco, afectándola en ese sector.

Su población alcanza más de 149 millones de habitantes para 2023, siendo el 77% ruso, 3.7 % tártaro, 1.4% ucraniano y el resto dividido entre más de 200 grupos nacionales y étnicos. Su población mayoritariamente es de edad media, con un promedio de 40 años de edad aproximadamente, con más del 65% de su población comprendida entre 15 a 64 años, el 17% mayores a 64 años y el 16% entre 0 a 14 años de edad.

La ciudanía, no se adquiere por nacimiento, debiendo ser uno de los padres ruso, reconociéndose la doble ciudadanía.

Desde el punto de vista económico, su industria se enfoca a diversas ramas, desde industrias mineras y extractivas, de gas, petróleo, químicos, metales; construcción de maquinaria, aviones, vehículos espaciales, industria defensiva desde radares, misiles, electrónica avanzada, construcción naval; equipo de transporte terrestre, naval, ferroviario; equipo agrícola, para la construcción, de generación y transmisión para energía eléctrica, textiles, bienes de consumo, equipamiento médico, equipos de medición, etc.

Su sistema de comunicación es mayoritariamente vía celular, el acceso de Internet es del 88% de su población, colocándolo en el puesto seis de acceso a dicho servicio a nivel mundial, con servicio de banda ancha.

Es un país que cuenta con ingresos considerables por la venta de energéticos, a Europa principalmente a Países Bajos y Alemania, por lo que tiene los recursos económicos para inyectar recursos al sector militar.

Su gasto militar es del 4% de su PIB, el servicio obligatorio es desde los 17 a los 27 años, voluntario hasta los 40 años, su fuerza efectiva antes de la guerra con Ucrania era de 900 mil y luego de la guerra se anunció que se expandiría a 1.5 millones de efectivos.

Su fuerza militar es mixta, compuesta por profesionales y reclutas, con capacidades en el combate terrestre, marítimo, aéreo, manejo de misiles estratégicos, con personal profesional en áreas de guerra cibernética, guerra electrónica, guerra espacial.

La misión de sus fuerzas, al margen de las tradicionales dirigidas a la protección de la soberanía, es las mantener y expandir el poder de Rusia fuera de sus fronteras, debiendo disuadir amenazas de USA y la OTAN, principalmente en países exmiembros de la antigua URSS.

En los conflictos de Rusia, se observa que en 2005 Estonia y Rusia firmaron un acuerdo fronterizo técnico en el mes de mayo y luego unilateralmente Rusia retiro su firma en junio 2005, debido a la añadidura del parlamento estonio de un acontecimiento histórico referente a la ocupación soviética y las fronteras estonias antes de 1920.

El denominado Tratado de Tartu, para Rusia representa el preámbulo histórico un reconocimiento territorial que podría ser usado por Estonia para el reclamo de territorio ruso actualmente,

llegando a reabrirse las negociaciones en 2012, ya sin el referido preámbulo y con firma el 2014, sin que hasta 2020 se haya ratificado por ninguno de los países.

Entonces, de la caracterización del país, se observa que militarmente la ciberseguridad y la ciberguerra constituyen ramas militares parte de sus capacidades, cuya manejo es del tipo profesional dentro de sus fuerzas armadas, cuyo desarrollo y objetivos están fijados con orientación a la expansión y participación en mantener presencia e influencia en los Estados que alguna vez fueron miembros de la URSS, que coinciden con los países de la Europa del Este.

Aspecto relevante, pues los sucesos en Estonia, luego Georgia y actualmente en Ucrania, compartiendo fronteras con las tres, responden a una visión del Estado ruso, más allá si es promovida por su líder, el cual no sólo la representa también lo maneja directamente en diversos frentes.

De los tres Estados fronterizos con Rusia, dos sufrieron ataques militares directos a excepción de Estonia en 2007, pues este ya formaba parte de la OTAN desde 2004, mientras que Georgia y Ucrania aún, lo que permitió a que las fuerzas rusas actuaran en 2008 y 2022 respectivamente, antes de que se anexaran, buscando presencia territorial que demarque su zona de influencia y lo coloque más cerca de la frontera con Europa occidental.

Esto también representa amenazas latentes para los otros Estados fronterizos, a excepción de países como China, Corea del Norte, Mongolia y Bielorrusia por ahora. El resto busca de una u otra forma mantener la neutralidad, en el caso de Finlandia ante su ingreso a la OTAN lo convierte en un problema más serio para Rusia al compartir frontera directa.

La ciberguerra, es un frente de operación importante para el Estado Ruso, combinado a sus capacidades de guerra electrónica y espacial, lo convierte en un actor relevante en el sector de los ciberataques y ciberseguridad, cuya experticia la fue desarrollando durante décadas y es en los últimos años que se observa el incremento de sus ataques en función de sus intereses, con especulaciones sobre su participación inclusive en la elecciones norteamericanas en las que gano Trump en el país del norte.

Sin embargo, su primera incursión de repercusión en el ciberespacio fue precisamente producida en 2007, sin que se logre hasta el día de hoy, aparentemente, vincularlo directamente sobre el ciberataque desplegado a Estonia en ese año. Pasando a describirse a continuación.

6.1.5 DESCRIPCIÓN CIBERATAQUES

CASO ESTONIA: En 1947 en conmemoración a los combates derivados durante la Segunda Guerra Mundial, en la que la URSS expulso a la Alemania nazi de territorio estonio, se erigió la estatua de un soldado de bronce denominada “Monumento a los Libertadores de Tallin”, ubicada en la capital del mismo nombre, conocido mediáticamente como el Soldado de Bronce.

Para la época, Estonia al ser parte de una sola república soviética, el simbolismo de dicha estatua fue asimilada. Décadas después, con criterios encontrados entre la población de ascendencia rusa y los estonios nacionalistas, en 1991 luego de la independencia de Estonia, se generaron dos corrientes sobre la representación de dicho símbolo.

Para los simpatizantes y partidarios independentistas, la estatua representaba el yugo al que fueron sometidos por el anterior régimen soviético con antecedentes marcados que se remontan hasta 1917, mientras que para los prorusos era la representación de la victoria y libertad por parte de las antiguas fuerzas soviéticas, devenidas luego de 1991 en Rusia.

En 2007, el gobierno, de forma discreta en la noche decide mover la estatua del Soldado de Bronce de Tallin, indicando además que realizaría obras en el lugar donde se encontraba para ubicar cuerpos de soldados caídos y trasladar sus restos al cementerio militar, al cual también trasladaron la estatua.

La polémica entre estonios nacionalistas y los estonios de ascendencia rusa principalmente, encendió confrontaciones entre bandos, en los que la prensa rusa también apoyaba al sector proruso, generando una fake new[59] para encender las emociones y provocar reacciones, indicando que tanto la estatua como las tumbas soviéticas de la guerra estaban siendo destruidas. Derivando en enfrentamientos callejeros, manifestaciones, utilización de la fuerza pública y represiones con el objetivo de contener las revueltas violentas que se produjeron.

Para 2007 Estonia, había logrado automatizar la mayoría de su Estado, no sólo gobierno, iniciativa que derivó de la necesidad de reconstruir el país en base a escasos recursos con los que contaba luego de su independencia en 1991. Las revueltas derivadas del traslado de la estatua, fueron el justificativo para la externalización de los conflictos

El 27 de abril de 2007, luego de dos noches intensas con diversas revueltas, arrestos y lastimosamente una persona fallecida, Estonia recibió un ciberataque que duró semanas, dejando incomunicado a bancos, entidades gubernamentales, medios de comunicación y población.

Las direcciones de Protocolo de Internet o IP del inglés, ubicaban que los ciberataques provenían de Rusia, este últimos que siempre lo negó.

El ciberataque sincrónico consistió en uno del tipo DDoS (ataque distribuido de denegación de servicio), en el que se realizan peticiones a los servidores para recibir respuesta, pero al realizarse peticiones de forma repetida atacando varias veces al mismo servidor, esto genera que los servidores por su capacidad de atención limiten su capacidad de respuesta y si los pedidos de atención se van realizando muchas veces por segundo, los sistemas colapsan y fallan; que en el caso del sistema estonio el 27 de abril inició con paquetes de petición que alcanzaban los miles en los primeros minutos hasta llegar a más de cuatro millones por segundo en las siguientes semanas, buscando destruir de esa forma el sistema informático del Estado.

Resultado de los ciberataques, se cortaron los servicios públicos, las noticias, las operaciones bancarias, las comunicaciones, inundando las redes con spam.

[59] *Euronews. (2022). Estonia: proteger el ciberespacio frente a las intenciones rusas. El país báltico es el tercero del mundo en cuanto a ciberseguridad. Acceso web 2023, https://es.euronews.com/next/2022/05/27/estonia-proteger-el-ciberespacio-frente-a-las-intenciones-rusas#:~:text=El%2026%20de%20abril%20de,gubernamentales%20y%20medios%20de%20comunicaci%C3%B3n*

El ataque se registró por lo menos en dos dimensiones, del 27 al 29 de abril, se produjeron ataques repetitivos, que no demostraban complejidad generando ataques a páginas web del gobierno, la de los partidos políticos y la recepción de mensajes basura o spam en los servidores, hasta el punto de bloquearlos.

El 28 de abril de 2007, se activaron los equipos de respuesta rápida, denominados CERT, junto a personal de diferentes ministerios, con apoyo técnico de expertos de la OTAN (Jara, 2020, pág. 58), lo que denotó un acierto para identificar y confrontar los ataques que se venían realizando, estableciendo la seriedad y gravedad de lo que aconteció y la alerta a nivel internacional de los hechos que activo la Cooperación Internacional.

El 30 de abril de 2007, los ataques pasaron de poco sofisticados a mostrar el manejo de técnicas de ciberataque, el uso de diferentes herramientas y la coordinación organizada desplegada en los mismos. Los objetivos fueron medios de comunicación de prensa, cajeros automáticos de bancos, con bloqueos que no llegaron a ser totales en ese momento, además de atacar a figuras políticas a través de sus páginas web.

Para el CERT (Jara, 2020, pág. 59), los ataques consistieron en: 1) DDoS o Denegación de Servicio, utilizando botnets encargados de realizar solicitudes de forma masiva e insistente, hasta colapsar al sistema. Eligiendo a las páginas web del gobierno e intuiciones en el manejo de infraestructura crítica; 2) Web site defacement, distorsión o deconstrucción de páginas web, siendo los objetivos líderes políticos de Estonia y 3) Spam, a través de correo electrónico de forma masiva y reiterada de manera tal de colapsar los servidores, objetivos fueron el gobierno, políticos líderes, bancos, instituciones públicas y privadas.

Los ataques continuaron por varios días, inclusive en las celebraciones de 9 de mayo en Moscú (Jara, 2020, pág. 60), incrementando el ataque DDoS en un 150%, pasando de 21 ataques realizados el 3 de mayo de 2007 a 58. El CERT luego identificó que las direcciones IP de los ciberataques correspondían a las del gobierno ruso, con identificaciones adicionales de ataque provenientes de Perú, Vietnam y Egipto, no denotando estos últimos sean aparentemente el origen de los mismos, sino el desvió de las direcciones IP originales a través de mecanismos del uso de servidores remotos de redes privadas que enmascaran los servidores reales.

Rusia, ante los acontecimientos, pidió inclusive que el gobierno de Estonia sea cambiado, generó protestas en la embajada de Estonia en Moscú con la retirada de la bandera del país, negó su participación en los hechos, el 9 de mayo de 2007 día de la Victoria Putin manifestó que el desmantelamiento de estatuas de héroes siembran discordias entres personas y estados. El 17 de mayo de 2007 el jefe de prensa del presidente Putin, afirmo que los ataques contra Estonia provenían de diversos países, que Rusia no estaba implicada en ciberterrorismo y que las direcciones IP podrían ser falsas.

Lo que se buscaba, según declaraciones (Jara, 2020, pág. 66), era no sólo afectar a Estonia, también medir las capacidades de respuesta de la OTAN frente a este tipo de acontecimientos. Esta OI lo que hizo fue reconocer que en ese momento era difícil rastrear el origen de los ciberataques, evitando culpar directamente a Rusia y apoyando la versión de Estonia sobre el origen.

CASO GEORGIA: con la experiencia suscitada en Estonia en 2007, Rusia ataco las redes informáticas de Georgia, si bien a diferencia de Estonia, este país no era dependiente de las redes en el grado que alcanzo el primero.

Por otro lado, tampoco Georgia era parte de la OTAN, por lo que los ataques podían realizarse físicamente, como aconteció en la realidad y también aprovechando el ciberespacio. Por lo que, en un nuevo escenario de guerra, los ataques se suscitaron por los espacios tradicionales, incorporando novedosamente el de la virtualidad.

El ataque según reportes[60], se habría producido previamente el 20 de julio de 2008, mediante ataque de DDoS o denegación de servicio, ubicando servidores inclusive en USA inicialmente, para luego detectarlos en Rusia.

El caso georgiano, los ataques se escalaron para evitar que el gobierno del país, puedan comunicarse a través de sus páginas oficiales y otros medios en línea, provocando aislarlos y por ende cortar líneas de coordinación ante los ataques que se desarrollaban militarmente en su territorio.

El ciberataque, se dividió en dos frentes, por un lado se dirigió al gobierno, tanto a sus páginas oficiales como a sus sistemas de comunicación, exentos de medidas de ciberseguridad fuertes, por lo que fueron neutralizadas e inoperantes durante periodos de tiempo prolongados. El segundo frente, fue dirigido a instituciones financieras, medios de comunicación nacionales y extranjeras, empresas y a un grupo de hackers georgianos que contaba con una página web.

El objetivo era no sólo desconfigurar sus redes, sino capturar información valiosa, por lo que lograron aparentemente obtener correos electrónicos de funcionarios gubernamentales, que contenía información valiosa para los fines de los ataques que estaban realizando en el campo de batalla las tropas rusas.

En este caso, se logró generar descontrol, efectos psicológicos sobre la población, manejo de la información del enemigo para lograr ataques más precisos en el campo de batalla, aislamiento del Estado atacado dentro y fuera del país, logrando capturar los objetivos con el menor costo y esfuerzo.

Al igual, que en el Caso de Estonia, no se pudieron obtener pruebas que vincule oficialmente a Rusia con los ciberataques perpetrados en Georgia, que coincidieron con los ataques físicos.

CASO UCRANIA: la experiencia en Estonia y Georgia, mostraron la importancia en el dominio de herramientas de ciberataque y manejo del ciberespacio, así como detectar las fortalezas y sobre todo debilidades de las ciberseguridad del enemigo.

Rusia, cuando atacó en febrero de 2022 a Ucrania, lo hizo al igual que en Georgia atacando diversos frentes en los espacios físicos, pero al mismo tiempo en el ciberespacio, pues al igual

[60] *Markoff, J. El País. (2008)..Georgia sufre la ciberguerra cibernética. Tbilisi acusa al Kremlin de piratear sus sitios gubernamentales en Internet. Acceso web 2023, https://elpais.com/diario/2008/08/14/internacional/1218664803_850215.html?outputType=amp*

que Georgia, Ucrania no forma parte de la OTAN, es un país deprimido económicamente y sus capacidades militares fueron evaluadas como disminuidas.

Los ciberataques a Ucrania, antes de la guerra por parte de Rusia, ya se habían realizado (Gavrila, 2022), con afectaciones a la red eléctrica en 2015, a la Tesorería de Ucrania en 2016, ataque de malware NotPetya en 2017, que fue parte de otras variantes como el WannaCry, que afectaron no sólo a sitios web de empresas, gobierno, bancos, empresas de comunicación, electricidad y otros; también a países, debido a su extensión y capacidad e infección, tales como USA, Alemania, Reino Unido, etc.

Los ciberataques, al igual que en el Caso Georgia, se realizaron con semanas de antelación, iniciando el 14 de enero de 2022, buscando generar el efecto psicológico de terror o preocupación, correspondiendo al primer factor descrito por Gaitán (Gaitán, 2012, pág. 7), desconfigurando páginas web del gobierno como los del Consejo de Seguridad y Defensa, Ministerio de Relaciones Exteriores y otras (Gavrila, 2022, pág. 5).

Para el día siguiente, 15 de enero de 2022, se realizaron ciberataques de DDoS, al Ministerio de Defensa, los dos principales bancos de Ucrania, la página de su Ejército.

Horas antes del ataque a través de las fronteras, se realizó un ciberataque a la red satelital Ka-Sat de ViaSat (Gavrila, 2022, págs. 7 - 8), desactivando turbinas eólicas alemanas de ViaSat que usaban para comunicarse, la red de Internet se cayó en Ucrania siendo inaccesible, y el impacto no fue mayor. Porque, la UE envió un equipo CERT a Ucrania para mitigar ciberataques y fortalecer sus capacidades de ciberseguridad.

Logrando identificar tipos de malware, de procedencia de la inteligencia rusa. Según el mismo estudio (Gavrila, 2022, pág. 9), la inteligencia americana logró identificar que los ciberataques se fueron perpetrando desde 2021, en un primer instante para recopilar información de inteligencia para conocer capacidades, controlar infraestructuras críticas, robar planes de política exterior y militares y proceder a inutilizar el sistema TIC de Ucrania. Por lo que el día de los ataques mientras se disparaban misiles y las fuerzas terrestres invadían el país, paralelamente la ciberguerra quería tomar control de las infraestructuras energéticas principalmente, aislar a Ucrania del mundo, bloqueando sus comunicaciones, generar caos en la población con guerra de desinformación y provocar desolación aprovechando el factor psicológico.

Esto no ocurrió, como se observó en Georgia en 2008, pues gracias a la Cooperación Internacional en temas de ciberseguridad, incluyendo el apoyo de empresas como Microsoft y Google que alojaron mucha información crítica en la nube, se evitó que las consecuencias sean de gravedad (Gavrila, 2022, pág. 10)

6.1.6 IMPLICANCIAS GEOPOLÍTICAS Y DE LOS CONFLICTOS

Estonia, se destacó ya para 2000 como un Estado de avanzada dentro del campo de las TIC, cuyos avances desde su independencia, derivó que en 1994 establezca su estrategia para la sociedad de la información, con avances en su infraestructura de informática, actualizaciones en sus políticas y la implementación del voto a través de Internet en 2005 siendo el primero a nivel global.

El conocimiento sobre su vecino, influyo que apenas se independice en los años siguientes pase a formar parte de diversas OI, como la Unión Europea, la OTAN y muchas otras. Dicha decisión fue crucial para fortalecer su estabilidad como país independiente, contar con apoyo del equipo de respuesta rápida cibernética de la OTAN, denominada CERT y sobre todo evitar ser invadida militarmente. Que a contrario sensu, fue lo que pasó con Georgia y Ucrania, ninguna de las dos pertenecientes a las OI referidas.

El Art. 5 del Tratado fundacional de la OTAN, es preciso sobre la doctrina de la Defensa Colectiva, la cual luego de los acontecimientos de 2007, se extendió al ciberespacio, obligando a que la OI y sus Estados miembros potencien sus capacidades e implementen sus equipos CERT.

Para Rusia, dentro la evaluación de su posición determinó que la OTAN no podía estar como vecino o en sus fronteras, por lo que para Putin y su Estado, han desarrollado objetivos militares específicos para influenciar sobre los países de la Europa del Este y de ser posible establecer presencia rusa en ellos, considerándose un país agredido y que debe responder con el uso de la fuerza, autoidentificándose como la "fortaleza asediada" por parte de USA y la OTAN principalmente, por lo que reclama presencia en territorios que fueron parte de la antigua URSS.

La ubicación de Rusia no es la más ideal, pues posee territorio con fronteras extremadamente extensas, muy difíciles de proteger casi hasta la imposibilidad, contando con puertos marítimos cuyo tráfico comercial mundial y/o estratégicos busca estén bajo su dominio, entendiendo que debe también ganar posición y presencia física en otros territorios de países vecinos, que en otrora formaron parte de la URSS, para acercarse geográficamente a Europa de manera directa, así como a regiones con tráfico marítimo relevantes.

La mayor concentración de su población está alrededor de Moscú y próximos a los países de Europa del Este, por lo que estos durante la existencia de la URSS constituían barreras de protección para posibles ataques a su centro político y poblacional, por lo que al no contar con dichas protecciones, establece para la visión rusa, riesgos para su propia seguridad.

Su geografía, observando el mapa, si bien es extensa, en esencia es desventajosa, pues no está en Europa plenamente, tampoco en Asia, sus accesos no son ideales dependiendo de estrechos para movilizarse como los del Báltico y Bósforo, que son aparentemente fáciles de bloquear por otras potencias, por lo que requiere controlar sus pasos de forma autónoma y no depender de terceros.

Para Rusia es muy difícil que Ucrania y Bielorrusia estén en la OTAN, deben ser parte de su espacio de poder, debido a que se debilitaría y se vería vulnerable para acceder a océanos del mundo, colindar con la UE y verse aislada dependiendo de terceros países, perdiendo control e influencia.

Rusia es un país rodeado por potencias como USA, China y Europa, pese a su extensión. Para Rusia es muy importante tener control sobre Bielorrusia y Ucrania, pues le permite llegar a Asia central, que para sus redes energéticas son importantes así como para su comercio exterior, sin soslayar expandir su zona de influencia en el medio oriente y contacto mucho más directo con Turquía e Irán.

Desde el punto de vista marítimo comercial, el Cáucaso domina dos mares al este el mar Caspio y al oeste el mar Negro, esa zona es relevante y permite que Rusia salga al mundo sin depender de Europa, explicándose porque su presencia también en Georgia.

Por otro lado, los deshieles que se están produciendo en el Ártico, allana grandes posibilidades para Rusia, pues al poseer la mayor frontera física con dicha región, le permitiría controlar las rutas de transporte desde el Asia hacia Europa, que por la ruta tradicional desde Japón hasta Europa, pasando por las regiones asiáticas, demora aproximadamente cuarenta días actualmente, mientras que por la nueva ruta a través de la zona ártica se reduciría a veinte días aproximadamente.

La posición y accionar ruso, obedece a herencias de la antigua URSS apoyados en el dilema de la seguridad, postulado por Herz, entendiendo o por lo menos usando el justificativo que la OTAN y sus países miembros al expandir su presencia territorial, contar con medios y tecnologías de orden militar y estar cada vez más próximos a sus fronteras constituyen una amenaza para la seguridad de Rusia, en la visión de la ya invocada "fortaleza asediada".

En contrasentido, para defenderse en base a su propia visión, el Estado ruso debe en correspondencia responder a dichas provocaciones y por ende fortalecer sus posiciones, recuperar y expandir sus zonas de influencias, incrementando sus capacidades de tipo militar y tecnológico, contando además con arsenal nuclear heredado de la antigua URSS que los siguen situando como potencia mundial, cuya utilización es compleja pero seguirá constituyendo gran amenaza.

Para lograr influenciar en las zonas de países de la llamada Europa del Este, utiliza como base para sus intervenciones, la presencia de población con ascendencia rusa a quienes los consideran compatriotas, sean o no nacidos en el país, por lo que sin importar que tengan la nacionalidad de los países en los que residen, los trata y busca a través de acciones de Cooperación Internacional enfocadas a la cultura y educación, por ejemplo, apoyarlos.

De esa forma, tienen la base para justificar que deben proteger a sus compatriotas, en los países de interés. Además, que existe presencia de rusos en diferentes países de la región de interés de Rusia, por lo que dicha población cumple por lo menos triple función como mínimo, por un lado mantiene los lazos con Moscú, se entremezclan con las propias sociedades de los países de interés y pueden constituir de ser necesarios en agentes con diversos fines.

Este último, se evidencia en los tres conflictos de análisis en esta sección, pues en Estonia en 2007 los agentes desestabilizadores o de protesta fueron población de ascendencia rusa, quienes generaron disturbios confrontando a población nacionalista y fuerzas de seguridad.

En Georgia, durante el conflicto en 2008, Rusia estableció que las agresiones de ese país debían responderse protegiendo a la población rusa en las regiones de Abjasia y Osetia del Sur, resultando en invasión militar y quedándose en esos territorios bajo dominio de la Federación Rusa.

Ucrania, no fue diferente, pues derivado de conflictos que se fueron sucediendo, principalmente desde el primer quinquenio de 2000, con repuntes importantes en 2013 y 2014 cuando Rusia toma Crimea, suscitando conflictos bélicos y no resueltos desde ese tiempo, hasta que en febrero de 2022, derivaron en la invasión, con reclamaciones por parte de Rusia de territorios del Dombás en el que anexo unilateralmente territorios ucranianos a la Federación Rusa, en la que habitan compatriotas rusos y que deben ser protegidos, en plena guerra, como fueron Donestk, Kherson, Zaporizhzhia y Luhansk.

Esos ataques denotan que Rusia, sigue fines y objetivos definidos en la región, por lo que los países fronterizos con ese Estado buscan anexarse a Europa y a la OTAN para hacer frente a la amenaza, siendo Polonia, Finlandia y Estonia ejemplos de dicha tesis. O por otro lado, buscar la forma de estar bajo la protección rusa, mantenerse "neutrales" y supeditados de forma directa o indirecta a las decisiones de Moscú, siendo ejemplo de lo último Bielorrusia, Azerbaiyan, Kazajastan, Mongolia.

Estos últimos, no son parte de la OTAN, no son parte de la UE, incluyendo a Ucrania y Georgia, que como se observó fueron atacados por Rusia militar y físicamente, al margen de los ciberataques.

En el caso de Corea del Norte y China, merecen análisis individualizados. Los otros países fronterizos, como Noruega, Finlandia, Estonia, Letonia, Lituania y Polonia, son parte de la OTAN y Europa, sea que están dentro la UE o la CEE.

Por otro lado, desde el punto de vista geopolítico, el atacante, identificado como Rusia "aparentemente", debía observar la forma de realizar el mismo, si asumía un ataque armado representaba altos costos en diferentes frentes, con un alto riesgo de confrontación, no sólo con Estonia, también con la OTAN y su Art. 5 de su Tratado fundacional, ya activado en 2001 tras los ataques a USA el 11 de septiembre de 2001.

Paralelamente, si activaba a su diplomacia y buscaba resolver soluciones negociadas dentro del ámbito de las RRII, lo cual no abandono pero tampoco incidió en esta última forma, sobre todo por la proclamada y reconocida soberanía, independencia y autodeterminación al que tienen derecho los países de interés para Rusia, se observa que en caso de negociaciones hostiles contarían con apoyo internacional los primeros, dificultando la labor rusa de expansión en esos territorios por esa vía.

Por lo que, la tercera opción, no por eso única, en la que se pueden mezclar las otras dos, es la de actuar en lo que se denomina la Zona Gris, vale decir, que se escala en el conflicto de formas diversas en contra de los objetivos y se busca su desgaste, a partir de actuaciones que son progresivas y se realizan en tiempo; vale decir, no se improvisan, no son inmediatas y deben seguir una planificación para su desarrollo, implicando que quien las aplique debe tener paciencia y recursos para mantenerla en el tiempo. Rusia, las tiene.

La estrategia multidimensional o multiespacial, que implica su carácter hibrido, responde al carácter de la imposición de los conflictos de forma "pacifica", pero no por eso ilegales o maliciosas, en el que el Estado atacante o en este caso actor dentro de dicha Zona Gris, no viola el Art. 51 de la Carta de las NNUU, pues aparentemente no es un Estado invasor o atacante que está utilizando fuerzas bélicas en contra del o los Estados objetivos.

Pues, en la Zona Gris el Estado que las genera crea conflictos híbridos contra el o los Estados objetivo, que no deben confundirse con Guerras Hibridas convencionales. Por lo que en primera instancia el actor (el que realiza las acciones) buscara conseguir objetivos provenientes de la víctima (sobre el que se realizan las acciones), posicionándose en espacios de ventaja y sin ser detectado en lo posible o de así quererlo el actor. El ciberespacio es ideal para este tipo de acciones en la Zona Gris.

Las actuaciones, por su naturaleza, no pueden improvisarse pues requiere se cuente con la infraestructura, conocimientos, medios y tiempo para desplegar la Zona Gris, lo que implica que las capacidades se van adquiriendo en el tiempo y se trabaja con evidencia empírica en escenarios similares o directos sobre los que se actúa.

En la práctica, Rusia utilizó aparentemente como teatro de pruebas y luego operaciones, a Estonia, Georgia y Ucrania, con despliegue de ciberataques de forma aparentemente similar, pero con herramientas cada vez más avanzadas acorde a la experiencia que fueron acumulando, ya que los mismos se realizaron en diferentes momentos, 2007, 2008 y 2022 de forma concentrada, pero con antecedentes en años anteriores en cada uno de los casos.

Por otro lado, Rusia tuvo que fortalecer sus capacidades para actuar en el ciberespacio, no sólo adquiriendo tecnología, también conociéndola, identificando fortalezas y debilidades, obtener información de diversas fuentes de inteligencia, desplegar a esta última tanto en terreno como virtualmente, potenciar su ciberseguridad, capacitar a su personal, reclutar personal externo, capacitar a población civil, identificar fuentes de energía e infraestructuras críticas, coordinar con su personal local y muchas otras actividades.

Por eso, cuando sucedió lo de Estonia en 2007, los ciberataques tuvieron diversos objetivos interactuando con su personal civil en terreno, provocando disturbios y caos en las calles. En Georgia, el aislamiento comunicacional y el descontrol para coordinar las defensas y en Ucrania, si bien no se provocó quizás el daño que se pretendía, termino con el ataque militar al territorio de este último.

Por lo que, el ciberespacio es primordial para las actuaciones en la Zona Gris, pues los propósitos que se buscan son los de generar cambios en la sociedad y descontrol, para lograr al final anexionar territorios, implantar otro gobierno o régimen político, independizar zonas o territorios dentro de la zona o país de objetivo en el que se actúa. Que en el caso de análisis, para Rusia son de altísima importancia, cuyo desgaste de recursos militares, económicos y tecnológicos en la guerra con Ucrania, generan incertidumbre sobre lo que podría suceder, aunque es sabido que dentro la doctrina rusa se establece la "paciencia estratégica", vale decir, desgastar al enemigo, contando el Estado ruso con los recursos y el tiempo para hacerlo.

Los instrumentos, en la Zona Gris, que se utilizan son primordialmente los del factor psicológico (Gaitán, 2012, pág. 6), a partir de la denominada implantación de la narrativa en primer lugar, explicadas por el Prof. Josep Baqués[61], en la que explica que ese conflicto hibrido no se gana inicialmente con el uso de armas sino el de las palabras, por lo que para lograr efectos buscados, deben realizarse de forma continuada y en el tiempo, lo que implica que no son actividades improvisadas ni aleatorias, sino que responden a una planificación, estratificación, posicionamiento y repetición del discurso, que cale en el pensamiento de la población objetivo.

Para el Prof. Baqués, esto permite que se logre movilizar población civil, que constituye otro de los recursos de la Zona Gris, quienes internamente se encargaran se socavar el orden público,

[61] *Baques, J. (28 de junio de 2021) Global Strategy. Conferencia durante el curso de verano de 2021 sobre Conflictos híbridos y creación de zonas grises, organizado por el Instituto Universitario General Gutiérrez. Acceso web 2023, https://youtu.be/h6CVZE8FGsE?si=QM0AKtTLVAmaJalj*

generaran protestas sin que se las pueda vincular con el generador de la Zona Gris directamente, como se observó en los disturbios en Estonia en 2007.

Utilizando, también medidas del tipo económico, ya sea aprovechando la libre oferta y demanda, en la que los precios se fijaran acorde a lo que establezca la fuente, en el caso de Rusia con los energéticos del cual es propietario, que sin ser directamente sancionatorios pueden provocar alzas en los precios o deficiencias en los suministros de manera de buscar generar algún tipo de bloqueo o escasez que repercute contra la población; siendo más evidente en la guerra con Ucrania y los efectos sobre Europa.

Otro de los recursos que también se utilizan en la Zona Gris, es la distribución de tropas en las zonas fronterizas del país objetivo, que entrarían en actuación cuando los actos realizados en la Zona Gris fallen o se vean afectados por el país objetivo y/o aliados. Tal cual como pasó en Ucrania a finales de 2021 y principios de 2022 antes de la invasión. Coincidiendo con la caracterización del Prof. Baqués en junio de 2021, meses antes de los sucesos en Ucrania.

Desde el punto de vista tecnológico, las TIC representan una forma económica y eficiente para atacar a los objetivos, como sucedió en Estonia, Georgia y Ucrania. Esto si se compara con el costo en caso de conflictos armados, que conllevan recursos insertados desde la producción, traslado y utilización de proyectiles o misiles por ejemplo, utilizar aviones militares, desplazar tropas, personal especializado, activar logística en zonas de operación y mucho más.

Entonces, si el agresor se prepara con tiempo para los ataques en el ciberespacio, contará con el factor sorpresa y constituirá ventaja al momento de atacar infraestructuras críticas, generar descontrol en la población y afectar a las estructuras gubernamentales. Pero para poder solventar dichos ciberataques, la víctima o el país sobre el que se actúa, debe contar con capacidades de ciberseguridad, siendo Estonia y Ucrania ejemplo de aquello, mientras que Georgia fue lo contrario.

La evidencia empírica, demostró que hasta el momento no se llegaron a afectar grandes infraestructuras críticas, no sólo las del tipo energético en los conflictos, que son fundamentales para todos los sectores, también los de reactores nucleares ucranianos u otras. Esto no quiere decir, que desde el punto de vista comunicacional y narrativo no se hayan logrado obtener resultados, lo cual también constituyen problemas para los Estados no sólo en conflicto, también para el Sistema Internacional, por lo que su escalada se supone se incrementará en diversos conflictos que se produzcan en diferentes regiones del mundo.

Sin embargo, toda infraestructura conectada al ciberespacio, posee vulnerabilidades asociadas, ya sea que se aprovechen para obtención de inteligencia o para acceder al sistema, por lo que su protección es importante para evitar ciberataques y generen catástrofes contra la población que no participa en los conflictos. Constituyendo los casos Estonia, Georgia, Ucrania versus Rusia, muestra de aquello, destacando que no se pudo vincular a este último Estado con ninguno de los ciberataques suscitados, generando impunidad legal y de responsabilidad al respecto.

6.2 CASO ISRAEL – PALESTINA (HAMMAS)

6.2.1 ISRAEL

Israel, país cuya historia trasciende más allá de los últimos dos milenios, ha logrado desarrollar su industria invirtiendo y fomentando la I+D+i, convertido en polo a nivel global tecnológico, con avances no sólo en el campo de la salud, medioambiente, agricultura, química, aviación, electrónica, agua, biológicos, farmacéuticos, computación, programas informáticos, ciberseguridad de uso civil y muchas otras.

Desde el punto de vista militar se ha posicionado como líder en la industria, así como en capacidades operativas y de despliegue enfocadas a la seguridad, incluyendo servicios de inteligencia, vigilancia electrónica, inteligencia artificial, naves no tripuladas por humanos, comunicación a distancia, desarrollo de armas, munición, misiles, aplicaciones láseres, ciberseguridad del tipo militar y muchos más.

Es un país con fuerte arraigo religioso, con pluralidad de creencias, con alta incidencia del judaísmo en más del 73% de su población y el resto repartido con musulmanes con 18% de creyentes, cristianos y drusos con el 1.9% de su población cada uno y el 4% practicado por otro tipo de religiones.

Su pirámide poblacional, dan cuenta que su población es mayoritariamente joven, con un promedio de 30 años de edad, en la que la cuarta parte de su población es menor a 15 años, el 64% está comprendida entre mayores de 15 hasta 64 años y el resto 12% son mayores de 64 años.

Desde el punto de vista del Derecho Internacional, no está sujeta a la jurisdicción de la Corte Internacional de Justicia ni de la Corte Penal Internacional, al no contar con instrumentos ratificados.

Su fecha de independencia es el 14 de mayo de 1948, mandato de la Sociedad de Naciones bajo la administración británica en ese año. No cuenta con Constitución formal, por lo que utiliza o se apoya en las denominadas enmiendas de su Declaración de Establecimiento de 1948, la Ley de retorno y sus enmiendas, así como las denominadas Leyes Básicas. En este caso la Knesset o su poder unicameral legislativo es el encargado de aprobar por mayoría reformas o propuestas de los ministros israelís.

Sin olvidar su historia, se tomará en cuenta el corte desde la fecha fundacional del actual Estado de Israel en el siglo XX aproximadamente, para tratar de comprender el contexto de lo que acontece en la región.

La Asamblea de la ONU, propuso dividir el Mandato Británico para Palestina en dos regiones, una para los árabes y otra para los judíos, con rechazo árabe lo que generó conflictos armados en los que la parte perdidosa fue la árabe, acontecimientos denominada la guerra de 1948 suscitada luego de la retirada de británicos. Entonces, en 1949 la ONU reconoce al Estado de Israel y lo admite como miembro de la misma.

Reconocidos como Estado en el Derecho Internacional Público, la población en Israel se incrementó, proveniente principalmente del Medio Oriente y Europa, luego de lo acontecido en la segunda guerra mundial y el holocausto padecido. Sin embargo, los países árabes se resistían a

aceptarlos como Estado, lo que desencadeno en la guerra de los seis días en 1967, resultando en la ocupación de Israel de Cisjordania, Gaza y Jerusalén Este, debiendo además enfrentar a países árabes compuestos principalmente por Egipto, Siria, Jordania y de forma indirecta Irak.

En 1973, derivado de lo ocurrido seis años antes, la tensión en la región continuo, por lo que Egipto, Siria y sus aliados decidieron durante el Yom Kipur judío atacar a Israel de forma sorpresiva, habiéndose preparado para dicho ataque con la adquisición de tanques, misiles antitanques y material bélico de origen soviético.

Las fuerzas israelís nuevamente se hicieron con la victoria, por lo que en acuerdos de paz promovidos por USA, devolvieron territorio ocupado en 1967 a Egipto en 1982, correspondiente a la Península del Sinaí, así como su retiro de territorio sirio, conservando control sobre el Golán. De esa forma logro el statu quo con sus vecinos de la región y los conflictos se enfocaron en grupos islamitas.

La tensión con grupos palestinos, se intensificaron contra Israel, por lo que para mitigar la tensión Israel firma acuerdos provisionales con líderes palestinos en 1990, con autogobiernos en Cisjordania y Gaza, retirándose en 2005 del territorio de Gaza.

Posteriormente, tratando de que las relaciones con la Autoridad Palestina, se lleguen realizar se negoció el estatus definitivo en 2014, para luego también firmar acuerdos de normalización con otros Estados árabes, a través de la intervención de USA, resultando en los "Acuerdos de Abraham" con Marruecos, Emiratos Árabes Unidos y Bahréin en 2020, y Sudan en 2021.

Al margen de su liderazgo en tecnología alcanzado por Israel, desde el punto de vista de RRNN, descubrió gas natural en Tamar y Leviatán, lo que lo sitúa en un proveedor importante del energético en la región. Para lograr la explotación de dichos yacimientos, negoción a través con USA acuerdos entre Israel y Líbano, al saber cuál es su frontera marítima establecida.

El actual primer ministro israelí, estuvo al frente del Estado desde 2009 hasta 2021, retornando al poder en 2022 y liderando al país actualmente. Lo que lo convierte en el líder con más tiempo al frente del Estado.

El 07 de octubre de 2023, Israel sufrió ataques por parte del grupo armado Hamás, en la zona sur del Estado de Israel, con efectivos armados del grupo provenientes de la Franja de Gaza, lo que provocó la reacción de Israel por parte de las Fuerzas de Defensa de Israel (FDI), por lo que en respuesta el Primer Ministro Benjamín Netanyahu, declaró la guerra el 08 de octubre y el 28 de octubre se desplegaron ataques terrestres dentro de Gaza de alta intensidad, procurando rescatar rehenes israelíes capturados por invasores de Hamas que los capturaron en su incursión al territorio sur israelí, ocultándose en la red de túneles que poseen y que abarcan prácticamente todo el territorio de Gaza, con centros de comando debajo de escuelas y principalmente hospitales, utilizados como camuflaje táctico para evitar ser descubiertos.

La complejidad del conflicto, en el que sólo los primeros días, se estima se lanzaron más de 3 ó 4 mil misiles desde la Franja de Gaza contra Israel, más la agresividad en sus incursiones del 7 de octubre, con el asesinato de familias enteras, incluyendo bebes, niños, adultos mayores y personal no combatiente por parte de Hamás a generado alta tensión en la región.

Conflicto armado que se está produciendo en todos los espacios, terrestre, aéreo, marítimo y ciberespacio; este último que no sólo involucra a Hamas, también a sus aliados contra Israel, por lo que dados los acontecimientos se pasará a describir lo que acontece allí.

6.2.2 PALESTINA

Se hará una corte en la historia palestina[62], a partir de 1917 luego de la Primera Guerra Mundial. Durante 1917 a 1947, Palestina fue parte del territorio otomano, que pasaron a ser administrados por mandato de laa Sociedad de las Naciones, bajo administración británica. Dicha administración fue partidaria del establecimiento en la denominada Palestina de un hogar nacional para el pueblo judío, introducido en la Declaración de Balfour.

Entre 1922 y 1947, bajo la administración británica, se produjo la primera ola de migrantes israelíes de forma masiva, desde Europa oriental principalmente. Se observaron incrementos en la década de 1930, debido a la persecución de la Alemania nazi en esos años. Por la parte árabe hubo rechazo a las migraciones israelíes, provocando que ambos bandos se enfrenten repetidamente con actos violentos. Siendo difícil el manejo de la situación beligerante entre israelíes y palestinos, la administración británica acudió ante la ONU en 1947, para que se resuelva el problema desbordado en esa región.

La ONU, pone fin el mandato administrativo británico y propusieron dividir el territorio en disputa en dos Estados independientes, uno para los israelíes afectado por el holocausto y la guerra mundial concluida, la otra parte para el pueblo árabe palestino, en el que Jerusalén estaría bajo un régimen internacional, términos reflejado en la Resolución 181 (II) de 1947 de la ONU.

Israel proclamo su independencia en 1948, por lo que los árabes se unieron para confrontarlo militarmente, resultando en que Israel terminó ocupando más territorio, incluido parte de Jerusalén. Por lo que debido a ese ataque árabe contra el nuevo estado, población árabe huyo de los territorios ganados por Israel.

El territorio restante de lo asignado inicialmente, estuvo bajo control de Jordania y Egipto, acorde a la Resolución 181 de la ONU.

En 1967 la coalición árabe, nuevamente ataca a Israel y está nuevamente vence en los combates ante los ataques que sufrió, ocupando más territorio, incluyendo la Franja de Gaza y la Ribera Occidental, Jerusalén oriental que fue parte de Israel. Lo cual derivó nuevamente en que población árabe se desplace.

La ONU mediante Resolución 242, a través del Consejo de Seguridad de la ONU, establecieron principios para una paz justa y duradera, para esto Israel debía retirarse de los territorios ocupados derivados de la guerra, solucionar el problema de los refugiados, conclusión de beligerancias entre las partes o discusiones al respecto.

Sin embargo, en 1973, nuevamente Israel fue atacada, por lo que la ONU aprobó la Resolución 338, instando a que las parte en conflicto inicien negociaciones de paz. Para luego en 1974 la Asamblea General de la ONU reafirmara derechos inalienables del pueblo palestino a la libre determinación, su independencia nacional, soberanía y retronó de los refugiados.

---

[62] *ONU. (2023). La cuestión Palestina. Historia de la cuestión Palestina. Acceso web 2023,* https://www.un.org/unispal/es/history/

En 1975, la Asamblea General instauro el Comité para el Ejercicio de los Derechos Inalienables del Pueblo Palestino, reconociendo a la Organización de Liberación de Palestina (OLP) como observador en la Asamblea y conferencia de las NNUU.

Entre 1977 a 1990, las tensiones en vez de disminuir escalaron aún más, por lo que en 1982 Israel decide eliminar a la OLP, invadiendo el Líbano, las tropas del ejército de la OLP se refugiaron en países vecinos, mientras que los refugiados palestinos que se encontraban en los campamentos de Sabra y Shatila, según indica la ONU, fueron masacrados.

Por lo que en 1983, la Conferencia Internacional sobre la Cuestión de Palestina, decide oponerse a los asentamientos israelíes y que se cambie el estatus de Jerusalén, reconociendo el derecho a que los Estados vivan dentro de los límites que fueron reconocidos en Asamblea, así como el reconocimiento del derecho inalienable de Palestina.

Pero no contentos con eso, en 1987 se levanta el pueblo palestino contra la ocupación israelí, denominada Intifada, con ataques terroristas y respuestas por parte del ejército israelí con muchos muertos por medio, además de heridos.

En 1988 en Argel, el Consejo nacional de Palestina proclamo el establecimiento del Estado de Palestina. En 1991, se celebra Conferencia de Paz en Madrid, España. Para eso se diseña la estrategia en la que Israel negocie la paz con los Estados árabes y por otro lado lo haga con Palestina, en base a las Resoluciones 242 y 338 de 1967 y 1973, respectivamente.

Dicha conferencia concluyo con el Acuerdo de Oslo, en el que Israel reconoció a la OLP como representante del pueblo palestino. Lo que significó que Israel se retire de ciertos territorios parcialmente, se produzcan elecciones del Consejo Palestino, se elija al Presidente de la Autoridad palestina, administración de zonas palestinas autónomas por su propia autoridad, liberación de palestinos detenidos en los combates, quedando pendiente la discusión sobre el estatuto permanente de Palestina, que se realizaron en 2000 y 2001 en USA, sin llegar a ningún acuerdo.

A pesar de los intentos, en 2000 estalló la segunda intifada, por lo que Israel construyo muros de separación dentro del Territorio Palestino Ocupado en la ribera Occidental, en la que la Corte Internacional de justicia fallo declarándola ilegal. En 2003, se buscó la solución biestatal, tranzados una hoja de ruta por parte de Estados miembros del Consejo de Seguridad, USA, Rusia, UE y la ONU, aprobando la Incoativa de Paz Árabe.

Logrando que en 2003 se firme un acuerdo de paz no oficial, para luego en 2005 se logre que Israel retire a sus tropas y población de Gaza, controlando sus fronteras, costas y el espacio aéreo.

En 2006 se realizaron elecciones parlamentarias en Palestina y en 2007 asumió el poder Hamás en base al uso de las armas, por lo que Israel bloqueo los territorios, para que entre 2007 a 2008 tampoco se logre acuerdo alguno sobre el estatus peramente. Por lo que Hamás ataco a Israel con cohetes en 2008 e Israel ataco Gaza vía terrestre en la operación denominada “Plomo Fundido”.

Los años siguientes los conflictos no cesaron, en 2011 el Presidente palestino M. Abbas solicito a la ONU admita a Palestina como Miembro de la NNUU, la UNESCO si la admitió, pero en 2012 nuevamente se generó violencia entre Gaza e Israel, en la que Egipto tuvo que intervenir para un alto al fuego.

Por lo que para trata de apaciguar la escalada de violencia, el 29 de noviembre de 2012 la Asamblea General de las NNUU reconoció a Palestina como Estado observador no miembro de la OI, para luego en 2014 la propia ONU declara el año de solidaridad con el el Pueblo Palestino.

En el mismo año, 2014, nuevamente hubo ataques entre Gaza e Israel, el Consejo de Seguridad nuevamente trato el problema en 2016 y en 2017 USA reconoció a Jerusalén como capital de Israel, con traslados de su embajada y otros países a dicha ciudad.

Ya en 2020, USA medió para que Israel y Emiratos Árabes Unidos, Burén, Sudán y Marruecos, logren que las relaciones con Israel se normalicen, firmando el Acuerdo de Abraham. Luego la propia Asamblea General de la ONU pidió a la CIJ que emitiera una Opinión consultiva sobre la ocupación de Israel desde 1967 e implicancias para los Estados miembros.

La ONU el 15 de mayo de 2023, conmemoró el 75 aniversario de la Nakba, que es el dia en que población palestina huyo de sus hogares debido al nacimiento del Estado de Israel en 1948.

El 7 de octubre de 2023, miembros armados de Hamás invaden territorio israelí en zonas fronterizas con la Franja de Gaza, asesinado a población civil, por lo que Israel declara la guerra y la lucha hasta la extinción de Hamás, generándose movimientos de apoyo a Hamás en diferentes lugares del mundo en un principio, así como el rechazo contundente de muchos Estados a los ataques perpetrados por dicho grupo, que además tomo rehenes civiles para intercambiarlos por sus prisioneros, llegando a asesinar a rehenes.

Grupos árabes han manifestado su respaldo a Hamás, como Hezbollah, pero Estado como Irán, Qatar, Argelia, Afganistán, Libia, Venezuela, Chile, Iraq, Yemen, Sudán, Túnez, Líbano, Siria, Iraq. Estados, que mayoritariamente, se encuentran en las cercanías de la zona en conflicto, excepto los sudamericanos,

Los actuales combates también se están realizando en el ciberespacio, en primera instancia atacando páginas web y redes sociales de hacktivistas, por lo que el despliegue al respecto se analizará abajo.

6.2.3 DESCRIPCIÓN CIBERATAQUES

Los ataques del 7 de octubre de 2023, no estuvieron ausentes de confrontaciones en el ciberespacio, generando la participación de bandos partidarios por cada uno de los países en conflicto, con la presencia de piratas informáticos, hasta noviembre de 2023, se detectaron más de 65 piratas informáticos propalestina y en el lado israelí aproximadamente quince[63].

Los ciberataques se produjeron sobre sitios públicos israelíes, empresas y personas. Destacándose el ataque a la aplicación de advertencia de ataque con misiles y cohetes que posee la población israelita, de nombre Alerta Roja, que estuvo fuera de servicio por horas, siendo los responsables grupos propalestina.

Según el reporte, se logró identificar grupos de Pakistán, Malasia, Bangladés, Indonesia, así como rusos como el grupo Anonymous Soudan, el grupo iraní Cyber Av3ngers, sospechando que haya sido también amplificador de los ataques perpetrados.

[63] *Diario Octubre. (2023). La ciberguerra entre Israel y los palestinos. Acceso web 2023, https://diario-octubre.com/2023/11/25/la-ciberguerra-entre-israel-y-los-palestinos/*

Israel, estaría actuando a través de grupos indios proisrael, como el grupo Cyber Force. Según informó la página Security Report[64], poco después del ataque muchos grupos políticos en la red o hacktivistas, tomaron partido en el conflicto, en la Dark web grupos como Killnet y Anonymous Soudan declararon su apoyo a Palestina, iniciando este último con ataque DDoS a servidores israelíes forzándolos a que sus páginas colapsen.

Por su parte, Killnet dejo fuera de funcionamiento durante horas, las páginas web del gobierno y la agencia de seguridad israelí Shin Bet. Atacándose también a la página del periódico israelí The Jerusalem Post.

Un tercer grupo de nombre AnonGhosts, creo una aplicación de alerta de cohetes y misiles para confundir a la población israelí, al extremo que avisaron alertando de un misil nuclear, con el propósito de generar caos generalizado.

Compañías especializadas del sector informático con presencia mundial, tales como Intel, Nvidia, Microsoft, Google, Facebook, Apple, están tomando medidas de ciberseguridad al estar instaladas en Israel, siendo uno de los sectores de alta importancia para la economía israelí, que de generarse inseguridad tendría impacto negativo para el país.

Inclusive el hecho de que sus empleados, reservistas del ejército, sean convocados por el gobierno para defender su Estado.

Para Check Point Software Technologies, según nota del editor de Ciso Advisor de Brasil[65], los ataques sobre Israel se incrementaron en un 20% durante la guerra, destacando que los ciberataques al margen de frecuentes también fueron sofisticados, iniciando como ya se mencionó con ataques de DDoS.

Sin embargo, luego grupos iraníes denominados APT (amenaza persistente avanzada), atacaron utilizando malware, rasonware y limpiadores potentes, con dirección a organismos gubernamentales, empresas proveedoras del gobierno, empresas y entidades públicas.

Surgiendo el grupo Cyber Toufan, que amenazó atacar a organizaciones israelíes, incluyendo empresas, como Signature-IT, dedicada al comercio electrónico y alojamiento de páginas web. Logrando sacar de esa compañía datos de millones de usuarios, correos electrónicos, con datos de contacto de los usuarios.

También, en el ciberataque el referido grupo, logró filtrar información de la empresa israelí Max Security, dedicada al ciberseguridad y geointeligencia, así como su empresa colega Radware, también a la propia Autoridad de Innovación de datos que impulsa la innovación en Israel.

Para Messing, en la misma publicación, el grupo Cyber Toufan son operadores financiados por Irán, realizando análisis sobre las formas de realizar los ciberataques y comportamientos detectados en otros casos.

---

[64] *Security Report. (11 de octubre de 2023). Comienza la ciberguerra entre Israel y Palestina con ataques de grupos hacktivistas. Acceso web 2023, https://www.securityreport.com.br/ciberguerra-se-inicia-entre-israel-e-palestina-com-ataques-de-grupos-hacktivistas/*

[65] *Ciso Advisor. (24 de noviembre de 2023). Nota del Editor. Ciberataques crescem com expansao da guerra Israel-Hamas. Ataques cibernéticos tem aumentado em frequencia e sofisticacao a medida que o conflito Israel-Hamas se intensifica. Acceso web 2023, https://www.cisoadvisor.com.br/ciberataques-crescem-com-intensificacao-da-guerra-israel-hamas/* .

Lo descrito hasta aquí no sólo refleja que las confrontaciones en el problema entre Israel y Palestina, se limita a los espacios físicos, de manera similar a lo sucedido entre Rusia y los países de Europa del Este, el ciberespacio confluye en enfrentamientos con ciberataques de diversas fuentes.

La proliferación de grupos de hackers o piratas informáticos como los llaman algunas publicaciones de prensa, denotan que cada vez aumentan y están organizados, si a eso se le suman recursos de países como Irán y sus aliados, que los financian, generan ya no sólo preocupación sino la necesidad de obtener cada vez mejores y más potentes herramientas de ciberseguridad que hagan frente a estos.

En el actual conflicto, de las notas repasadas en esta parte del trabajo, debe llamar la atención la violación a la seguridad de empresas de Israel de ciberseguridad, por lo que si estas últimas son las responsables de resguardar a sus clientes y no lo hacen correctamente, dejando se filtren datos, generan no sólo desconfianza, también preocupación y desesperación, cuestionándose en quien se podría confiar y que requisitos deberá cumplir quien se haga cargo de la ciberseguridad cuando sean requeridas.

El conflicto que se está llevando a cabo en 2023, muestran que el sector de la ciberseguridad, tiene que trabajar de forma más intensa y eficiente, pues a estas alturas después de poseer experiencias en conflictos en el ciberespacio, obligan a contar con mejores medidas y herramientas a favor de sectores críticos, como los gubernamentales y estatales, empresariales, de seguridad incluyendo ciberseguridad, entidades financieras, sectores de la salud, energía y prácticamente todos los que estén conectados a internet o a la red.

Por otro lado, el papel de Irán en el conflicto, muestra su activa participación, aunque como es regular deberá "demostrarse" su participación en los ciberataques de forma directa o indirecta, creando otro problema a resolver, no bastando las directrices del Manual de Tallin 2.0, por ejemplo, cuya redacción y reglas brindan luces al respecto, pero no solucionan en la práctica al problema, que se traduce en la aplicación o efectivizarían de las mismas.

6.2.4 IMPLICANCIAS GEOPOLÍTICAS Y DEL CONFLICTO

Israel se enfrenta a desafíos fronterizos por su ubicación geográfica, al noroeste y al sur, ubicado en un lugar donde los recursos son escasos y su salida marítima al mediterráneo es una fortaleza para su conectividad con la región y el mundo.

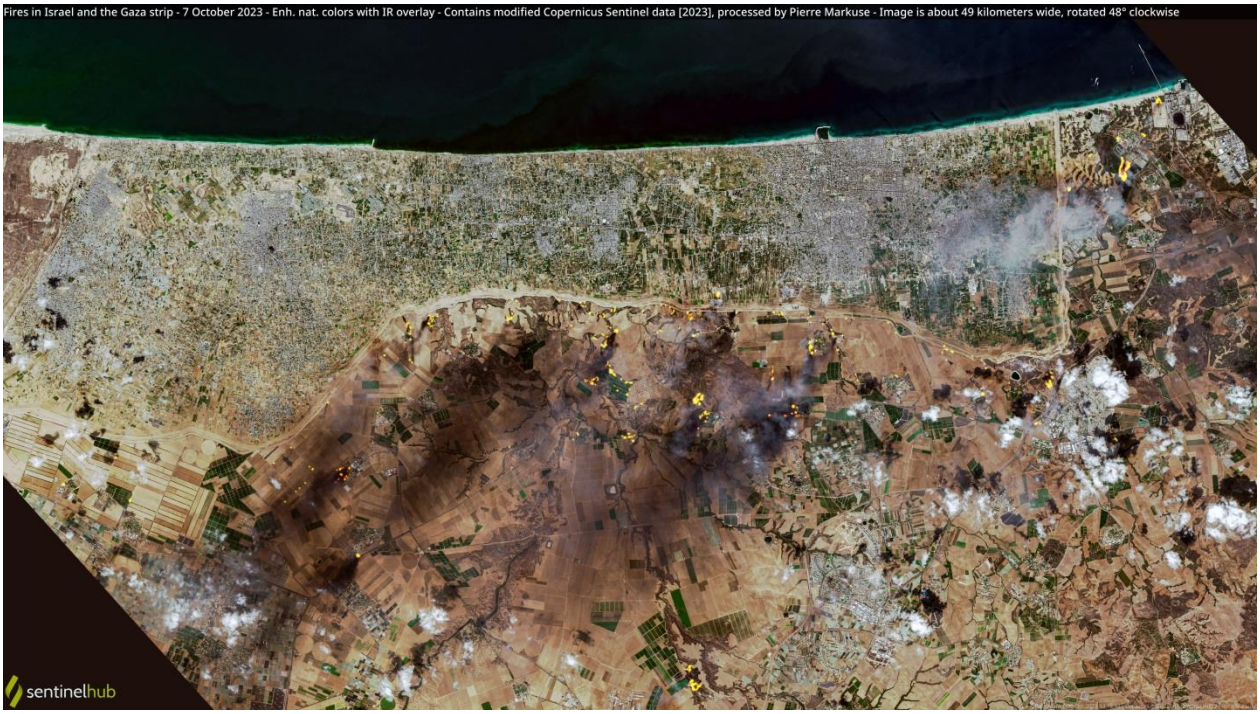
Dividido en tres zonas, la del llano costero es la parte central del país y concentra a las principales áreas industriales, de comunicación como aeropuertos y zonas urbanas de relevancia como Tel Aviv, Jaifa y Jerusalén. Costa que se extiende a lo largo de la zona mediterránea, pero con poca profundidad, esto tiene implicancias para su defensa, pues la proximidad de las zonas significa que ante posibles ataques entre las zonas continuas, en caso de misiles, estos llegarían en cuestión de minutos cuya defensa con las tecnologías militares existentes es difícil de mitigar.

La geografía de Israel, obliga a que su defensa deba instalarse y proteger cada zona elevada, pues le permite tener visión no sólo en las zonas continuas dentro su territorio, también controlar las zonas cercanas en las fronteras, principalmente en el norte del país, acechada por las fuerzas de Hezbollah, que son protegidas por el gobierno iraní y declaradas su brazo armado, contando con potencia de fuego elevado a partir de misiles y drones, con el suministro adicional de recursos económicos por parte de Irán.

Esto significa que Israel protege cada ubicación ventajosa que posee, ya no sólo por su defensa, fundamentalmente por su sobrevivencia, en un territorio en el que ninguno de los dos pueblos habitantes en él, pueden expandirse a otro lado.

En el caso de Cisjordania, a través de asentamientos legales e ilegales de israelitas, es relevante para buscar la forma de neutralizar a la población de Palestina, pues ya no se trata sólo de un tema de respeto al Derecho Internacional, sino de no perecer como país, por lo que la denominada zona "C" está siendo poblada entre la población palestina de forma impuesta pero necesaria para Israel, lo cual implica que se están violando posiblemente acuerdos y resoluciones de la ONU, pero tampoco esta última a través de su Consejo de Seguridad, el cual está dividido, actuará dentro de dicho territorio, debiendo encontrar salidas imaginativas, que para colmo en un territorio en el que prácticamente todos los días se producen confrontaciones, es complicado, más aún luego de los ataques del 7 de octubre de 2023.

Esos asentamientos, provocan el ensanchamiento de esa zona estrecha que posee Israel y el potenciamiento de una zona que debe poseer para evitar que el Estado de Israel sea fraccionado o lo peor extinguido. Debiendo dominar el norte, a Cisjordania y resguardar a sus zonas urbanas.



Incendios en Israel y la franja de Gaza – 7 de octubre de 2023. Foto: Datos modificados de Copernicus Sentinel [2023], procesado por Pierre Markuse (Wikimedia Commons/CC BY 2.0). https://commons.wikimedia.org/wiki/File:Fires_in_Israel_and_the_Gaza_strip_-_7_October_2023_(53245908850).jpg

La fortaleza israelí, se apoya en su desarrollo tecnológico, convirtiéndose en un país en el que se fomenta el emprendimiento, apoyado en la I+D+i, lo cual implica que su sistema informático es relevante para el manejo de sus infraestructuras críticas y sobre todo sus capacidades militares, dado el constante asedio al cual están sometidos.

En el que su escudo de hierro, para eliminar misiles, funciona de manera permanente, dando muestras por su efectividad de las capacidades tecnológicas que posee Israel. Con innovaciones

que han insertado el uso de rayos laser para gestionar las respuestas contra misiles, lanzados principalmente desde la Franja de Gaza, con mayor rapidez y así proteger a su población.

Al sur, por otro lado se encuentra la zona Negev, acoge la ciudad portuaria de Eilad que conecta a Israel con el Mar Rojo y por ende con el comercio internacional, de valor importante para evitar además cualquier tipo de bloqueo marítimo en el mediterráneo. En el Negev, también se encuentra Gaza y adicionalmente la península del Sinaí con la que tiene frontera.

La península es una zona muy compleja estructuralmente por la geografía que posee, siendo aprovechada por el contrabando, refugiados y yihaidistas para esconderse en él. Dicha morfología de la región, ayuda a evitar que sus vecinos Egipto, Jordania y Arabia Saudita ataquen al país y puedan llegar directamente al centro del país, siendo una ventaja defensiva geográfica por ahora.

En el norte de Israel, se encuentra Galilea, siendo relevante por contar con zonas acuíferas, ubicándose en esa región las zonas agrícolas principales, así como las industrias manufactureras de Israel. Con fronteras complejas limitando al norte con Siria y Líbano, control militar israelí de los Altos del Golán de sobre 1200 km de los 1800 km que lo constituyen, 240 km a cargo de la UNDOF o Fuerza de las Naciones Unidas de Observación de la Separación desplegada desde 1974, y el resto bajo soberanía Siria. Esta última región limita con Jordania, Siria y el Líbano.

En dicha zona, se generan también conflictos, pues en el Líbano están apostados miembros de Hezbolah, Siria ha participado en ataques contra Israel desde su formación en 1948 y Jordania firmo un acuerdo de paz con Israel en 1994, que se ve amenazado por lo que acontece en la actual crisis, pues para el rey jordano Abdalá II, sí debido a estos se vuelve a desplazar a población palestina de Gaza y Cisjordania, significará una declaración de guerra para Jordania, que desde los anteriores combates en 1948 y 1967 refugió a millones de palestinos en su territorio[66].

Para la región, Israel es un aliado que es considerado líder en tecnología, por lo que esa reputación bien ganada, se ve amenazada por los ciberataques que está recibiendo, el conflicto no sólo detuvo la firma de acuerdos con Emiratos Árabes Unidos, sino pone en riesgo la estabilidad de la región, pues Irán busca por otro lado expandir su influencia en el mundo árabe y para países como Emiratos Árabes Unidos y otros aliados, el estado islámico constituye una serie amenaza, debiendo buscar aliados a través de Israel como USA y su fuerza militar, UE y por ende la OTAN.

Para Israel, las afectaciones de los conflictos, también implican que empresas de tecnología, reevalúen su presencia en su territorio, pues lo que se busca al margen de avances tecnológicos, talento humano, impulso para la innovación y otros, es seguridad, estabilidad, paz para desarrollar sus proyectos e iniciativas. Lo que las principales compañías mundiales en tecnología no están viendo en este momento en territorio israelí.

Lo avanzado por las Fuerzas de Defensa de Israel, FDI, en Gaza, no podrá deshacerse pero se podrá buscar una salida al conflicto, en el que Hamás por más mermado y a punto de extinguirse que este, no desaparecerá, más aún si cuenta con apoyo de países enemigos de Israel, siendo el

[66] *Amirah F., H. Real Instituto El Cano. (2023). Jordania ve en las acciones de Israel en Gaza y Cisjordania una amenaza existencial.* https://www.realinstitutoelcano.org/analisis/jordania-ve-en-las-acciones-de-israel-en-gaza-y-cisjordania-una-amenaza-existencial/

principal Irán y sus grupos satélites a quienes no duda en financiar y apoyar, como Hezbollah y otros.

El uso de las TIC, demuestra que las comunicaciones se pueden interrumpir y generar caos, siendo herramientas de ciberataque que se seguirán usando en los conflictos, más aún ante una sociedad hiperconectada que necesita estar al corriente de lo que acontece prácticamente en tiempo real y en cualquier lugar. Siendo de valor en las ciberguerras y ciberataques que se promuevan en los conflictos.

6.3 IMPLICANCIAS PARA LA COOPERACIÓN INTERNACIONAL

Los acontecimientos de 2007, 2008 y 2022, en Estonia, Georgia y Ucrania, no siendo los únicos, han impulsado a la Cooperación Internacional a que a través de sus OI, asuman diversas medidas enfocadas a la ciberseguridad.

La intervención que han brindado tanto en Estonia como en Ucrania, a través de los grupos de respuesta o reacción de ciberseguridad, conocidos como CERT, han demostrado la importancia que significa el actuar de forma coordinadas pero sobre todo usando precisamente la Cooperación entre Estados como herramienta para mitigar la escalada de conflictos que se generan en el ciberespacio.

Si bien, Estonia y sobre todo Ucrania, han podido enfrentar los ciberataques sin que generen mayores daños a sus infraestructuras críticas, con reacciones rápidas por parte de OI tales como la OTAN y la UE, que como se describió cada vez cuentan con organismos y políticas dirigidas a potenciar la ciberseguridad en sus zonas de influencia a favor de la población que protegen; han encontrado en la Cooperación Internacional la respuesta para ganar tiempo, experiencias, conocimientos, optimizar recursos, evitar repetición de esfuerzos y trabajar coordinadamente en un problema cada vez más frecuente y relevante.

La utilización de la denominada Zona Gris, por parte de algunos Estados, para buscar desestabilizar el statu quo, denominados Estados revisionistas o inconformes, que buscan crear un Nuevo Orden Internacional acorde a sus intereses, están ayudando a que el resto de Estados se preparen de mejor manera, aunque no siempre lo harán todos y de hacerlo no siempre será a tiempo.

Por otro lado, la Cooperación Internacional está trabajando en establecer límites para las actuaciones en el ciberespacio, en el que se establezca deberes, responsabilidades, derechos y garantías para que sea utilizado de manera responsable, libre, soberana, pacifica, sin que eso signifique que se caiga en libertinaje, abuso, impunidad, caos y destrucción.

El DI es primordial para la regulación no sólo del derecho de gentes, también de su correcta aplicación, para lo cual se apoya precisamente en la Cooperación Internacional, que tiene el desafío de articular de forma practica la aplicación de normas del DIH y los DDHH al ciberespacio.

Para lograr el propósito, deberán los Estados, como indica el Prof. Baqués, sobre todo la Cooperación Internacional, seguir los lineamientos expuestos a continuación:

1) Potenciar las instituciones y su estructura. Incluye establecer credibilidad y confianza.

2) Potenciar las propias capacidades, las regulaciones normativas, los servicios de inteligencia con expansión al ciberespacio, estructuras críticas y no críticas, fortalecer la Cooperación Internacional.
3) Desarrollar comunicación estratégica, debiendo interactuar con la Cooperación Internacional para capacitar a especialistas acerca de la forma y sobre todo dominen que deben comunicar, que al final repercutirá en sus sociedades y evitara el desorden y caos.
4) Desarrollar sistemas de alerta temprana, para lo cual deben invertirse en capacidades de vigilancia, detección y respuesta ante ciberataques que aprovechando la Zona Gris se introducen a los sistemas antes de ser detectados.
5) Mejorar la inteligencia en sus diversas fuentes, incluyendo las de Redes Sociales, para lo cual la Cooperación Internacional con OI de relevancia como la OTAN, UE y ONU cuentan con acervo de conocimientos prácticos que deben ser utilizados para ganar tiempo y camino para confrontar ciberataques, ciberamenazas y posibles ciberguerras.
6) Adquirir capacidades no sólo defensivas, también ofensivas para repeler y contraatacar ciberataques y confrontar de ser necesario ciberguerras, para lo cual deberá contarse con los puntos anteriores ya desarrollados.
7) Conformar grupos especializados en las Fuerzas Armadas o de Seguridad, en nuevas doctrinas y nuevos perfiles de combatientes, con conocimientos avanzados en diversas disciplinas, no sólo tecnológicas, también RRII, sociología, psicología, geopolítica, etc.
8) Proteger infraestructuras críticas, estableciendo protocolos, grupos de respuesta a las crisis y de coordinación con la Cooperación Internacional.
9) Potenciar las estructuras de ciberseguridad cada día, coordinando esfuerzos con la Cooperación Internacional, para optimizar recursos.
10) Denunciar, públicamente ciberataques detectados, creando rechazo, preparación a favor de la población para evitar sean sorprendidas con fake news, por ejemplo, o generación de narrativas perjudiciales para la estabilidad del país.

Lo propuesto por el Prof. Baqués, sí se observa el trabajo de las OI ya se viene realizando, no significando que ya se haya logrado, la Cooperación Internacional está trabajando en el tema, significa un gran desafío por lograr para los Estados, habiéndose iniciado de diversas formas en diversos países.

Cobrando altísimo valor la Cooperación Internacional para mitigar los problemas que surgen cada día, inclusive en conflictos armados, generando escenarios para que se busque y encuentre la paz, no todos los Estados actuaran en consonancia, pero será precisamente la Cooperación entre otros Estados el que al final lograran contener a los disidentes y problemáticos, pues a ninguno le conviene vivir en constante conflicto o aislado del Sistema Internacional y el ciberespacio es una continuidad de la realidad de la humanidad en el que la ciberdiplomacia jugara roles importantes frente a los avances tecnológicos que son cada vez más disruptivos.

CAPITULO III

1. *CONCLUSIONES*

Originalmente, los sistemas informáticos, tanto HW como SW, no fueron concebidos, por lo menos comercialmente, para fines ilícitos, sino como herramientas de colaboración a las tareas realizadas por las personas y sus diferentes organizaciones.

La degeneración en el uso de esos recursos para fines contrarios a los propósitos de su creación afecta a todos los usuarios y cuando estos últimos son entes institucionales estatales o gubernamentales, así como OI que manejan recursos sensibles a través del uso de las TIC, se generan los conflictos a la seguridad, más aun si a través de los recursos informatizados se manejan infraestructuras sensibles, como plantas nucleares, energéticas, de comunicación, transporte, hospitales, armas y otros.

Luego de la Segunda Guerra Mundial, se generaron muchos cambios en la humanidad y en la vida de los propios Estados, no sólo el nacimiento de la ONU y su carta fundacional marcaron guías relevantes para el Sistema Internacional, vino aparejada con el desarrollo tecnológico, pues la Inteligencia Artificial en concepto nació en esos años como la conocemos hoy, surgieron avances relevantes en la electrónica con la miniaturización de los transistores y el nacimiento de los avances en los chips, las bombas atómicas también fueron parte de esa historia y la necesidad de mantener el equilibrio y la paz en el mundo es un clamor.

Los avances en las TIC cada vez acercan a la humanidad a la automatización, investigaciones sobre la posibilidad de conectar al hombre a las maquinas, el desarrollo de la IA, la posibilidad de encontrar superconductores, las computadoras cuánticas, la nanominiaturización de los procesadores, los avances en robótica, construcción de exoesqueletos y muchos más.

Significa que el ciberespacio cada vez estará más cerca de la realidad físicamente que sólo en el mundo virtual. Esto quiere decir, que el hombre está delegando más el manejo de sus sistemas o infraestructuras críticas a las máquinas y estas trabajan en base a programas junto con componentes físicos, por lo que el sistema debe ser protegido, necesita ser cuidado y la ciberseguridad requiere cada día mejor y mayores herramientas.

Los ciberataques por ahora han logrado afectar bases de datos, obtener información de estos, desconfigurar páginas web, detener el funcionamiento de las redes durante espacios de tiempo no tan prolongados, interrumpir comunicaciones, suplantar claves y autenticaciones, cortar o afectar redes de distribución energética, interrumpir señales de telefonía e Internet y otras más.

Sucesos que se han presentado, no dan cuenta de destrucción o daño relevante a infraestructuras críticas, siendo quizás lo más extremo la explosión o afectación catastrófica de una planta de energía nuclear, el control sobre naves de transporte con saldos fatales de pérdidas de vida, apoderarse de vehículos o provocar el lanzamiento de armas de destrucción masiva o en masa.

Eso no quiere decir que la búsqueda para lograrlo se haya detenido, aún no se logró y eso no significa que no se podrá hacer, obligando a que los Estados trabajen de forma mucho más ágil y

responsable en adquirir capacidades de protección junto a medidas de regulación y sanción al interior de sus territorios y en el Sistema Internacional.

En el trabajo, se observa como OI de tipo mundial y regional, lideres dentro del Sistema Internacional han asumido el desafío, cuyo trabajo lleva varios años y sigue en continuo desarrollo, demostrando que la base del fortalecimiento de sus respectivos esfuerzos se apoya en la Cooperación Internacional, que como ya se refirió es la herramienta de mitigación que se está utilizando para confrontar ciberataques a los Estados.

Para OI como la OTAN, dentro sus Conceptos Estratégicos de 2022, ha definido a países como Rusia y China como generadores de conflictos y ataques en el ciberespacio, por lo que son considerados riesgosos para la seguridad internacional.

La UE, si bien no declaró a esos países como parte del problema, empíricamente los consideran así contra la ciberseguridad no sólo en la región sino a nivel global, razón por la que de forma similar a la OTAN ha delineado rutas para procurar disminuir y en lo posible eliminar su dependencia con esos países, principalmente China de quien se adquieren muchas componentes para sus propios sistemas informáticos y de ciberseguridad.

La implementación de estándares y certificados que deben cumplir los equipos y componentes a ser comercializados dentro la UE respecto a la garantía de ciberseguridad que deben poseer, está equilibrando el mercado por un lado y fortaleciendo la oferta de servicios y productos de ciberseguridad en la Unión.

Dichas iniciativas también fortalecen la relación entre los gobiernos de los Estados y la sociedad civil y empresarial, pues de la mano no sólo están construyendo estándares y reglas, también interactuando para fortalecer estructuras, apoyados en la experiencia y visión que poseen, principalmente las compañías.

Desde el punto de vista defensivo, la UE a través de su plan Brújula Estratégica, en actual desarrollo, busca lograr contar con capacidades militares y tecnológicas para 2030 fortalecidas, en el que incluyen a la ciberseguridad y por ende el ciberespacio como escenario de actuación.

Los sistemas de salud y dispositivos biomédicos, son críticos para el mantenimiento de la vida, siendo prioritario al margen de los sistemas de defensa, blindar los mismos de ciberataques, así como los sistemas de energía del cual dependen, ingresando en sector de la IoT y la conectividad con las redes 5G, que cada día se van implementando, representando otro desafío a la ciberseguridad.

Los sistemas de defensa como se observó en el trabajo son muy importantes para los Estados, en los que armas y transportes no tripulados, se utilizan cada vez más en los conflictos, dependiendo de líneas de comunicación en el ciberespacio con sus pilotos, debiendo encriptar comunicaciones y que por otro lado son susceptibles de ser descifradas con ayuda de la IA y equipos de procesamiento computacional cada vez más sofisticados.

El ciberespacio es relevante para la geopolítica, si bien no cuenta con territorio, fronteras físicas, ni soberanía e independencia, esto no inválida la importancia que posee en los conflictos que se generan. La Zona Gris en la que actúa es ideal hoy en día por el desarrollo de redes sociales y diversas formas de establecer comunicación.

La Cooperación Internacional, ha logrado fortalecer su presencia ya no sólo como un financiador de proyectos para el desarrollo, sino como la herramienta con la que cuentan los Estados para mitigar el mal uso que algunos Estados hacen de las TIC, lo que está impulsando al trabajo en equipo entre diversos Estados.

La labor descriptiva en el presente trabajo ha brindado elementos que deben ser profundizados, el análisis geopolítico que tuvieron los ciberataques en diversos conflictos son aproximaciones a los problemas estudiados, que se pretende sirvan de base para nuevas investigaciones.

Se ha cumplido con el objetivo general planteado y los objetivos específicos para los fines del presente trabajo. Invitando a que se siga avanzando en el tema.

1.1 LÍNEAS DE INVESTIGACIÓN SUGERIDAS

Se sugiere se continúe y profundice investigaciones en:

a) El rol del Derecho Internacional y Derecho Internacional Humanitario extendido al ciberespacio, ciberataque y ciberguerras.
b) Regulaciones y sanciones dentro de la debida ciberdiligencia de los Estados en caso de generación de ciberataques en sus territorios.
c) Limitaciones, regulaciones y sanciones en contra de cibertrolls y creadores de ciberbots que actúen en escenarios de Zonas Grises con fines de desinformación y afectación a los sistemas democráticos de los países.

2. *BIBLIOGRAFÍA*

Abello, R., Arevalo, W., Olasolo, H., & Antonio, V. (2020). *DIÁLOGOS Y CASOS IBEROAMERICANOS SOBRE DERECHO INTERNACIONAL PENAL, DERECHO INTERNACIONAL HUMANITARIO Y JUSTICIA TRANSICIONAL*. Recuperado el 2023, de books.google: https://books.google.es/books?hl=es&lr=&id=RPECEAAAQBAJ&oi=fnd&pg=PT10&dq=DI%C3%81LOGOS+Y+CASOS+IBEROAMERICANOS+SOBRE+DERECHO+INTERNACIONAL+PENAL,+DERECHO+INTERNACIONAL+HUMANITARIO+Y+JUSTICIA+TRANSICIONAL&ots=pJt6AqkLDn&sig=VFY3b6CCq6fHWRzHI3hSXqPUmXQ#v=o

Adeva, A., & Jose, V. (2023). Ciberseguridad, seguridad de la informacion y privacidad. *SIC*.

Amaro, J. A., Rodriguez, C., Macias, M. d., & Andrade, M. D. (2018). *CIBERATAQUES A UN PASO DE LA CIBERGUERRA*. Recuperado el 2023, de Ecos Sociales: CIBERATAQUES A UN PASO DE LA CIBERGUERRA

Benedicto, M. (23 de Abril de 2013). *EEUU ANTE EL RETO DE LOS CIBERATAQUES*. Recuperado el 2023, de Dialnet: https://dialnet.unirioja.es/servlet/articulo?codigo=7482959

Calduch, R. (1991). *LAS ORGANIZACIONES INTERNACIONALES GUBERNAMENTALES*. Recuperado el 2023, de ucm.es: https://www.ucm.es/data/cont/media/www/pag-55159/lib1cap9.pdf

Cocchini, A. (Enero de 2021). *LOS CIBERATAQUES DE LOS ACTORES NO ESTATALES Y LA "CIBERDILIGENCIA DEBIDA" DE LOS ESTADOS.* Recuperado el 2023, de EBSCO: https://web.p.ebscohost.com

Cocchini, A. (2 de marzo de 2021). *Real instituto ELCANO.* Recuperado el 2023, de Ciberdiligencia debida: ¿una actualización necesaria: https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari27-2021-cocchini-ciberdiligencia-debida-actualizacion-necesaria-para-derecho-internacional-del-ciberespacio.pdf

Connable, B. e. (2023). *RAND Corporation.* Recuperado el 2023, de Russia´s Hostile Measures. Combating Russian Gray Zone Agression Against NATO in the Contact, Blunt, and Surge Layers of Competition: https://www.rand.org/topics/cyber-warfare.html

Consejo de Europa. (23 de noviembre de 2001). *Convenio sobre la ciberdelincuencia* . Recuperado el 2023, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Consejo de Europa. (4 de junio de 2021). *Adhesión al Convenio de Budapest sobre la Ciberdelincuencia: beneficios, El convenio de Budapest sobre la Ciberdelincuencia.* Recuperado el 2023, de Consejo de Europa: https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

Dominguez, J. (2014). *La ciberseguridad: Aspectos Juridicos Internacionales.* Recuperado el 2023, de Dialnet: https://dialnet.unirioja.es/servlet/articulo?codigo=5217932

Ferrando, A. (diciembre de 2018). *La ciberseguridad como reto internacional: la protección frente a las ciberamenazas.* Recuperado el 2023, de Universitad Oberta de Catalunya (UOC): https://openaccess.uoc.edu/handle/10609/88685

Gaitán, A. (2012). *La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las tic en la guerra regular*. Recuperado el 2023, de Escuela Superior de Guerra (Revista: estudios en seguridad y defensa): https://esdegrevistas.edu.co/index.php/resd/article/view/194

Gavrila, A. (10 de Noviembre de 2022). *La gran ciberguerra de Ucrania que no ocurrió.* Recuperado el 2023, de Instituto Español de Estudios Estrategicos: https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO99_2022_ADAGAV_Ucrania.pdf

INTERPOL. (s.f.). *Los terroristas utilizan las redes sociales para radicalizarse, reclutar, financiar, planificar y ejecutar actividades terroristas.* Obtenido de Analizando redes sociales (Interpol): https://www.interpol.int/Crimes/Terrorism/Analysing-social-media

Jara, P. (JUNIO de 2020). LAS RELACIONES BILATERALES RUSIA-ESTONIA Y SU ESCALADA EN EL CASO DE LOS CIBERATAQUES DEL 2007. Madrid, España.

Kolesnikov, N. (2023). *Más de 50 Estadísticas de Ciberseguridad para el 2023 que debes Conocer: Dónde, Quiénes y Qué se Encuentra en el punto de Mira*. Recuperado el Noviembre de 2023, de Techopedia: https://www.techopedia.com/es/estadisticas-ciberseguridad

Lara, C. (15 de septiembre de 2023). *Internet y Derechos HUmanos*. Recuperado el 2023, de Derechos Digitales : https://www.derechosdigitales.org/22329/diplomacia-y-peligro-negociando-la-paz-en-el-ciberespacio/

Lazar, E., & Dragos, C. (2018). *LOS CIBERATAQUES: UNA NOCIÓN SIN TIPIFICACIÓN, PERO CON UN FUTURO*. Recuperado el 2023, de Repositorio Universidad de Coruña (vuc): https://ruc.udc.es/dspace/handle/2183/22352

Linares, N. (2019). *LOS CIBERATAQUES EN EL DERECHO INTERNACIONAL PUBLICO*. Recuperado el 2023, de e-repositori upf: https://repositori.upf.edu/handle/10230/42136

Madrigal, R. (Enero de 2020). *IMPACTO DE LOS CIBERATAQUE EN LA SEGURIDAD INTERNACIONAL IMPACT OF THE CIBERATAQUE ON INTERNATIONAL SECURITY*. Recuperado el 2023, de Dialnet (Revista Caribeña de Ciencias Sociales): https://dialnet.unirioja.es/servlet/articulo?codigo=9061864

Marin, A. (2023). *Los Sistemas de Armas Autónomos Letales y el Derecho Internacional Humanitario en la Guerra de Ucrania*. Recuperado el 2023, de EBSCO: https://web.s.ebscohost.com

Martinez, C. (Junio de 2015). *El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia*. Recuperado el 2023, de Repositorio comillas (Universidad Pontificia): https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/1222/TFG000913.pdf?sequence=1

Martins, B. (mayo de 2022). *Convenio de Budapest sobre la ciberdelincuencia en America latina*. Recuperado el 2023, de Derechos Digitales: https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

Organizacion de las Naciones Unidas . (diciembre de 2015). *Carta de fecha 15 de diciembre de 2015 dirigida a la Presidenta*. Obtenido de Consejo de seguridad (Naciones Unidas8.

Organizacion de las Naciones Unidas (ONU). (13 de febrero de 2017). *Resolucion 2341*. Recuperado el 2023, de Consejo de seguridad (Naciones Unidas): https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/038/62/PDF/N1703862.pdf?OpenElement

Organizacion de las Naciones Unidas (ONU). (2 de Agosto de 2017). *Resolucion 2370*. Recuperado el 2023, de Consejo de Seguridad (naciones unidas): https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/241/74/PDF/N1724174.pdf?OpenElement

Organizacion de las Naciones Unidas (ONU). (24 de Junio de 2020). *Dos Reglamentos de Naciones Unidas sobre Ciberseguridad y Actualizaciones de Software preparan el terreno para la introducción masiva de vehículos conectados*. Recuperado el 2023, de Comunicados de prensa (naciones unidas): https://unece.org/es/press/dos-reglamentos-de-naciones-unidas-sobre-ciberseguridad-y-actualizaciones-de-software

Organizacion de las Naciones Unidas (ONU). (29 de junio de 2021). *Permanezcamos alerta ante las tecnologías que pueden poner en peligro las generaciones futuras*. Recuperado el 2023, de Noticias ONU (naciones unidas): https://news.un.org/es/story/2021/06/1493862

Organizacion de las Naciones Unidas (ONU). (s.f.). *Carta de las Naciones Unidas*. Obtenido de Naciones Unidas : https://www.un.org/es/about-us/un-charter/full-text

Organizacion de las Naciones Unidas (ONU). (s.f.). *Ciberseguridad*. Recuperado el 2023, de Naciones Unidas.

Organizacion de Naciones Unidas (ONU). (16 de diciembre de 1966). *Pacto Internacional de Derechos Civiles y Políticos*. Recuperado el 2023, de Naciones Unidas: hchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights#:~:text=Artículo%2019,-1.&text=Toda%20persona%20tiene%20derecho%20a,otro%20procedimiento%20de%20su%20elección

Organizacion General de Naciones Unidas (ONU). (2 de JULIO de 2018). *Examen de la Estrategia global de las naciones unidas contra el terrorismo.* Recuperado el 2023, de Asamblea General (Naciones Unidas): https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/198/84/PDF/N1819884.pdf?OpenElement

Paredes, I. (2018). *"ATAQUES EN EL CIBERESPACIO BAJO EL DERECHO HUMANITARIO Y POLITICAS DE CIBERSEGURIDAD COMO FORMA DE DEFENSA"*. Obtenido de Bibliotecadigital de la Universidad de Alcala: https://ebuah.uah.es/dspace/handle/10017/38888

Paredes, I. (2018). *"ATAQUES EN EL CIBERESPACIO BAJO EL DERECHO HUMANITARIO Y POLITICAS DE CIBERSEGURIDAD COMO FORMA DE DEFENSA"*. Recuperado el 2023, de Biblioteca digital Universidad de Alcala: https://ebuah.uah.es/dspace/handle/10017/38888

Robles, M. (10 de Noviembre de 2020). *Sanciones contra ciberataques: la acción de la Unión Europea.* Recuperado el 2023, de Dialnet: Sanciones contra ciberataques: la acción de la Unión Europea

Ruiz, L. (2016). *Una nueva Taxonomía para los Ciberataques* . Recuperado el 2023, de SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2829313

Velazquez, A. (Abril de 2017). *LA RESPONSABILIDAD INTERNACIONAL DEL ESTADO COMO CONSECUENCIA DE LOS CIBERATAQUES UTILIZADOS COMO METODO DE COMBATE A A LUZ DEL DERECHO INTERNACIONAL HUMANITARIO.* Obtenido de Repositorio Comillas (Universidad Pontificia): https://repositorio.comillas.edu/xmlui/handle/11531/23550

Wajsman, G. (2022). *Ciberguerra entre Israel e Irán: desde Stuxnet hasta los ciberataques actuales.* Recuperado el 2023, de SEDICI: http://sedici.unlp.edu.ar/handle/10915/146056