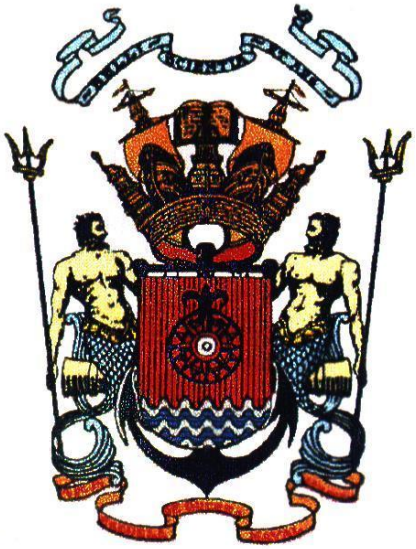
UNIVERSIDAD DE LA DEFENSA NACIONAL

FACULTAD DE LA ARMADA

UNIDAD ACADÉMICA ESCUELA DE GUERRA NAVAL

MAESTRÍA EN ESTUDIOS ESTRATÉGICOS

TESIS



TEMA:

Guerra Cibernética

TÍTULO:

"La influencia de la Guerra Cibernética en las relaciones entre estados Post Guerra Fría"

AUTOR: Capitán de Fragata Daniel Eduardo GIUDICI

DIRECTOR DE TESIS: Capitán de Navío Félix Eugenio PLAZA

-2021-

RESUMEN.

La presente Tesis, busca determinar la influencia actual de la Guerra Cibernética en las Relaciones Internacionales, en especial en períodos de crisis o conflictos entre estados.

La expansión tecnológica y el creciente uso de la informática y medios controlados a través de sistemas computarizados, no solamente han constituido el objeto de mejoras en la calidad de vida de la sociedad, también han materializado el advenimiento y expansión en el uso del ciberespacio como conductor de operaciones destinadas a la delincuencia, espionaje, desequilibrar sistemas financieros y como acción culminante, la Ciberguerra.

Actualmente la Guerra Cibernética tiene un alcance solamente limitado por la capacidad de defensa de los actores de la Comunidad Internacional. Su evolución durante la última década como así también su vinculación a las operaciones tradicionalmente llevadas a cabo en mar, aire y tierra, han hecho de ella una influencia destacable en los enfrentamientos entre actores estatales y no estatales por algún interés definido.

Así como evolucionó la doctrina militar, también tuvieron que hacerlo las Relaciones Internacionales. Ya no puede tomarse exclusivamente como espacios necesarios de controlar y para resolución de conflictos, el mar, el aire, la tierra y el espacio; una nueva dimensión de la mano del crecimiento y uso de la tecnología se ha hecho presente, el Ciberespacio.

Al desarrollar el presente trabajo de investigación y hacia el final, se establecen conclusiones que se encuentran con conceptos de la tesis y coadyuvan a comprender como la Guerra Cibernética y el Ciberespacio no reconocen límites geográficos y brindan capacidades para afectar los núcleos o instrumentos estratégicos, que si bien en muchas ocasiones son intangibles, su efecto decanta directamente en la perturbación del funcionamiento normal de los Estados y sobre su Poder Nacional.

TABLA DE CONTENIDOS.

BIBLIOGRAFÍA

INTRODUCCIÓN.

Durante los últimos años la Guerra Cibernética o Ciberguerra se ha transformado en un desafío para aquellos que custodian la soberanía y los intereses nacionales de los Estados.

Si bien durante el año 1988, se considera se produjo el primer ataque cibernético a la "autopista de la información" afectando la internet con un virus tipo "gusano", este fue sólo el comienzo de una nueva amenaza.

Durante el mes de enero de 2010 mientras inspectores de la Agencia Internacional de Energía Atómica se encontraban visitando instalaciones de una planta nuclear en Natanz - Irán, observaron que las centrifugadoras empleadas para el enriquecimiento de uranio habían comenzado a presentar fallas en su operatoria; luego de una investigación detallada los expertos pudieron determinar que la causa de estos hechos era un malicioso virus informático.

Este virus conocido como Stuxnet fue el encargado de tomar el control de 1.000 máquinas que participaban en la producción de materiales nucleares y a través de su codificación dio instrucciones de autodestruirse; un ataque cibernético logró dañar parte de la infraestructura estratégica y vital de un estado independiente.

Pero no fue solamente lo ocurrido, además la situación hizo que el presidente Ahmadinejad, culpara a Israel y Estados Unidos de ser los creadores de Stuxnet y perpetradores del ataque, al mismo tiempo que por otra parte su acción disuadió a Israel de un ataque aéreo sobre Irán y retrasó el programa nuclear iraní, obteniendo tiempo para que la política y diplomacia hicieran su trabajo.

Aquí tenemos un claro ejemplo de cómo en un conflicto multidimensional un actor utiliza los medios técnicos de ciberguerra en su maniobra estratégica, buscando resolver el

conflicto a su favor, evitando que otros actores usaran medios más violentos y ganando tiempo político en todo el escenario.

En otro hecho sin antecedentes en los últimos años, durante el 2013 países europeos negaron la autorización para que una aeronave oficial de un Primer Mandatario, sobrevolara sus espacios aéreos; el mandatario boliviano Evo Morales fue retenido y tuvo que realizar una escala en Viena – Austria, dado que Francia, España y Portugal no le permitieron el pasaje libre por sus cielos, sosteniendo que en ese avión se encontraba refugiado y era trasladado un hacker, Edward Snowden.

Esta circunstancia, supuestamente influenciada por el gobierno de los Estados Unidos, fue el inicio de una crisis diplomática donde lógicamente, se generaron descargos por parte de los países integrantes de UNASUR repudiando lo acontecido.

Puede verse claramente como un escenario político – diplomático se ve alterado por hechos vinculados con el manejo de la información y la desarticulación de infraestructuras estratégicas, trayendo consigo escenarios de crisis que afectan y dificultan poder mantener el status quo en las Relaciones Internacionales.

Si se considera que un ataque cibernético no reconoce límites y que sus perpetradores de manera anónima están en capacidad de afectar núcleos o instrumentos estratégicos para el funcionamiento de un Estado, resulta pertinente el interés por el estudio, sobre todo porque permite abordar una problemática para la cual se debe estar preparados y con capacidad de enfrentar los desafíos impuestos por esta nueva dimensión.

La creciente importancia de los sistemas de información en los ambientes de crisis y conflictos actuales, revelan que la seguridad de las redes informáticas es crítica para la obtención de la victoria y el desarrollo de las actividades antes, durante y posterior a la crisis / conflicto.

Al abordar los diferentes ambientes de guerra, el de la ciberguerra se ha convertido en los últimos años en algo emergente que evoluciona constantemente y se hace más fuerte y precisa en su accionar.

Actores estatales y no estatales, con fuerte presencia en el desarrollo tecnológico como Estados Unidos, Japón o China entre otros, o también aquellos con pobres estructuras de su Poder Nacional, pueden valerse de medios informáticos para atacar, corromper, infectar o desequilibrar plataformas e infraestructuras informatizadas del entorno mundial, regional o zonal, actuando de manera remota y anónima[1].

Con el apoyo de un estudio realizado por el Instituto Ponemon se demostró la generalización de los ataques cibernéticos, así como la vulnerabilidad de una organización al riesgo de ser abordado por un ciberataque[2].

Es importante entonces detenerse en estos aspectos y optar por estar preparados a ser receptores de eventuales ataques cibernéticos que intenten desequilibrar las estructuras convencionales del Estado, sea en tiempo de paz o de guerra.

La creación de virus informáticos es sólo un ejemplo de cómo los estados, organizaciones o simplemente personas, pueden servirse de esto para "espiar" a otros.

Así, se podría llegar al extremo que un país deje paralizada a una nación enemiga sin necesidad de una invasión militar y con sólo controlar su infraestructura electrónica como las redes de comunicación, usinas eléctricas y bancos[3].

1 Ponemon Institute LLC. (2010). First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies. Traverse City, Michigan: Ponemon Institute LLC. Baskerville, R. L., & Portougal, V. 2003. Pág. 20

2 Ponemon Institute LLC. "2011 Cost of Data Breach Study: United States". Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC. Traverse City, Michigan, USA. 2012. Pág. 27

3 Tritz, Gerald L. "Cyberspace and the Operational Commander". Naval War College. New Port. USA. 2010. Pag. 12.

Estas acciones, entendidas como objetivos de nivel estratégico están directamente ligadas e influyen con el desarrollo de las actividades y operatoria de un estado.

Durante el 2010 y a partir que Estados Unidos inauguró su Cibercomando lanzando la "Iniciativa Integral de Seguridad Cibernética Nacional"[4], donde la infraestructura digital de los Estados Unidos debía ser considerada un activo nacional estratégico, de un modo general se comenzó a conducir un amplio espectro de operaciones para defender las redes militares estadounidenses, así como dirigir y realizar los ataques que fueran necesarios contra otros países.

La misión principal de este comando sería la de planear, coordinar, integrar, sincronizar y conducir actividades con el fin de dirigir operaciones y dar defensa a las redes de información que el Departamento de Defensa designara como vitales o de importancia dentro del Poder Nacional[5].

Esta iniciativa generó tanto en tecnología como en doctrina un efecto reflejo en países como Gran Bretaña, Corea del Sur, Corea del Norte y China, entre otros. Estos, bajo diferentes acepciones crearon comandos que entienden en temas de guerra cibernética y buscan básicamente cumplir con los lineamientos que persigue Estados Unidos[6].

La Ciberguerra, su realidad actual y concreta aplicación durante las últimas crisis entre Estados, es lo que ha impulsado a estos países ha adoptar formas y procedimientos bien específicos y definidos, buscando que la misma se constituya como un arma estratégica, sin importar si es con fines defensivos u ofensivos,

4 The Comprehensive National Cybersecurity Initiative. The Executive Office of the President of United State. http://www.fas.org/irp/eprint/cnci.pdf 22 junio de 2012.

5 Rozoff, Rick. "El Pentágono se asocia con la OTAN para crear un sistema de guerra ciberspacial global". Disponible en http://rebelion.org/noticia.php?id=114884 .15 de octubre de 2010

6 Ramírez, Gustavo. "Prepara EU ofensiva cibernética con 4 mil nuevos miembros en su Cibercomando". CiberPoliticos.com. Disponible en http://ciberpoliticos.com/?q=EUofensivacibernetica4milCibercomando. Fecha de captura 28 de enero de 2013.

buscando escrutar su gran potencial para agenciar los objetivos que caracterizan a los conflictos modernos.

Se puede decir entonces que, la seguridad informática ha pasado a ser un área sensible para la defensa de un Estado, aumentando con el paso del tiempo la probabilidad que agentes foráneos lleven a cabo actos de elevado nivel de hostilidad utilizando como alternativas, complejos y maliciosos programas que por su nivel de destrucción virtual reciben el nombre de Armas Cibernéticas[7].

Con el advenimiento tecnológico y los avances en materia de información, los movimientos dentro del espectro cibernético y su llegada a los diferentes centros de gestión del Estado, hacen necesario cambiar el punto de vista y el paradigma sobre las políticas de seguridad y el concepto territorial sobre el que se custodia la soberanía.

En el Siglo XXI, los estados no pueden defender sus fronteras con medios militares o implementarlos como instrumentos de disuasión de forma exclusiva. Un ataque cibernético puede ocasionar el colapso de infraestructuras a gran escala, economía, servicios, redes, todas fundamentales para el funcionamiento de una nación y que la influencia de este nuevo ambiente de guerra busca, encuentra, selecciona y acciona sobre vulnerabilidades de los estados no preparados para prevenir debidamente sus intereses en este nuevo ambiente de conflicto[8].

Es así que varios autores, han realizado un ejercicio de prospectiva estableciendo un campo de operaciones futuro[9] y las amenazas potenciales que se presentarán para diferentes niveles de seguridad de un estado, analizando cómo proteger los centros

7 Cyberspace & Information Operations Study Center. Disponible en http://www.au.af.mil/info-ops/cyberspace.htm#cyber. Fecha de captura, 01 de mayo de 2013.

8 Cohen, Fred. "Influence Operations". U.S.A. 2011. Pag. 10. Disponible en: http://all.net/journal/deception/CyberWar-InfluenceOperations.pdf.

9 Air War College. Battlefield of the future. 21st Century Warfare Issues. Studies in National Security Nro.3 Air University. Maxell Aire Force Base. 1998.

de gravedad del impacto y desarticulación que generan las operaciones de Guerra Cibernética[10].

Todo lo relacionado a la red informática ha pasado a ser gracias a su velocidad de diseminación y transferencia de información y datos, un objeto en su conjunto, transnacional y que en función de cómo se administre y controle afecta la estabilidad de los estados y por consiguiente podría influir en la forma en que se devienen las Relaciones Internacionales.

10 Lukasik, S., Goodman, S. & Longhurst, D. Protecting Critical Infraestructures Against Cyber-Attack. Oxford University Press for The International Institute for Strategic Studies. London, UK. 2003.

CAPITULO 1

1.1 Ciberguerra y las Relaciones Internacionales.

El centro de gravedad de la presente Tesis es el Ciberespacio, la Guerra Cibernética y como ha influido con su aparición en las relaciones entre los estados.

Este es un escenario y flagelo relativamente moderno el cual ha aparecido vinculada al proceso de globalización. Por ello el trabajo de investigación a los fines de acotar la misma se centrará en algunas de las crisis y conflictos posteriores al fin de la Guerra Fría y donde se pudo determinar un efecto en su aplicación.

El impacto que impone a la seguridad global y regional, su accionar transnacional y la existencia de agentes estatales tanto como no estatales que encuentran como atractivo contar con esta capacidad, debe ser un área de interés y tema de agenda para la política de seguridad y defensa de un estado.

1.2 Descripción general de la Investigación.

Con esta investigación se pretende establecer las características de la Ciberguerra y tipo de operaciones que considera esta amenaza.

Es así como se puede observar en el desarrollo de los distintos capítulos, como se van abordando los objetivos específicos poniéndose especial énfasis en los últimos, donde el centro del desarrollo será la naturaleza de la guerra cibernética, medio que la identifica y tipo de operaciones probables de ser ejecutadas durante las diferentes etapas de una crisis o conflicto.

Esto último hace necesario para una mejor comprensión de la temática, el estudio y análisis de aquellas situaciones de crisis o conflicto, donde la guerra cibernética mantuvo un rol transversal y preponderante.

A los fines del estudio se centrará la atención en actores estatales Estados Unidos, Rusia e Irán. Si bien son varios los estados de la comunidad internacional que se suman constantemente a la lista de afectados o generadores de ataques cibernéticos, estos casos serán suficientes desde el punto de vista del autor para poder determinar una línea conceptual del objetivo principal de la investigación.

Teniendo en cuenta esta muestra es que se examina las consecuencias e implicancias impuestas por las operaciones de ciberguerra, obteniendo conclusiones que sustentan la hipótesis sobre la influencia de la Guerra Cibernética en las relaciones entre estados Post Guerra Fría.

1.3 Planteamiento del Problema.

En función de la perspectiva y visión del investigador, con la investigación se busca describir cual ha sido el resultado de las acciones de Guerra Cibernética llevadas a cabo durante los conflictos modernos, dando respuesta al interrogante: ¿Cómo se vieron afectadas las relaciones entre los estados con la aparición de la Guerra Cibernética y el nuevo escenario: Ciberespacio durante las crisis y conflictos modernos.

El análisis del presente trabajo, a partir de la perspectiva sobre aquellos conflictos tanto estatales como para estatales desarrollados post Guerra Fría permitirá determinar, tanto los efectos inmediatos como las consecuencias en las Relaciones Internacionales.

1.4 Fundamentación del Tema.

Al abordar los diferentes espectros o ambientes de guerra, la cibernética se ha convertido en los últimos años en un desafío emergente, que evoluciona constantemente haciéndose cada vez más fuerte y precisa en su accionar.

Desde la óptica del tesista, esta temática tiene como alcance el estudio, descripción y análisis, sobre el efecto de las

operaciones de guerra cibernética en los conflictos modernos y sus consecuencias en las Relaciones Internacionales.

Actores estatales y no estatales, con fuerte presencia en el desarrollo tecnológico como Estados Unidos, Japón o China, entre otros, o con pobres estructuras del poder nacional, pueden valerse de medios informáticos para atacar, corromper, infectar o desequilibrar plataformas e infraestructuras computarizadas del entorno mundial, regional o zonal, actuando de manera remota y anónima[11].

Con la aparición de internet se pudo advertir un constante avance tecnológico y una exponencial mejora en la comunicación entre seres humanos que ha alcanzado un nivel transnacional.

A primera vista sólo se percibió sus beneficios, pero como toda nueva tecnología, la internet presentó en 1988 su primera problemática, era vulnerable a manipulaciones no deseadas que no buscaban otra cosa que alterar y corromper el sistema.

Durante este año la internet fue afectada por un virus del tipo "gusano" dando lugar al al que se considera el primer ataque y la creación del primer equipo de reacción rápida para enfrentar este tipo de contingencias y amenazas cibernéticas.

Explícito en sus declaraciones al respecto ha sido el Secretario de Naciones Unidas Ban Ki-moon al decir que: "Internet es un excelente ejemplo de como los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional"[12].

A partir de ese momento, se comenzaron a observar durante diferentes operaciones militares inicialmente, como eran

11 Ponemon Institute LLC. (2010). First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies. Traverse City, Michigan: Ponemon Institute LLC. Baskerville, R. L., & Portougal, V. 2003.

12 Oficina de las Naciones Unidad contra la Droga y el Delito. "El uso de internet con fines terroristas".Nueva York 2013.Disponiblexen:https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

llevadas a cabo operaciones de ciberguerra con fines ofensivos; vale citar el caso de los ataques recibidos por fuerzas aliadas de la OTAN en Kosovo cuando hackers intentaron penetrar sistemas de información aliados, o también durante 1998 cuando estos obtuvieron acceso a las computadoras del Pentágono[13].

Con el apoyo de un estudio realizado por el Instituto Ponemon, se demuestra la generalización de los ataques cibernéticos, al punto de que en esencia está garantizado que cualquier organización eventualmente será el blanco de un ataque de este tipo[14].

Es importante entonces detenerse en estos aspectos y optar por estar preparados a ser receptores de eventuales ataques cibernéticos que intenten desequilibrar las estructuras convencionales del Estado, sea en tiempo de paz o de guerra.

Esta tesis busca exponer cuales serán los retos para la seguridad de un Estado, representados por la Ciberguerra y a su vez permitirá en un futuro llevar a cabo otras investigaciones que estén orientadas a determinar cuáles podrían llegar a ser considerados actos de ciberguerra, y desarrollar nuevas doctrinas de defensa y modos de acción para su aplicación.

Del mismo modo esta investigación, podrá ser tomada como punto de inicio de estudios, orientados al análisis del marco legal internacional y su competencia en asuntos relacionados con el Ciberespacio y su empleo.

1.5 El Problema.

Todo lo relativo al ciberespacio y su explotación se encuentra en constante evolución y desarrollo, sin dejar de lado la

13 Ponemon Institute LLC. "Possibility Theory Framework for Security Evaluation in National Infrastructure Protection. Journal of Database Management". Baskerville, R. L., & Portougal, V. A. Traverse City, Michigan, USA. 2003.

14 Ponemon Institute LLC. "2011 Cost of Data Breach Study: United States". Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC. Traverse City, Michigan, USA. 2012.

amplitud de problemas y situaciones imperantes relativas a ello. Uno de esos problemas esta ligado fuertemente al impacto de lo cibernético en las Relaciones Internacionales, como es el caso de los ciberdelitos y la ciberseguridad.

En la actualidad y a partir que resulta vital mantener las vinculaciones entre estados empleando el Ciberespacio, para la comunidad internacional es un objetivo vital sostener políticas que la posicionen a la vanguardia de los cambios en este nuevo escenario a fin de continuar la construcción de lazos en sus Relaciones Internacionales sin sobresaltos.

Actualmente la interconexión global de la que somos usuarios y a su vez esclavos, nos impone a la "RED" como camino crucial y vital para el desarrollo social y de las actividades de comunicación en general. Debido a esta interconexión global, toma trascendencia la ciberseguridad y con ella el escenario internacional respecto de sus relaciones.

Sucesos como los ocurridos en las plantas de enriquecimiento de uranio Iraníes durante el 2010 o filtraciones de información como fue en el caso de WikiLeaks durante el 2013, no son más que alguno de los ejemplos de infinidad de acciones de este tipo que se llevan a cabo y no solamente por actores estatales, sino que también ya comenzaron a surgir actores no estatales, casi mercenarios de este tipo de accionar.

De esta forma el abordaje de la investigación toma este problema y busca dar respuesta al interrogante y objetivo principal: ¿cuál es la influencia y los efectos generados por la Guerra Cibernética en las Relaciones Internacionales a partir del fin de la Guerra Fría?

1.6 Objetivos Específicos.

Objetivo 1: Describir las relaciones internacionales y su evolución a partir de la Segunda Guerra Mundial y hasta el fin de la Guerra Fría.

Los conflictos dentro de la comunidad internacional entre estados, han estado siempre presentes y sufrido una evolución, producto de los avances tecnológicos y cambios en las relaciones de poder e intereses entre los estados.

La descripción de los tipos de operaciones a partir de la Segunda Guerra Mundial y hasta el fin de la Guerra Fría, permiten comprender el cambio de paradigma a través de la visualización de la evolución del conflicto tradicional convencional, al instaurado en la actualidad.

Objetivo 2: Describir el Ciberespacio, la Ciberguerra y sus operaciones.

Tanto el Ciberespacio como la ciberguerra constituyen un escenario y ambiente de guerra relativamente nuevo y poco explorado. Sin embargo su amplio espectro de aplicación en la actual realidad internacional, lo transforma en un área de interés, que por el sólo hecho de los efectos probables de ocurrencia, hacen que sea necesario tener en cuenta su potencial de amenaza.

Con este objetivo se buscará definir el concepto de Ciberguerra, cuales son las operaciones que comprende e individualizar sus efectos y objetivos.

Objetivo 3: Describir las Relaciones Internacionales a partir de la globalización.

La RRII son cada vez más complejas, dado que actualmente nos encontramos con mayor cantidad de actores estatales y no estatales que influyen utilizando su poder, para obtener situaciones de equilibrio favorables a sus intereses; esas situaciones son temporarias y existe un equilibrio inestable con períodos más o menos prolongados de un status quo de pseudo tranquilidad.

Es por ello que, se encuentra necesario realizar una aproximación a la evolución de las Relaciones Internacionales sobre todo a partir de la globalización.

Objetivo 4: Describir situaciones de conflicto o crisis entre Estados a partir de 1989 donde la tecnología Cibernética fue empleada como instrumento de poder, centrando análisis en situaciones afrontadas o llevadas adelante por actores como podrían ser Estados Unidos, Rusia e Irán.

CAPITULO 2

2.1 Marco Teórico y Reglamentario.

A lo largo del presente capítulo, se establecerá el marco teórico de la investigación a partir de conceptos pertenecientes a los ámbitos de la Ciberguerra y las Relaciones Internacionales. Estos permitirán facilitar el cumplimiento de los objetivos planteados, respetando las limitaciones y alcances impuestos.

Para llevar adelante esta investigación se eligió de manera deliberada escapar a un marco teórico específico, que aglutine bajo su prisma de un único enfoque, los distintos episodios que se incluyen.

Es decir se podría haber seleccionado como marco teórico desde el punto de vista del conflicto a la visión de la Escuela de Guerra Naval, que sostiene el conflicto como inherente a las relaciones sociales y por lo tanto de permanente existencia en distintos niveles. Ello podría haber sido coherente con un marco teórico realista desde el punto de vista de las RRII.

Sin embargo la propia dinámica y diversidad de actores involucrados en el empleo del ciberespacio en acciones cooperativas, competitivas o simplemente perturbadoras o criminales, obliga a criterio del investigador a ampliar el abordaje.

El hecho de usar como ejemplos distintos episodios de múltiples actores sostiene la decisión, que en lugar de usar un marco teórico específico, interactuar con distintas visiones y fuentes, reglamentarias, normativas, pero también de opinión.

Es por eso que , al escapar a un marco estrecho, en esta sección el trabajo listará una serie de definiciones básicas que permitirá entender el proceso de investigación y en especial las opiniones surgidas de los casos investigados.

Como ejemplo de esta anterior aseveración comento que a continuación explicitaré definiciones de conflicto, guerra,

caos, crisis, etc. De haber seleccionado como marco teórico para el conflicto el usado en la cátedra de estrategia de esta maestría, estas definiciones hubieran sido innecesarias, pues cada una de estos términos son simplemente el conflicto que adopta distintos niveles en su escalada.

Más allá de esta explicación parece oportuno, sí mencionar algunas fuentes primarias y secundarias con las cuales se interactuará en el trabajo.

En el trabajo se emplearán publicaciones del entorno de la defensa, tanto a nivel nacional como internacional, como así también de carácter general, pero que constituyen una parte esencial para poder obtener información actualizada de este ambiente de guerra.

Como fuentes secundarias, no sólo se seleccionaron las doctrinarias del área militar, también se puede ver la referencia y aporte desde la perspectiva de relaciones internacionales y ciencias sociales. A través de estas últimas se puede fundamentar una actitud ofensiva y generadora de crisis y conflictos de un actor estatal o no estatal.

Habiendo efectuado esta definición conceptual es momento de explicitar las definiciones básicas a las cuales me refería.

Para poder llegar a ello, se emplean diferentes publicaciones del entorno de la defensa, tanto a nivel nacional como internacional, como así también de carácter general, pero que constituyen una parte esencial para poder obtener información actualizada de este ambiente de guerra.

Como fuentes secundarias, no sólo se seleccionaron las doctrinarias del área militar, también se puede ver la referencia y aporte desde la perspectiva de Relaciones Internacionales y Ciencias Sociales. A través de estas últimas se puede fundamentar una actitud ofensiva y generadora de crisis y conflictos de un actor estatal o no estatal.

Es necesario desarrollar los conceptos de Guerra, Crisis, Conflicto, Caos, Ciberguerra y Relaciones Internacionales. A tal efecto y teniendo en cuenta que son variados los autores que se pueden citar para estos conceptos, a los fines de limitar y poder permitir el avance de la investigación solamente se verán los más destacados:

- Ciberguerra

Ciberguerra o guerra informática o guerra digital es todo conflicto bélico que se realiza utilizando el ciberespacio y tecnologías de la información como campo de batalla o campo de operaciones.[15]

Puede ser entendida como una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para imponerle la aceptación de un objetivo propio, sustraer información, cortar o destruir sus sistemas de comunicación o alterar sus bases de datos, con la diferencia que el medio empleado no sería la violencia física sino un ataque informático a escenarios críticos que van desde:

- Fraude Electoral
- Espionaje Industrial.
- Ruptura del mercado de valores por beneficio o diversión.
- Espionaje industrial
- Provocar derrames intencionados de petróleo.
- Toma del control de la fabricación.
- Comprometer el Smartphone de un político.
- Chantaje masivo a través de las redes sociales.
- Ataque contra una central eléctrica.

15 LOS ESTADOS Y LA CIBERGUERRA Gema Sánchez Medero Profesora de Ciencias Políticas en la Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010

- Ataque contra una central hidroeléctrica[16].

En términos más generales[17]:

- Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo.
- Interrumpir o romper el flujo de la información.
- Destruir físicamente la información del adversario.
- Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información.
- Impedir al adversario acceder y utilizar los sistemas y servicios críticos.
- Engañar a los adversarios.
- Lograr acceder a los sistemas del enemigo y robarles información.
- Proteger sus sistemas y restaurar los sistemas atacados.
- Responder rápidamente a los ataques o invasiones del adversario.

Considerando el amplio espectro de objetivos e intereses que pueden surgir en una ciberguerra, es necesario advertir que existen tres clases de ciberguerra[18]:

- **Clase I:** Personal Information Warfare: área relacionada con las cuestiones y la seguridad personal, así como la

16 Instituto Espanol de Estudios Estrategicos. Ciberguerra: Los escenarios de Confrontacion. Eguskiñe Lejarza Illaro . 21 de febrero de 2014. http://www.ieee.es

17 LOS ESTADOS Y LA CIBERGUERRA Gema Sánchez Medero Profesora de Ciencias Políticas en la Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010

18 LOS ESTADOS Y LA CIBERGUERRA Gema Sánchez Medero Profesora de Ciencias Políticas en la Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010

privacidad de los datos y del acceso a las redes de información.

- **Clase II** Corporate/Organizacional Level Information: área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado) o al mismo nivel (de Estado a Estado).
- **Clase III** Open/Global Scope Information Warfare: área relacionada con las cuestiones de ciberterrorismo a todos los niveles, como pueden ser: los ataques realizados desde computadoras a centros tecnológicos; la propaganda como forma para enviar sus mensajes y para promover el daño ocasionado por sus ataques; y/o la planificación logística de atentados tradicionales, biológicos o tecnológicos.

- Ciberseguridad

Se define normalmente como la protección de datos, información y sistemas conectados a la red Internet. Este concepto extiende el de seguridad clásica conocido y tan empleado al de nociones propias del ciberespacio, como integridad, disponibilidad, autenticidad, confidencialidad o la mencionada denegación del servicio de la red de datos[19].

Tal es así, que en un primer momento la ciberseguridad obedecía a un enfoque de protección de la información (Information Security), donde solamente había que proteger la información de los accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones no permitidas. Actualmente este enfoque está evolucionando hacia la gestión de riesgos del ciberespacio (Information Assurance), donde la ciberseguridad consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos

19 Gema Sanchez Medero. La ciberguerra: los casos de Stuxnet y Anonymous.Disponible en:https://dialnet.unirioja.es/descarga/articulo/4331298.pdf 2012

usados basándose en los estándares internacionalmente aceptados[20].

- Ciberataque

Un ciberataque es considerado el conjunto de acciones ofensivas contra sistemas de información, perpetrados para dañar, alterar o destruir instituciones, personas, empresas[21]. El ciberataque puede dirigirse tanto a los equipos y sistemas que operan en la red anulando los servicios que prestan, como a los datos e información que se almacenan en bases de datos.

Al momento de clasificarlos y categorizarlos se puede decir que de acuerdo a su finalidad están separados en[22]:

- **Cibercrimen:** utilizando técnicas como el phishing, roban la identidad de personas o empresas para realizar fraudes financieros y todo aquello ligado generalmente con fines económicos.
- **Hacktivismo:** los hackers vulneran páginas de empresas o gobierno del estado. El objetivo de estos ciberataques es ideológico, social, y dentro de los hacktivistas, la organización Anonymous es la más conocida.
- **Ciberespionaje:** compromete la ciberseguridad en las empresas y el estado, ya que trata del robo de información sensible y valiosa, como información financiera, o desarrollo tecnológico como así también toda información sensible que pudiera llegar a usarse en contra de un actor estatal a fin de general un desequilibrio en el balance de intereses.

20 Real Instituto Elcano-Espana. Ciberseguridad en España: una propuesta para su gestiónEnrique Fojón Chamorro y Ángel F. Sanz Villalba www.realinstitutoelcano.org/2010

21 LOS ESTADOS Y LA CIBERGUERRA Gema Sánchez Medero Profesora de Ciencias Políticas en la Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010

22 https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos 2018.

- **Ciberterrorismo:** este es el caso de los ataques que suelen ir dirigidos contra gobiernos o estados, afectando servicios e infraestructura vital como el área de la salud o defensa.

- Relaciones Internacionales

Desde la Paz de Westfalia los pensadores han debatido acerca de la sinergia e interacción que se presenta de manera constante entre los estados del sistema internacional.

Sin embargo la complejidad propia de los tiempos, los intereses particulares y diferentes problemáticas que cada estado de manera aislada tiene, su diversidad de posturas y formas de abordarlas y buscarles solución han hecho que sea complejo el control de los conflictos internacionales y por supuesto imposible su erradicación.

Conflictos, que no son otra cosa que resultados de interacciones propias de las partes, que salen a la luz a partir que existen diferentes apetencias sobre un interés u objeto que no pueden dejarse de lado y en pos de lograr el éxito y darse con la victoria, se busca generalmente la neutralización, el daño o el control total o parcial sobre la otra parte.

En el escenario mundial de las Relaciones Internacionales, los análisis y razonamientos tienen distintos abordajes. Una línea de acción pone atención a las probables y posibles amenazas que pesan sobre los Estados y por transición sus sociedades e individuos; de esta manera atienden la problemática sobre la Seguridad Internacional y el equilibrio de las relaciones entre los estados.

De la misma manera también hay un análisis que toma en cuenta los aspectos puramente teóricos que en su conjunto coadyuva a llevar a cabo una descripción de los distintos sucesos, permitiendo que se puedan explicar, entender y hasta hacer un

pronostico al respecto de cómo puede evolucionar una situación planteada[23].

Desde el punto de vista teórico cada una de las conductas tomadas como parte de la interacción de los estados alberga en su seno múltiples enfoques y teorías que, aunque comparten un conjunto de postulados básicos, difieren en materia de matices específicos[24].

Siendo una de las quizás más conocidas y difundidas de las corrientes, el Realismo es la línea de pensamiento que marca el rumbo de la mayoría en cuestiones de las Relaciones Internacionales. Los estados de la comunidad internacional, al igual que los pensadores sostienen la mayor cantidad de coincidencias acerca de su denominación y características básicas, sin dejar de lado que cuenta con la tradición teórica más dilatada en el tiempo con antecedentes en el siglo V AC con Tucídides[25].

De manera dispar respecto al Realismo y sus preceptos, se puede encontrar el Liberalismo, el mismo que también ha tenido diferentes denominaciones entre ellas Internacionalismo Liberal, Pluralismo, Legalismo, Idealismo que no dejan de ser prácticamente lo mismo o al menos tener como base los mismos conceptos[26].

Ahora bien, a estas dos corrientes teóricas predominantes se suma, el Marxismo, doctrina y teoría social, filosófica, económica y política ideada por Karl Marx, que sostiene un enfoque sistemático del mundo; por el contrario a las anteriores,

23 PONS Luis. Claves del Siglo XXI. IUN-Dunken, Buenos Aires 2000, p.11

24 BARTOLOME, Mariano Cesar. Un abordaje general a la Teoría de las Relaciones Internacionales. http://repositorio.ub.edu.ar/bitstream/handle/123456789/3505/4104%20%20teoria%20de%20las%20relaciones%20internacionales%20-%20bartolome.pdf?sequence=1&isAllowed=y

25 DALLANEGRA PEDRAZA, Luis, Realismo-Sistémico-Estructural: La Política Exterior como "Construcción" de Poder, (Córdoba, Edición del Autor, 2009) ISBN: 978-987-05-6072-2

26 BARTOLOME, Mariano Cesar. Un abordaje general a la Teoría de las Relaciones Internacionales. http://repositorio.ub.edu.ar/bitstream/handle/123456789/3505/4104%20%20teoria%20de%20las%20relaciones%20internacionales%20-%20bartolome.pdf?sequence=1&isAllowed=y.

carece de una producción teórica y de pensamiento, como así también es relativamente mucho más joven dado que no se remontaría más de dos siglos atrás y donde se fundamentaba sobre un profundo análisis económico de la sociedad capitalista[27].

Dicho esto y por ser la investigación tomada a partir del fin de la Guerra Fría, el Realismo se impone como la corriente más importante aplicada de las teorías de las Relaciones Internacionales y que a su vez muta y Kenneth Waltz toma sus conceptos y adecua para denominarlo Neorealismo o Realismo Estructural[28].

Dicha corriente, heredera en muchos aspectos del realismo de Hans Morgenthau, introduce la noción de «estructura» como elemento determinante de las relaciones políticas entre sus miembros. El neorealismo ha sido, en efecto, el principal blanco de las críticas que han anunciado la muerte del realismo por no haber sido capaz de anticipar un acontecimiento tan trascendental como la desaparición del imperio soviético y la consiguiente transformación del sistema internacional[29].

Para el neorealismo, la anarquía continúa siendo el elemento definitorio del sistema internacional, sumado a ello las siguientes consideraciones: los Estados poseen capacidad militar ofensiva, en mayor o menor medida pero al fin la tienen y con ello la potencial capacidad de generar un desequilibrio; los Estados nunca pueden estar seguros de las intenciones de otros Estados; la supervivencia es la fuerza que mueve a los Estados ya que éstos desean conservar su soberanía; finalmente, la perspectiva estratégica desempeña un papel esencial en el

27 DALLANEGRA PEDRAZA, Luis, Realismo-Sistémico-Estructural: La Política Exterior como "Construcción" de Poder, (Córdoba, Edición del Autor, 2009) ISBN: 978-987-05-6072-2

28 Ignacio Pérez Caldentey. El Realismo y el final de la Guerra Fría. Disponible en: revistas.pucp.edu.pe/index.php/agendainternacional/article/viewFile/7164/7364

29 Idem.

intento de supervivencia de los Estados en el sistema internacional[30].

Todo esto da lugar de manera genérica a decir que: los Estados temen a otros Estados, cada Estado intenta garantizar su propia supervivencia y por último, los Estados intentan maximizar su posición de poder relativo sobre otros Estados[31].

A partir del estos conceptos la multiplicidad de unidades y el antagonismo existente entre las mismas Relaciones Internacionales, independientemente de las diferentes corrientes que puedan encontrarse en el esquema mundial, resulta innegable la naturaleza conflictiva de los estados, como así también su agresividad, entendible a partir de una característica propia de la naturaleza humana, constante, universal e innata: el deseo de poder[32].

- Guerra

Sun Tzu, general y estratega chino, vivió alrededor del siglo V antes de Cristo. La colección de ensayos sobre el arte de la guerra atribuida a Sun Tzu resulta ser el tratado más antiguo que se conoce sobre este tópico tan particular.

En su obra el "Arte de la Guerra", sostenía que la guerra es de vital importancia para un Estado, el dominio de la vida o de la muerte[33].

Carl von Clausewitz, militar y estratega, en su obra "De la Guerra" aborda el concepto de Guerra diciendo que consiste en un acto de violencia el cual demanda al adversario a rendirse a una voluntad superior. La guerra es más que un acto político, es un

30 Idem

31 Idem

32 DALLANEGRA PEDRAZA, Luis, Realismo-Sistémico-Estructural: La Política Exterior como "Construcción" de Poder, (Córdoba, Edición del Autor, 2009) ISBN: 978-987-05-6072-2

33 Sun Tzu. El arte de la Guerra. 2003. http://www.biblioteca.org.ar/libros/656228.pdf.

instrumento político que aparece en escena al momento que las relaciones diplomáticas e internacionales han fracasado[34].

Apoyado en estas dos perspectivas sobre la guerra, se puede definir la misma como el acto en donde se encuentran involucrados al menos dos actores estatales, en una trama originada por intereses contrapuestos y que a través de sus capacidades y competencias buscan imponerse con la victoria y por ende conseguir sus intereses, siendo los permanentes dar protección a su Estado y salvaguardar su soberanía, contrarrestando las amenazas externas.

- Caos

De acuerdo a la Real Academia Española Caos: es un estado amorfo o indefinido que se supone anterior a la ordenación del cosmos.

También toma como definición confusión y desorden, pero por qué no tomar una de sus acepciones, y a los fines de nuestro estudio, como la más acertada y científica: desorden aparentemente errático o impredecible de algunos sistemas dinámicos deterministas con gran sensibilidad a las condiciones iniciales.

Caos y desorden son en muchas ocasiones utilizados como sinónimos. No obstante cuando el escenario que le da marco a un conflicto particular es el de la comunidad internacional y sus relaciones, los disparadores caóticos suelen ser la anarquía, desobediencia civil y sobre todo y de las más habituales el colapso institucional, dado que las instituciones de un estado son los entes que regulan el equilibrio en todo su espectro.

- Crisis

Para el caso de la definición de Crisis el Diccionario de la Real Academia Española establece que es un cambio profundo y de consecuencias importantes en un proceso o situación o en la manera en la que estos son apreciados.

34 Karl von Clausewitz. De la Guerra. http://www.biblioteca.org.ar/libros/153741.pdf.

Conceptualmente, una crisis no es más que una situación crucial o decisiva en cualquier aspecto de una realidad organizada, que involucra un cambio abrupto o decisivo; particularmente preciso es este concepto cuando lo proyectamos a la crisis de una estructura social. Allí, los cambios críticos, aunque previsibles, siempre están ligados a algún grado de incertidumbre, en relación a su ejecución, a su reversibilidad o grado de profundidad, y a sus consecuencias. Si los cambios sociales son profundos, súbitos y violentos traen consigo consecuencias trascendentales que van más allá de la crisis y se pueden denominar cambios revolucionarios[35].

Así conceptualizada, la crisis se manifiesta como un evento estresante, emocional y hasta traumático, que cambia o modifica sustancialmente la vida de las personas, a propósito de cualquier conflicto que al no resolverse, llega a su más alto nivel de tensión y desencadena eventos que modifican el equilibrio social[36].

Algo importante y a tener en cuenta es que algunas crisis son pseudo-crisis; es decir, pueden ser inexistentes, ya que no se sustentan en hechos reales, pero son creadas por la conveniencia de ciertos intereses[37].

Toda crisis es una competencia de influencias desarrollada para alcanzar la mejor y más sólida posición política dentro de una trama particular, donde escenario y actores se debaten en relaciones de poder y fuerza a fin de disponer de la mejor posición para negociar en las condiciones más ventajosas posible.

Es con frecuencia en el mundo globalizado que vivimos, que una crisis tenga más o menos impacto en función se le de mayor

35 TEORÍA DEL CAOS SOCIAL Cap.: 7 Crisis, conflictos y Caos Social· Andrés Simón Moreno

36 Pensando en la crisis y sus efectos en la sociedad actual. Silvia Viviana Pugliese. 18 abril 2018. https://apop.es/en-la-crisis-y-los-efectos-en-la-sociedad/

37 Crisis, Conflicto y Caos Social. Por Andrés Moreno Arreche. 11 junio 2009. https://teodulolopezmelendez.wordpress.com/2009/06/11/crisis-conflictos-y-caos-social/

entidad o trascendencia a través de los medios de comunicación, y con ello mayores o menores consecuencias internas o exógenas para las organizaciones e instituciones involucradas.

Una crisis, a los fines de la investigación puede ser la consecuencia de un hecho a gran escala que genera eventos traumáticos que implican un cambio abrupto y desequilibrio, trasgrediendo las fronteras geográficas y provocando un conflicto dentro de las organizaciones e instituciones de la sociedad.

Las crisis normalmente comienzan a gestarse de manera inconsciente, encuentran su estado natural de manera potencial, vigente y siempre listo a surgir, nacen, crecen y se reproducen en el preconsciente colectivo; cuando una crisis pasa el umbral de la evidencia, entonces se manifiesta como conflicto[38].

- Conflicto

El diccionario de la Real Academia Española señala al conflicto como un combate, lucha o pelea, un enfrentamiento armado, una situación de difícil salida, un problema o materia de discusión o la coexistencia de tendencias contradictorias.

Para el caso en estudio se toma un sistema donde existe una interacción y presencia de un escenario internacional, los estados reconocidos y participantes del mismo y aquellos organismos internacionales que los agrupan con un fin común como es el caso de la Organización de las Naciones Unidas y como fue su participación en la Guerra de Corea en 1950.

De esta forma puede tenerse un conflicto en la comunidad internacional cuando entre dos actores del sistema surge un contraste de intereses que tiende a prolongarse en el tiempo. El mismo puede ser no violento, mientras se apele a procedimientos

38 TEORÍA DEL CAOS SOCIAL Cap.: 7 Crisis, conflictos y Caos Social. Andrés Simón Moreno http://www.oxigeme.com/wp-content/uploads/2014/10/Teoria_caos_social.pdf

diplomáticos, o violento si es aplicable la fuerza por medio del Instrumento Militar estatal[39].

Sobre sus causas, hay diversas teorías: los monistas sostienen la idea de la causa única, los marxistas dicen que es el conflicto de intereses económicos y el realismo político es el interés nacional definido en términos de poder. Los pluralistas sostienen la idea de múltiples causas simultáneas: socio-económicas, políticas e ideológicas.

Ahora bien, los conflictos no solamente se circunscriben al ámbito internacional, también pueden darse en el marco interno de un estado e internacionalizarse cuando, a pesar de no traspasar las fronteras de un Estado, amenace la paz y la seguridad internacionales. Tan importante es ello que la Carta de la Organización de las Naciones Unidas prohíbe a la organización intervenir en los asuntos internos de los Estados miembros, excepto cuando se vea afectada la paz y seguridad internacional[40].

Un conflicto interno esta dado cuando surge una controversia interna como podría ser la oposición de intereses entre sectores de la población y a través de la cual se amenaza la paz y el equilibrio social en todo o parte del territorio bajo la soberanía o autoridad de un Estado; puede estar o no acompañada de enfrentamiento armado.[41]

2.2 Metodología.

Para este trabajo de investigación, se ha realizado una investigación histórica, explorativa, descriptiva, volcando el mayor esfuerzo al estudio de bibliografía y el análisis de

39http://www.eumed.net/diccionario/definicion.php?dic=3&def=220 23 julio 2018

40 Augusto Hernandez Campos. Los Conflictos Internos: Naturaleza y Perspectivas https://dialnet.unirioja.es/descarga/articulo/6302462.pdf 1999

41 Augusto Hernandez Campos. Los Conflictos Internos: Naturaleza y Perspectivas https://dialnet.unirioja.es/descarga/articulo/6302462.pdf 1999

diversas fuentes de información como: artículos, trabajos de investigación e informes disponibles en Internet.

Es histórica puesto que se basa en hechos acontecidos y que sirven como base para desarrollo de la problemática planteada.

Exploratoria, especialmente por su abordaje a un tema relativamente contemporáneo, pero que aún se encuentra poco estudiado e inclusive resulta un desafío para muchos integrantes de la comunidad internacional. Es así como el análisis a través del desarrollo del presente trabajo, busca establecer conclusiones aproximadas en torno de la temática y no buscar profundizar el conocimiento actual que hay sobre el mismo.

Descriptiva, porque lleva a cabo un diagnóstico de la amenaza, estableciendo sus efectos en el escenario de la comunidad internacional y conflictos modernos, identificando además sucesos y situaciones específicas.

En virtud de lo expresado se llega a la determinación del objetivo de la investigación, que es establecer el contexto que caracteriza a la Ciberguerra; esto logrado por medio de la descripción de conflictos ocurridos posteriormente al fin de la Guerra Fría y donde se hallan ejecutado operaciones de Ciberguerra.

De acuerdo al propósito y objetivos que se han planteado, el diseño de este trabajo es fundamentalmente no experimental, sustentando el mismo en la recolección de datos circunscriptos a un momento determinado y casos seleccionados de manera arbitraria.

Para el estudio de los casos será preciso tomar los mismos a partir de una misma base de abstracción, es decir mismo nivel de actores y que en ellos se hayan podido comprobar la influencia y el impacto de la guerra cibernética como un elemento estratégico.

Asimismo y a los fines de poder circunscribir el trabajo en tiempo y extensión, se plantea como limitante de la propuesta, al nivel de información disponible relacionado con la Ciberguerra.

Esta información y documentación obrante en el sistema internacional, se encuentra vinculada directamente con el accionar estratégico y por ello sus características de divulgación y acceso son sensibles y por lo general clasificadas.

Así entonces para poder desarrollar la investigación, se utilizaron documentos, reglamentos e información en general cuyas características son no clasificadas y en su mayor parte provenientes de fuentes secundarias.

En pos de dirigir la investigación a aquellas crisis y/o conflictos, donde se hayan presentado acciones de Ciberguerra, si bien se pondrá especial atención en casos ocurridos entre estados, por su elevado poder de desestabilización no hay que dejar de lado la probabilidad de ocurrencia de un ataque generado a partir de una célula terrorista.

CAPÍTULO 3

3.1. La Guerra: Evolución.

Se puede decir que la guerra es tan antigua como la humanidad misma y no es otra cosa que un fenómeno social que se encuentra inmanente en la Comunidad Internacional, que conforme al desarrollo de las sociedades y la tecnología evoluciona de manera constante.

Su progreso si se hiciera una línea de tiempo incluye actos circunstanciales de violencia entre clanes y que con el correr del tiempo fueron agrupándose bajo el liderazgo de una persona; así comenzó el uso de la hostilidad para resolver las controversias y con lo cual conllevó el aumento de la escala, duración y tipo de conflictos.

Sun Tzu, al observar este tipo de comportamientos en la sociedad, observó la necesidad de concebir teorías acerca de la guerra y su forma de hacerla. Si bien sus enseñanzas y escritos son anteriores a la era cristiana, aún hoy se lo reconoce como pionero en estos temas y mantiene la vigencia; inclusive ha transgredido las fronteras de lo militar llegando a aplicarse sus conceptos en ámbitos empresariales.

Su definición de la guerra sostiene que es el dominio de la vida o de la muerte y que guarda directa relación con la supervivencia de un imperio[42]. Quizás una definición acotada para la época, pero que podremos observar a continuación no ha cambiado en absoluto su esencia.

Más contemporáneo y también estudiado de manera constante en ámbitos tanto militares como empresariales, y que ha desarrollado su teoría sobre este concepto es Karl von Clausewitz. Militar prusiano que gracias a su experiencia, decidió compaginar una obra donde concentró temas relativos al

42 Sun TZU. El Arte delaGuerra.2003.Disponibleen: http://www.biblioteca.org.ar/libros/656228.pdf

ambiente militar y definió la guerra como algo inclusive mas sencillo de entender: "acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad",[43] asociando de manera directa el conflicto armado al escenario político refiriéndose como que la guerra resulta ser un instrumento político, empleado para que la política pueda obtener sus intereses por otros medios, cuando se han agotado por ejemplo las instancias diplomáticas.

Ahora bien, tan interesante resulta el tema de la guerra, que no suficiente con la claridad conceptual aportada por estos autores, durante el siglo XX continuaron surgiendo pensadores desarrollando diversas teorías sobre el tema. Entre ellos puede citarse a Georges Sorel, filósofo francés que definió la guerra como un acto político por medio del cual los Estados que no pueden remediar una controversia respecto a sus obligaciones, derechos o intereses por otros medios, usan el recurso de la fuerza armada para decidir cuál es el más fuerte e imponer la voluntad de quien gane[44].

Asimismo y con énfasis en el pilar político que da sustento a la guerra, Horacio Kallen, dice: "si la guerra se puede definir como un concurso armado entre dos o más entidades soberanas que emplean las fuerzas militares organizadas en la consecución de los fines específicos, el término significativo en la definición es organizado", agregando a su vez que la organización de las fuerzas armadas se extiende más allá de sí mismas, y afecta las actividades civiles, como la industria, producción y comercio, así como los aspectos sociales[45].

Entonces, la guerra es vista como una actividad social cuya génesis si bien no se puede determinar con precisión surge a

43 Karl von Clausewitz. De la Guerra. 2002. Edición Libro Dot.com. Disponible en: http://lahaine.org/amauta/b2-img/Clausewitz%20Karl%20von%20-%20De%20la%20guerra.pdf

44 GEORGES SOREL, Reflexiones sobre la violencia, Alianza Editorial, Madrid, 2005.

45 La guerra y la Teoría del Conflicto Social. Real Academia de Ciencias Morales y Políticas. Madrid 1962. Disponible en: http://www.racmyp.es/R/racmyp/docs/discursos/D82.pdf

partir del desarrollo, organización y avances de la humanidad; se adapta a sus respectivos cambios y como resultado de las actividades o condiciones relacionadas con la procesión de la evolución sociocultural del hombre[46].

Se podría continuar aportando pensadores, sociólogos y expertos, que hasta la actualidad siguen promoviendo teorías y conceptos acerca de la guerra, no obstante y por no ser este concepto el tema de investigación se debe acotar la conceptualización a la simple idea colectiva. A juicio del autor la guerra es un proceso mediante el cual los estados participantes de la Comunidad Internacional, conforman sociogramas junto a sus instituciones, buscando que sus intereses prevalezcan y que, cuando se agotaron las vías políticas optan por resolver las discrepancias por medio del enfrentamiento armado y empleo de la fuerza buscando así imponer su poder para destrabar el conflicto de intereses.

Concentrando aún más los aspectos vertidos, se puede decir que para que se den las condiciones de guerra clásica, debe haber actores estatales organizados y como mínimo dos adversarios o más, donde su eje principal son las fuerzas armadas; también muy importante es la legitimidad que otorga la población civil (ejemplo por el absurdo la Guerra de Vietnam)[47], esta puede afectar la voluntad de vencer, no sólo a los que se encuentran en los frentes de batalla, sino a las instituciones públicas y privadas.

Durante el Siglo XX, conflictos bélicos armados convencionales de gran escala como fue la Primera y Segunda Guerra Mundial y más acotados en su expansión como ha sido Vietnam e Irak, hasta llegar a la actualidad donde el terrorismo y la droga se imponen como flagelos desequilibrantes de los estados, han mostrado la

46 LAURA MILENA ECHEVERRI MARTÍNEZ. LA RELACIÓN DE LA CIBERGUERRA CON LA GUERRA INTERESTATAL CLÁSICA: ESTUDIO DE CASO ESTONIA, GEORGIA E IRÁN. Universidad Militar Nueva Granada. Julio 2016. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/15363/EcheverriMart%EDnezLauraMilena2016.pdf;jsessionid=9D4478627C12ADFF5D90E20DC6B7CF65?sequence=1.

47 Helio JAGUARIBE. El Vietnam y los Estados Unidos. La Rendición de Saigon. Abril 2018.

capacidad de destrucción a través de cifras alarmantes de muertos, discapacitados y en algunos casos hasta la destrucción del patrimonio de la humanidad.

Sin embargo cabe señalar que este tipo de acciones también favorecieron el desarrollo tecnológico de vanguardia como fue el caso del radar o el submarino, armas químicas, la energía nuclear y tantos otros, imponiendo en cada avance un cambio evolutivo y la transformación de la guerra, su concepto y modo de llevarse a cabo.

En un escenario donde la evolución y el acceso a las armas con el que cuentan algunos países desarrollados y teniendo conciencia de su potencial destructivo, los actores estatales comenzaron a evitar caer en un enfrentamiento bélico armado y buscaron la resolución de las controversias en aquellos espacios asociados a los FOROS como el caso de la ONU (Organización de las Naciones Unidas), OEA (Organización de los Estados Americanos), UNASUR (Unión de las Naciones Sudamericanas), el MERCADO, como lo son los organismos internacionales económicos, Banco Mundial, Fondo Monetario Internacional, Organización para la Cooperación y el Desarrollo Económico, Banco Interamericano de Desarrollo, Banco Internacional de Reconstrucción y Fomento en vez de imponerse a través de aquellos que representan el TERRITORIO.

Ahora bien, a pesar del abordaje diplomático que pudiera presentarse ante la necesidad de resolver una controversia o conflicto de intereses y tratar de mantener el nivel de un conflicto a baja escala, la guerra siempre se hace presente y hoy en día se presenta como Guerra de Cuarta Generación.

La globalización junto al incremento de flujos transnacionales ligado a este proceso, han generado un cambio en los campos de los poderes políticos, económicos, sociales y militares. La transformación de los patrones de comportamiento y estructura de intereses de los actores pertenecientes al Sistema

Internacional, hacen que sean factores críticos en la conformación de escenarios de combate donde actualmente ya no solamente se ven enfrentados esos mismos actores estatales, si no que comenzaron a aparecer como nuevos integrantes desequilibrantes de la Comunidad Internacional actores no estatales[48].

Como se ha dicho anteriormente la guerra ha evolucionado y con ello su forma de hacerla. Las llamadas Guerras de Primera Generación, comenzaron a partir de la aparición de las armas de fuego y su máxima expresión y paradigma fueron las guerras napoleónicas, donde las formaciones lineales y el orden preciso en el campo de batalla eran el común denominador de los enfrentamientos entre masas de hombres.

A partir de la invención de la máquina de vapor y con el advenimiento de la Revolución Industrial, los conflictos evolucionaron y aparecieron en los campos de batalla medios capaces de desplazar grandes masas de personas y suministros como así también artillería pesada y demoledora dando lugar a las denominadas Guerras de Segunda Generación, materializadas en escena durante la Primera Guerra Mundial.

Para la Segunda Guerra Mundial, nuevamente las tácticas y el armamento habían evolucionado. Para ese entonces el ejército alemán, determinado a conquistar Europa, dio lugar a la denominada Guerra Relámpago[49], la cual basaba su poder en dos principios de la guerra Velocidad y Sorpresa, pero asimismo que sumaba operaciones de guerra psicológica y tácticas de infiltración y todo ello daba forma a lo que se vendría en llamarse Guerras de Tercera Generación.

Pero para este momento histórico, donde Alemania viera desarticulada sus intenciones, la Comunidad Internacional

48 Patricio MUNOZ. La influencia de los actores no estatales en el sistema internacional. Disponible en: https://afese.com/img/revistas/revista58/influencia.pdf

49 Robert CITINO.DE LA BLITZKRIEG A TORMENTA DEL DESIERTO. Ediciones PLATEA. 2004.

habiendo sido testigo de la destrucción y muerte que fuera sembrada al finalizar la Segunda Guerra Mundial, comenzó a observar la necesidad de controlar los impulsos que pudieran surgir por la confrontación de intereses de diferentes actores; al mismo tiempo que de escalar un conflicto, tener la capacidad para neutralizar al enemigo, detectando y atacando sus debilidades y anular con ello su capacidad operativa.

Es así que como primer paso aparece en el escenario internacional las Naciones Unidas. Su intención primaria, evitar futuras guerras mediante el uso de la diplomacia y del diálogo entre las naciones. Esta organización formada por estados soberanos unidos de manera voluntaria crearon un foro donde sus miembros podían brindar mecanismos necesarios para resolver problemas y controversias y tomar decisiones que fueran por el bien de la humanidad.

A partir del trabajo constante de la Organización hubo una reducción de las tensiones internacionales, la atención se puso en la prevención de conflictos y en la tarea de poner fin a los combates que estuvieran en desarrollo, transformándose en proveedores de medios para mantener la paz y seguridad internacional.

Si bien esto marco de alguna manera la prescripción de la guerra y desde ese entonces técnicamente nunca más se declaró la guerra entre estados de manera oficial, en el Derecho Internacional aparecieron los denominados Conflictos Armados, sean estos internacionales o no.

Pero en 1991 un profesor de la Universidad Hebrea de Jerusalén Martín Van Creveld en su libro "La Transformación de la Guerra", dispara las ideas iniciales sobre lo que hoy se entiende como Guerras de Cuarta Generación[50].

50 Javier JORDAN. El terrorismo y la transformación de la Guerra. 2004. Disponible en: https://dadun.unav.edu/bitstream/10171/22067/1/ADI_XX_2004_09.pdf

Este autor considera que la guerra ha evolucionado y que ya no se puede tomar al pie de la letra aquellos aportes hechos en su oportunidad por Clausewitz.

Desde aproximadamente 1989, los Estados Unidos de Norteamérica, han visto la necesidad de concebir la llamada Guerra de Cuarta Generación, que no solamente es coincidente con la Caída del Gran Muro, si no que también se la puede asociar con la revolución informática[51].

Van Cleveld sostiene que conforme el sociograma internacional avanza, perderán su razón de ser las bases militares y el control de la población se efectuará mediante una mezcla entre operaciones psicológicas de propaganda y terror. Las fuerzas convencionales conocidas históricamente y donde el principio de masa era uno de los rectores, mutarán hacia sistemas mas automatizados, donde se reducirá la exposición de la vida humana, clásica en el campo de batalla y habrá una conversión a conflictos de baja intensidad también llamados Guerras Asimétricas.

Este tipo de conflicto bélico minimiza el factor de fuerza armamentista, y busca operar más desde la esfera de lo psicológico, procurando obtener la desarticulación a través de la movilización de la voluntad de la población abarcando los aspectos políticos, económicos, sociales y culturales de un estado[52].

Estas nuevas condiciones para el escenario internacional han hecho que los estrategas comiencen a plantear la conducción de una guerra dejando de lado la combinación de tácticas y medios tradicionales y por el contrario orientar sus políticas de

51 FREYTAS, Manuel. Guerra de Cuarta Generación. Disponible en:https://www.bibliotecapleyades.net /sociopolitica/sociopol_globalmilitarism157.htm. Marzo 2009.

52 Reflexiones sobre la guerra de cuarta generación, una visión desde los actores sin recursos de poder en términos tradicionales.
Disponibleen: https://www.researchgate.net/publication/284574184_Reflexiones_sobre_la_guerra_de_cuarta_generacion_una_vision_desde_los_actores_sin_recursos_de_poder_en_terminos_tradicionales

desarrollo de conflictos hacia una visión conceptual de guerra sin límites o sin restricciones[53].

Este tipo de guerra busca recurrir a medios que se salen de las reglas, normas y rutinas aceptadas generalmente por el conjunto de actores de un enfrentamiento: el no respeto de las reglas de guerra tal como las define el Derecho Internacional o la utilización de medios de destrucción no militares, económicos y sociales, entre otros[54].

Es por ello que actualmente los avances tecnológicos y la diferencia de recursos entre estados desarrollados y subdesarrollados imponen una asimetría, que según los estrategas postmodernos debe girar, en las siguientes formas de conflicto[55]:

- Cultural: imponiendo puntos de vista culturales diferentes
- Narcotráfico: invadiendo a la nación adversaria con drogas ilegales.
- Cooperación/influencia internacional: haciendo un empleo de la dependencia/interdependencia entre los actores de la trama de un conflicto para controlar al adversario.
- Recursos: controlando el acceso a los recursos naturales o manipulando su valor en el mercado.
- Contrabando: invadiendo el mercado del adversario con productos ilegales que desequilibran su economía.

53 Luis Alberto ACUNA.La guerra irrestricta – Guerra de Cuarta Generación. Revista de Ciencias de Seguridad y Defensa (Vol. III, No. 3, 2018). Disponible en: http://geo1.espe.edu.ec/wp-content/uploads//2018/06/12.pdf

54 Anónimo. Reflexiones sobre la guerra de cuarta generación, una visión desde los actores sin recursos de poder en términos tradicionales. Disponible en: https://www.researchgate.net/publication/284574184_Reflexiones_sobre_la_guerra_de_cuarta_generacion_una_vision_desde_los_actores_sin_recursos_de_poder_en_terminos_tradicionales

55 Reflexiones sobre la guerra de cuarta generación, una visión desde los actores sin recursos de poder en términos tradicionales. Disponible en: https://www.researchgate.net/publication/284574184_Reflexiones_sobre_la_guerra_de_cuarta_generacion_una_vision_desde_los_actores_sin_recursos_de_poder_en_terminos_tradicionales[accessed Nov 13 2018].

- Tecnología: ganando ventaja en el control de tecnologías civiles y militares.
- Medio Ambiente: destruyendo aquellos recursos ambientales de la nación adversaria.
- Mercado Financiero: subvirtiendo o dominando el sistema bancario del adversario y su mercado de valores.
- Leyes internacionales: subvirtiendo o dominando las políticas de las organizaciones internacionales o multinacionales.

El conflicto asimétrico no corresponde a ningún escenario preciso, identificable en una determinada situación actual. Si bien, aún no se reúnen las condiciones que permitan la generalización de dicha asimetría, el fenómeno ha evolucionado lo suficiente como para aplicar sus teorías y poder explicar la mayoría de conflictos actuales; la guerra asimétrica o de cuarta generación ha desplazado en importancia a sus predecesoras, en virtud de las singularidades que hoy presenta el Sistema Internacional[56].

Las nuevas guerras o conflictos mencionados anteriormente, constituyen una amenaza real para los estados sobre todo los occidentales, dada su rigidez estructural y sus deficiencias, que pudieran tener en el control y manejo de los flujos financieros, humanos, o de información[57].

Con la Guerra Asimétrica los estados han ido perdiendo lo que fuera el monopolio de la violencia signado con la paz de Westfalia y actualmente tienen que enfrentar enemigos no estatales, cuyas motivaciones e intereses difieren en muchas ocasiones de aquellos que un estado tradicional busca como

56 Anónimo. Reflexiones sobre la guerra de cuarta generación, una visión desde los actores sin recursos de poder en términos tradicionales. Disponible en: https://www.researchgate.net/publication/284574184_Reflexiones_sobre_la_guerra_de_cuarta_generacion_una_vision_desde_los_actores_sin_recursos_de_poder_en_terminos_tradicionales[accessed Nov 13 2018].

57 Idem.

objetivo común para su sociedad y el campo de batalla es la mente y voluntad de las poblaciones, no el territorio[58].

En este escenario asimétrico y con gran influencia tecnológica, gracias a la dependencia generalizada y casi ineludible del uso de las redes informáticas, es donde surge la Guerra Cibernética; nuevo tipo de conflicto que trae un nuevo ambiente, totalmente diferente a los convencionales y ya explotados del mar, aire y tierra pero que se encuentra interrelacionado estrechamente con ellos: el CIBERESPACIO.

Puede decirse en términos generales que en las Guerras de Cuarta Generación el sustento primordial es la inteligencia estratégica obtenida del ciberespacio mediante satélites y servidores, la utilización encriptada de computadores que permiten la comunicación segura; mediante el empleo de aviones no tripulados de ataque y drones que realizan "bombardeos quirúrgicos" de alta precisión, o drones del tamaño de un insecto equipados con cámaras de alta resolución que permiten obtener información táctica y operativa en tiempo real y que según Pastor y Coz los ejércitos regulares los están empleando en:

- Los componentes industriales del ámbito de la Defensa
- Los sistemas no tripulados y vehículos
- Los productos de automatización para grandes plataformas, tanto navales, terrestres y aéreas
- Dispositivos de uso personal
- Dispositivos de comunicaciones (routers, firewalls, sonar o radares, entre otros)

58 Arreguín, I. How the weak win wars. New York: Cambridge University Press. 2005. Disponible en: https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf

La guerra de cuarta generación es la mejor manera de combatir la amenaza asimétrica que se presenta como movimiento insurgente, terrorista, narcotraficante o crimen internacional organizado[59].

El ciberespacio surge como la cuarta dimensión del campo de batalla y bien empleado brinda mayor poder a los Estados y fuerzas armadas que tienen capacidad para su utilización, explotación y control.

En un mundo globalizado donde prima una agenda internacional que alienta el multiculturalismo, el terrorismo en todo su espectro, tiene más poder y alcance que el que tuviera tradicionalmente a través de sus acciones reales, tiene además un alcance mayor por medio del uso de la propaganda y simbología que puede hacer circular por las redes de comunicación en tiempo real y en vez de conquistar al oponente físicamente, busca conquistar su pensamiento.

3.2. Escenarios del Conflicto[60]:

- Terrestre

Considerando que el ser humano, por su mera existencia ha tenido que desarrollar sus actividades en la tierra y que el acceso a otros escenarios hasta tanto no sea estable, el terrestre ha sido el protagonista en las disputas mayormente conocidas a través de los tiempos.

Allí es donde normalmente se generan las controversias y conflictos de intereses siendo también este espacio, el ambiente de resolución a través de la defensa o conquista de objetivos según correspondiera.

59 PASTOR, Vicente, y COZ, José. La ciberdefensa militar ante el reto de Internet de las Cosas, Revista SIC. s.p.

60 Ministerio de Defensa de España. El Ciberespacio, nuevo escenario de confrontación. Febrero 2012. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Sus características singulares, bosques, montañas, llanuras, hacen que el ser humano deba adecuarse y emplear medios específicos para el despliegue de fuerzas, sostén logístico y control situacional y táctico de las mismas.

El reconocimiento adecuado del terreno, sus características propias y condiciones hidrometeorológicas, hacen que sea crucial tener un estudio pormenorizado del mismo.

- Marítimo

Aproximadamente el setenta por ciento de la superficie del planeta Tierra está cubierta por agua; el ser humano en su búsqueda de nuevos horizontes y por el misterio mismo que estas masas inquietas representaban, no tardó en darse cuenta que las debía dominar y en ello encontraría potenciales mejoras a su calidad de vida.

A partir de la exploración de las costas y a medida que la confianza en el arte de la navegación fue afianzándose, el transporte y el comercio marítimo se fueron haciendo más populares y con ello comenzó la necesidad de ejercer cierto control y hasta dominio de los mares.

Ayudado por la lentitud que representaba el transportarse por medios terrestres, el escenario marítimo y fluvial se convirtió hasta el siglo XVIII en el medio de transporte principal de mercancías y personas. Asimismo las vías marítimas y fluviales eran casi las únicas con las que se abastecían los ejércitos de personal, armamento, municiones y víveres.

Como el terrestre, el medio marítimo presenta también características exclusivas y una preparación muy específica para poder dominarlo. En el combate se hace sobre o bajo la superficie del agua y para el desarrollo de los mismos son necesarios medios específicos como ser barcos, lanchas, submarinos, etc.

Asimismo este medio precisa de tácticas de combate particulares, pero no deja de regirse por los mismos principios que las

operaciones terrestres, donde la capacidad de fuego, el movimiento, reconocimiento previo, posición ventajosa y sorpresa, son esenciales para acercarse a la victoria.

- Aéreo

Hasta aquí el ser humano había dominado dos dimensiones y en ellas se habían circunscripto los conflictos.

No sería hasta el desarrollo del globo aerostático en el siglo XVIII, donde se diera comienzo a lo que se transformaría en la dimensión aérea. Los globos aerostáticos con sus limitaciones, permitieron que gracias a su capacidad de posicionarse elevados respecto del nivel del escenario terrestre y marítimo tuvieran una aplicación durante los conflictos bélicos.

La ventaja que daba posicionarse en la altura y ser prácticamente inalcanzable, permitió a quienes dominaban este medio poder hacer las observaciones del terreno, su estudio y la dirección y corrección del tiro de la artillería, logrando además la introducción de un nuevo escenario a la disputa en los conflictos.

El empleo masivo de este nuevo escenario no se hizo esperar y a principios del siglo XX cuando una máquina más pesada que el aire pudo elevarse por sobre el nivel del suelo y podía ser controlada y dirigida a voluntad puso en desequilibrio el balance de las relaciones de fuerza.

De la misma forma que el terrestre y marítimo, el medio aéreo presenta características únicas y diferenciadas. El combate en el aire requiere unos medios totalmente diferentes a los necesarios en los otros entornos y tácticas y procedimientos específicos.

- Espacial

Al finalizar la Segunda Guerra Mundial, fueron tales los avances tecnológicos adquiridos en el perfeccionamiento de los motores, que se dio comienzo a la carrera espacial.

Comenzando con la puesta en órbita de satélites por los 50's, las potencias, Rusia y Estados Unidos, no tardaron en conseguir que el ser humano llegue al espacio, en 1969 llegara a la Luna y el ser humano posara sus pies sobre su superficie y en 1971 se pusiera en orbita la primera estación espacial, la Salyut soviética, con fines de investigación científica y estudio del medio espacial.

Muchos son los estados que cuentan con satélites artificiales en las órbitas terrestres, algunos propios y otros compartidos, pero solamente unos pocos de ellos tienen capacidades militares espaciales reales; debiendo enfrentar costos elevados en materia de investigación y desarrollo para poder efectivamente explotar el espacio, simplemente una minoría son los que se encuentran en capacidad y competencia para afrontar un conflicto en el escenario espacial.

Sin embargo y a pesar de lo difícil y costoso que pudiera ser la competencia por estar presente y controlar parte de este escenario, cabe señalar que en el fue donde se dirimió la polaridad mundial surgida al finalizar la Segunda Guerra Mundial.

Allí la política internacional se encontraba disputada fundamentalmente por los Estados más poderosos del mundo agrupados en dos grandes bloques: el capitalista u occidental, con Estados Unidos al frente y el comunista u oriental, liderado por la Unión de Repúblicas Socialistas Soviéticas.

Esta competencia se materializó en los terrenos político, cultural, deportivo, científico y tecnológico, siendo en este último donde la conquista del espacio fue el mayor protagonista y donde pudo verse como un fin las actividades de espionaje a través de los satélites que orbitaban alrededor de la tierra.

Sin embargo el agotamiento económico por parte de la Unión Soviética se vería deteriorado en su capacidad de sostener el esfuerzo científico y de esta manera se definía el resultado de

la Guerra Fría a favor de los Estados Unidos, dándole la supremacía y el control del escenario[61].

3.3. Nuevo escenario: Ciberespacio.

La Publicación Conjunta 1-02 del Departamento de Defensa de Estados Unidos define al Ciberespacio como: "Un dominio global dentro del entorno de la información, compuesto por una infraestructura de redes de tecnologías de la información interdependientes, que incluye Internet, las redes de telecomunicaciones, los sistemas de información y los controladores y procesadores integrados junto con sus usuarios y operadores" [62].

Puede observarse en esta definición la amplitud tomada en cuanto a las partes que constituyen de manera integral este espacio estratégico y que se lo ha comenzado a denominar como uno de los cuatro Global Commons.

Los Global Commons[63] son espacios que, normalmente no se encuentran bajo la influencia de soberanías particulares y que se emplean para que las naciones o estados, transporten personas, bienes y servicios o para transmitir datos. Aguas internacionales, Espacio Aéreo y el Espacio Exterior eran los principales de acuerdo a las capacidades del ser humano de poder explotarlos y que permitían el tránsito, hasta que el ciberespacio hizo su entrada en escena y por donde se intercambian datos e ideas.

Estos espacios comunes, espacio, aire y mar, tienen como característica que son naturales y por consiguiente, si bien el

61 Artola, Ricardo. La carrera espacial. Del Sputnik al Apolo 11. Madrid, Alianza. 2009.

62 Coronel Steven E. Cahanin. USaF. Principios Bélicos del Ciberespacio. 2012. Disponible en: http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_09_cahanin_s.pdf

63 Gerald Stang. Global commons: Between cooperation and competition.European Union Institute for Security Studies. Abril 2013. Disponible en: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_17.pdf

ser humano puede ser previsor de su dinámica, generar una alteración o control de los mismos no es factible.

Sin embargo el ciberespacio es un espacio donde puede observarse la impronta del ser humano y su facultades creadoras; este ha sido capaz de diseñar no solamente el escenario, si no también las herramientas y métodos para su empleo eficiente y donde la cantidad de variables a tener en cuenta es mucho mayor y directamente proporcional a capacidad de sus arquitectos.

Partiendo de la concepción westfaliana, rectora de la política de los Estados-Nación, el Internet y el ciberespacio imponen un reequilibrio de fuerzas en que la asimetría es una estrategia por sí misma[64].

Mientras que la industria ha progresado desarrollando sus sistemas priorizando la interoperabilidad y operatividad, se dejó de lado la seguridad de los mismos, permitiendo con ello que surgieran fisuras y vulnerabilidades tanto físicas como lógicas, en sistemas operativos, aplicaciones y protocolos de comunicaciones.

Estas vulnerabilidades dieron lugar al desarrollo de los primeros virus y su gran potencial para infiltrarse en los sistemas y desarticularlos, originándose a partir de ellos una industria que supo ver el potencial de los mismos y convertirlos en las armas del ciberespacio, donde determinados sectores grupos o mafias se valen de ellos para realizar ataques que van desde ciberdelincuencia, ciberataques, ciberespionaje, y ciberterrorismo, pero que también han permitido que surja la conciencia y necesidad de impulsar la lógica Ciberdefensa.

En el mundo informatizado, las fuerzas están mucho más equilibradas que en el físico, donde el poder en cierta forma se mide a través de la capacidad de despliegue y sostén logístico

64 Ministerio de Defensa de España. El Ciberespacio, nuevo escenario de confrontación. Febrero 2012. Disponible en:https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

de las fuerzas armadas, ligadas intrínsecamente al poder nacional.

Para los estados esta circunstancia de una comunidad internacional interconectada, trae también aparejado el desafío para afrontar las dificultades que pudieran darse a partir de su empleo conflictivo, al mismo tiempo que presenta un panorama inquietante a las naciones más poderosas; por un lado, observan como su relación de poder y fuerza se desequilibra en su contra y como empiezan a intervenir actores no estatales que forman sociogramas complejos y que se imponen con ideas que atentan contra el concepto tradicional en donde el estado es el único que mantiene el monopolio en el uso de la fuerza[65].

A partir de ello se puede decir que las inversiones presupuestarias para mantener un arsenal de armamento y sistemas de armas no se encuentran atadas a importantes desembolsos, sino más bien se deben asociar con la preparación para contrarrestar las ofensivas originadas provenientes de individuos o grupos organizados con la suficiente destreza informática y una estructura para su operación estable.

Grupos tales como Anonymous[66] concentran un papel protagónico sacando de la escena al menos parcialmente a las antiguas aún vigentes organizaciones estatales.

El ciberespacio como escenario de los conflictos presentes y futuros impone un estado permanente de conflicto y agresión en donde la totalidad de los actores sin excepción, sea cual sea su nivel de desarrollo, son susceptibles de ser atacados y si bien

65 SANCHEZ MEDERO, G.: «Los Estados y la ciberguerra», Boletín de Información del CESEDEN, número 317, 2010, en: http://www.ceseden.es/centro_documentacion/boletines/317.pdf

66 MoRCillo, C. y Muñoz, P.: «Anonymous, más allá de la máscara», diario ABC, 19 de junio de 2011, en: http://www.abc.es/20110619/mediosredes/abcianonymous 201106182338.html

no son agresiones cruentas, sus efectos sobre las personas, sociedades y organizaciones son totalmente reales[67].

Los usuarios del ciberespacio suponen en su conjunto una masa de potenciales agresores, difíciles de poder identificar y donde el Derecho Internacional tiene vacíos normativos para responder a situaciones de ciberataques y la atribución de responsabilidades[68]. La situación es compleja y se debe ser medido a la hora de tomar medidas, dado que a pesar que un ataque a sus redes estatales provenga de un servidor del gobierno, no puede tenerse certeza que tenga el respaldo del mismo[69].

La posibilidad de hacer daño desde el ciberespacio tiene potencialidades para todo tipo de organizaciones terroristas, criminales, etc. proporcionando un instrumento multiplicador de sus propias capacidades que los convierte en peligrosos y les da un alcance superior.

La notoriedad que buscan estas organizaciones está garantizada por la repercusión mediática que tienen los incidentes informáticos, especialmente cuando se combinan con acontecimientos de gran relevancia cuya seguridad física haría muy difícil actuar contra ellos directamente.

Asimismo la utilización de las redes informáticas es un elemento común para la captación, propaganda, financiación, instrucción y entrenamiento de redes criminales, constituyendo al ciberespacio en un elemento igualador de capacidades y reductor de asimetrías[70].

67 Ministerio de Defensa de España. El Ciberespacio, nuevo escenario de confrontación. Febrero 2012. Disponible en:https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

68 Jesús REGUERA. ASPECTOS LEGALES EN EL CIBERESPACIO. LA CIBERGUERRA Y EL DERECHO INTERNACIONAL HUMANITARIO. 18 de marzo 2015. Disponible en:http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

69 LiBiCki, M. C.: Cyberdeterrence and Cyberwar, RAND Corporation, 2009.

70 Gómez de ÁgReda, Á.: «Riesgos y amenazas en y desde el ciberespacio», Seguridad Global, número 1, Instituto Choiseul España, 2011.

Comparando los conflictos habidos en las últimas décadas en los que de alguna manera se aplicaron tácticas de ciberguerra con aquellos ocurridos del último siglo, se puede decir sin entrar en detalle que, las causas que los originaron, actores involucrados y las fases por las que pasaron son similares en cuanto a las consideraciones generales, llegando a la conclusión que los conflictos han sido y siguen siendo los mismos a lo largo de la Historia, y lo único que han variado han sido los escenarios en los que se llevaron a cabo[71].

Luego de los escenarios tradicionalmente conocidos en donde el ser humano se ha acostumbrado a enfrentarse, la comunidad internacional se encuentra frente a un nuevo escenario, desarrollado de manera vertiginosa desde que comenzara a existir la computadora, donde la sociedad se ha hecho totalmente dependiente y en el que la amenaza es constante.

3.4. El Conflicto en el Ciberespacio[72].

El ciberespacio es un ambiente cuya principal característica es que no existen los límites geográficos, no es un escenario físico; engloba a todos los grupos y organizaciones o individuos, formando un conglomerado de partes que, buscan controlar el escenario y en ese afán por prevalecer surge la competencia y confrontación de intereses dando lugar a los conflictos, que por cierto podría llamarse a partir de ello ciber conflicto (confrontación entre dos o mas actores de la comunidad mundial en donde al menos uno de ellos emplea ciberataques contra el otro).[73]

71 Luis Felipe COLLANTES. La ciberguerra en los conflictos modernos. Trabajo de Investigación. Santiago de Chile. Agosto 2012.

72 LUND, Michael S.: Curso de Certificación de Análisis de Conflictos, U.S. Institute of Peace, en: http://http://es.scribd.com/doc/61965893/5/Pazinestable

73 Ministerio de Defensa de España. El Ciberespacio, nuevo escenario de confrontación. Febrero 2012. Disponible en:https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf

Estos conflictos pueden ir desde disputas por el dominio de la información hasta aún más complejos como operaciones de ciberataques entre Estados que son ejecutados de manera aislada, o bien como parte de una guerra convencional. Por el absurdo vale la pena destacar el caso de Estonia donde los ciberataques que se llevaron a cabo no formaron parte de una confrontación de otros espacios.

Como en todo proceso, dentro de las Relaciones Internacionales y como parte de la sinergia entre estados y sociedades que los componen, hay diferentes etapas bien definidas que corresponden a[74]:

- **Paz:** países que no están enfrentados y luchan por intereses legítimos no convergentes.
- **Paz inestable:** intereses nacionales contrapuestos entre los estados. La tensión es elevada pero no hay violencia.
- **Tensión:** inestabilidad en aumento que genera alteraciones en la cotidianeidad de un Estado y su acción de gobierno, imponiendo un potencial peligro a la seguridad nacional ocasionando se activen los procesos y sistemas para el empleo de los recursos de la Defensa Nacional.
- **Crisis:** dentro de una situación de tensión existen momentos decisivos que son el disparadores de consecuencias aparejadas a la movilización de las Fuerzas Armadas.
- **Conflicto armado:** confrontación física organizada, aunque no necesariamente reconocidas a la luz del Derecho Internacional, caracterizada por el empleo de medios militares de combate con la finalidad de imponer cada una su voluntad.

74 United States Institute of Peace. Curso de Certificación en Análisis de Conflictos. 2004. Disponible en: http://online.usip.org/spanish/analysis/2_3_1.php

- **Guerra:** forma más violenta y desarrollada de los enfrentamientos a partir de la declaración de guerra correspondiente, donde existe la confrontación entre cuerpos políticamente organizados y con una estructura cuya finalidad es imponer la voluntad de una sobre otra o de defender los propios intereses. Se caracteriza por el empleo masivo y organizado de medios de combate.

Puede observarse que los conflictos en su evolución van pasando por diferentes etapas en el proceso de escalada de los grados de violencia, sin embargo y conforme a como van avanzando, por su versatilidad y gran espectro de aplicación e incidencia, la ciberguerra tiene presencia desde las primeras fases del conflicto.

Los medios informáticos han sido los que en gran medida y a partir su creación los que permitieron la construcción del mundo globalizado actual. El nivel de interconexión alcanzado por la raza humana, su capacidad de interacción, el acortamiento de las distancias y la simultaneidad de eventos posibles de ocurrir, han hecho que actores estatales y no estatales formen un sociograma virtual donde la influencia entre ellos es mutua y dan vida a una red en tiempo real.

Por ello los conceptos de globalización y ciberespacio van necesariamente unidos en este mundo moderno. Nuevas formas de poder en el que la información es de vital importancia y donde las fronteras han desaparecido y no existen los límites y hasta la identidad de se ve tergiversada[75].

Si las relaciones de poder dependen hoy más que nunca de la capacidad de obtención, clasificación y diseminación de información, el poder administrar la misma, de la manera y para lo que se necesite, en tiempo real y sin límite físico, hasta un número virtualmente ilimitado de receptores y en tiempo real

75 POZAS HORCASITAS, R. Globalidad - Léxico de la Política. Editorial Fondo de Cultura Económica. México. 2004.

supone sin ninguna duda capacidades que amplían el poder de un actor.

La diversidad y volumen de la información accesible en la red Internet como así también la interactividad, superan ampliamente la que cualquier otro medio de comunicación masivo, como son la radio y la televisión han sabido manejar.

El ciberespacio no solamente permite el acceso irrestricto a datos, ideas e información, también a través del mismo circulan la mayor parte del flujo financiero y por medio de el se puede llegar a modificar la conciencia colectiva de una sociedad o grupo de personas.

El ciberespacio permite, siempre y cuando la red tenga la capacidad de absorber la demanda, que la influencia de la información sea inmediata y simultánea, e inclusive que se actualice de manera constante y tan rápida que en muchas ocasiones no el mundo virtual muta sin que el entorno humano perciba los cambios.

En la actualidad el mundo globalizado necesita del ciberespacio. El ciberespacio forma una amalgama entre la oferta y la demanda en todos los órdenes de la vida y en la Comunidad Internacional, quien requiere de la estructura y capacidades de este mundo virtual para poder existir y gestionar.

Para el Departamento de Defensa de Estados Unidos, el ciberespacio es un campo de operaciones cuya entidad es igual a la tierra, el mar, el aire o el espacio y por ello considerado un escenario donde las operaciones defensivas y ofensivas, pueden llevarse a cabo[76].

Pese a que es un espacio virtual, el ciberespacio es un entorno físico de mayor extensión que los tradicionales; esto siempre

76 Department of Defense Strategy for Operating in Cyberspace. Julio 2011.Disponible en: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

teniendo en cuenta que está compuesto por una red de equipos informáticos y de comunicaciones, interconectados mediante enlaces físicos o inalámbricos, cables u ondas de radio o Wi-Fi, que constituyen una madeja de redes ligadas entre sí. En cuestión, es una supradimensión que engloba los espacios terrestre, marítimo, aéreo y espacial.

Los medios específicos para moverse, desenvolverse y combatir en este escenario, deben estar especialmente diseñados y configurados, computadoras de escritorio o portátiles, tabletas, teléfonos inteligentes y cualquier equipo que emplee un software, que sea por estar abierto a la red o vulnerable físicamente, requieren de sistemas de detección de intrusos, componentes de hardware robustecidos, sistemas operativos y aplicaciones especialmente diseñados y codificados, que inclusive deben responder a configuraciones reforzadas y redundantes para permitirles alta disponibilidad en caso de ataques.

El ciberespacio y sus operaciones impone el empleo de doctrina, tácticas y técnicas específicas, difícilmente de mantener actualizadas dada la gran velocidad de mutación del medio; lo que sirve para un caso particular, puede llegar a ser diametralmente opuesto para otro[77].

A pesar de tratarse de un mundo virtual, el factor humano es fundamental. Debido a que el ser humano es su creador y quien se encarga de continuar con su desarrollo y evolución, su presencia es crítica dado que no pueden los sistemas autogobernarse, siempre habrá una persona que controle, administre, configure, programe y/o repare los sistemas informatizados sin dejar de lado lo más importante que es el proceso de la toma de decisiones, siempre habrá alguien que plantee un objetivo

77 Department of Defense Strategy for Operating in Cyberspace. Julio 2011.Disponible en: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

estratégico, lo tenga que operacionalizar y tácticamente ejecutar.

El ciberespacio es un dominio que no se encuentra perfectamente limitado como el resto de los escenarios conocidos y ya mencionados, pero integra a los mismos, cada vez que en cada uno de estos dominios exista un punto de comunicación que se encuentre enlazado con otro, ya sea por cable o inalámbricamente.

De tener que hacerse una estratificación del conflicto, el ciberespacio debería ser la primera de ellas, el primer escenario a ser jugado, sobre todo teniendo en cuenta que el ciberespacio no solamente se puede extender su impacto al centro de gravedad del combate, también es extensivo a desarticular el mismo centro de gravedad de los poderes del estado, afectando su supervivencia y sostenimiento.

De la mano de la evolución tecnológica e informática, evoluciona el ciberespacio, entendiendo a este como el conjunto de sistemas informatizados y de comunicaciones junto a sus operadores. Esto plantea un interrogante acerca de las causas que dan pie a esta imposición firme de un escenario de conflicto virtual y donde la intensidad y frecuencia de los mismos es cada vez mayor.

Es claro que por la propia concepción del escenario, este puede ser accedido por cualquier organismo estatal o no estatal, y a partir de allí surge la implementación del sigilo en las acciones llevadas a cabo, puesto que este acceso puede ser anónimo y hacerse mediante acciones que hagan muy difícil saber, o hasta imposible ubicar al ejecutor, dando además cierta inmunidad respecto de posibles represalias.

Las armas por excelencia en este escenario son simples sistemas informáticos, que operados por personal especializado, hacen que tengan una eficiencia en su accionar cuyos resultados son positivamente desequilibrantes y transforman a la ciberguerra en un paradigma al alcance de aquellos con menos recursos económicos. Un equipo sencillo en las manos correctas, puede

llegar a originar y sostener de manera individual acciones suficientes como para paralizar un estado.

Asimismo su capacidad para introducir propaganda y hacer difusión, son incomparables. Un atacante puede buscar y obtener adhesiones a su causa gracias a la fácil difusión pública que permite la Red, siendo los riesgos físicos del que se adhiere a una causa pocos o nulos[78].

Ejemplo de ello es el acontecimiento que tuviera lugar en año 2008, donde Israel al tratar de romper el bloqueo de Gaza, sufrió una serie de ataques cibernéticos contra alguna de sus instituciones por parte de grupos y personas que se adherían de manera voluntaria a la causa palestina; mediante la descarga de un malware desde determinada página web, se conectaba a la computadora del internauta a una botnet, que era la que ordenaba los ataques de denegación de servicio contra los sitios israelíes[79].

El impacto psicológico que se genera sobre el blanco, con la simple denegación del servicio o alteración de la página web socaba la voluntad. Esto particularmente se da por la sensación de vulnerabilidad e impotencia que surgen a partir de la recepción de un ataque.

Esta sensación se produce por el hecho de saber que se están sufriendo ataques y se desconoce su origen y se encuentran diseminados a lo largo de la red mundial, produciendo además un efecto desmoralizador. Sumado a esto se puede incrementar el efecto cuando los ataques son factibles de transmitirse en vivo, caso de los ataques de Anonymous a países suramericanos,

78 Carrillo, R. (1995). La guerra psicológica.Departamento de Estado de los Estados Unidos. Agenda de la política exterior de los Estados Unidos. Abril 2012. Disponible en: de usembassy-mexico.gov: http://www.usembassy-mexico.gov/bbf/ej/ijps0301.pdf

79 Disponible en: http://www.europapress.es/tecnologia/internet00446/noticiawebbancoisrael cerradadosdiasciberataqueislamista20080428184547.html y https://cert.s21sec. com/index.php?option=com_content&view=article&id=279:loshackerssesirven delconflictodegazapara-difundirmalware&catid=53:otros&Itemid=69

operación Andes Libres que iba siendo anunciada por Twitter y Facebook[80].

De la mano del impacto psicológico, también va la disuasión; un ciberataque bien dirigido y previo al choque de las fuerzas convencionales, esta en capacidad de desarticular las mismas, hasta dejar al estado en un estado de indefensión casi total. Caso de Georgia durante el año 2008[81].

La información puede considerarse lo más valioso que tiene el ser humano dado que controla la vida social y personal de las personas y en ella se basan fundamentalmente las decisiones políticas, económicas, militares y sociales que un estado puede tomar. Es por ello que se depende irremediablemente de los sistemas de información y las comunicaciones constituyendo ellos un centro de gravedad para los estados desarrollados y los transforma en objetivos críticos.

Analizando profundamente las estructuras de los estados, sus fortalezas y debilidades, sus medios y fines y viendo ejemplos históricos podríamos asegurar que hoy el control del ciberespacio es la meta inicial para un actor en un conflicto. Asimismo la declaración explícita de un conflicto, la gestión de ataques preventivos o preemtivos, hoy debería sin duda materializarse en el ciberespacio.

Vale decir, si hoy replicáramos las tensiones políticas entre Japón y los EE.UU en la II GM, el Pearl Harbour de los EE.UU sería un ataque a sus redes de comunicaciones, informáticas y herramientas digitales.

80 Anónimo. Operación Andes Libre Segunda Fase. Diario La República. Junio 2011. Disponible en: https://larepublica.pe/tecnologia/551680-operacion-andes-libre-segunda-fase-que-webs-han-caido

81 Néstor Ganuza ARTILES.LA SITUACIÓN DE LA CIBERSEGURIDAD EN EL ÁMBITO INTERNACIONAL Y EN LA OTAN. Febrero 2010. Disponible en:https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=2ahUKEwj51ZCAifHgAhWxCtQKHdAmDD8QFjAGegQIBhAC&url=https%3A%2F%2Fdialnet.unirioja.es%2Fdescarga%2Farticulo%2F3837337.pdf&usg=AOvVaw3dzew59vZogrFtZF8sSCOF

3.5.Guerra Cibernética.

Con el auge y el crecimiento constante de la Era de la Información, junto a la introducción masiva de la tecnología digital y el enlace de datos a través de las redes informáticas, el ciberespacio es un escenario que ha ido cobrando importancia y materializándose de manera constante como un ambiente favorable, para el desarrollo de la vida humana.

Gran parte de las actividades llevadas a cabo, por no decir su totalidad, gubernamentales, financieras, económicas y militares se valen de las facilidades impuestas por la tecnología y hacen un amplio uso de este escenario y las redes de información que se tienen a lo largo de este.

Distintas formas de incidir no solamente en la información que se puede encontrar en la red cibernética, sino también golpear el centro de gravedad de las infraestructuras que permiten la comunicación de estos datos e información.

Desde Crímenes cibernéticos, manipulación de información, espionaje empresarial y estatal, el ciberespacio junto con la Guerra Cibernética han establecido por su accionar la idea que este ambiente podría ser tenido en cuenta como uno de los nuevos ambientes de Guerra y equiparable a la hora de diagramar los planes de contingencia, con los conocidos aire, mar y tierra y espacio, siendo de esa forma un problema de escala global y que atraviesa transversalmente a todos los núcleos de poder del estado y la vida del ser humano[82].

Como todo nuevo escenario, con su aparición, ha traído la necesidad imperiosa de establecer nuevas reglas de comportamiento, aptitudes para su empleo, limitaciones y vulnerabilidades. A partir de ello, los conceptos de la defensa y seguridad de un estado, convencionales como se conocían, han

82 Lukasik, S., Goodman, S. & Longhurst, D. Protecting Critical Infraestructures Against Cyber-Attack. Oxford University Press for The International Institute for Strategic Studies. London, UK. 2003.

tenido que comenzar a redefinirse para poder adaptarse al nuevo espacio que tiene como una de sus características propias ser intangible.

Es así como países en la vanguardia tecnológica, caso Estados Unidos, Israel, China, Japón y otros pertenecientes a la Unión Europea, comenzaron a verlo como un desafío y volcaron un esfuerzo de personal y material para crear áreas de la defensa y seguridad directamente relacionadas con el desarrollo y uso de variados sistemas para contrarrestar esta amenaza.

3.6 Naturaleza y Concepto de la Ciberguerra.

La guerra ha existido desde que el hombre es un ser social. Su condición de vida en comunidad, no solamente lo han favorecido en su desarrollo, también le han impuesto la necesidad de evolucionar y para ello fue necesario plantearse intereses que en muchas oportunidades han sido compartidos o se han opuesto generando con ello crisis o desequilibrios en el status quo de la comunidad internacional.

La naturaleza primaria de la guerra siempre ha sido el de la consecución de un objetivo o interés por medio de la imposición de la fuerza. Como se ha visto anteriormente el político tiene a su alcance como herramienta de disuasión y poder el monopolio del uso de las armas.

Sin embargo con el correr del tiempo y a medida que la tecnología, tácticas y estrategias han ido evolucionando, también lo ha hecho la guerra y la forma de hacerla.

A grandes rasgos los enfrentamientos de tropas en extensas formaciones y las falanges, fueron creciendo en su complejidad y capacidades, conforme fueron apareciendo los diferentes materiales, el bronce y el hierro, la rueda, el arco y la flecha, la pólvora, el dominio del vuelo y la navegación, los agentes químicos, la energía nuclear y en la actualidad la tecnología

cibernética, sin embargo puede decirse que ha mantenido su esencia.

La guerra cibernética o la ciberguerra es sencillamente el arreglo de los medios tecnológicos desarrollados por el ser humano para su empleo y dominio de los diferentes aspectos que requieren de su empleo para tener accesos y control a la información, permitiendo con esto la manipulación de la misma.

De acuerdo a lo establecido en el Diccionario Militar de los Estados Unidos, es la dimensión que contiene la infraestructura tecnológica, internet, redes de telecomunicaciones, sistemas de computadoras, procesadores, controladores, softwares y hardware como parte integradora de la red de información global[83].

Es en el ciberespacio donde se llevan a cabo las operaciones de Ciberguerra, entendiéndose por ellas al conjunto de acciones ejecutadas por una nación o estado a fin de penetrar en la red informática de otra nación o estado con el propósito de causar daños[84].

Desde la aparición de la informática, el mundo se ha transformado, favoreciendo la interdependencia y la globalización en todos los aspectos, sobre todo en donde la revolución tecnológica con su avance en cierta forma descontrolado dio lugar a la aparición de las armas cibernéticas.

A través de estas armas se puede lograr la parálisis parcial y/o total de los sistemas de información, su funcionamiento errático o intermitente como así también hacer incurrir en errores a los usuarios errores, inclusive haciendo colapsar los sistemas de comando y control en general.

83 Rain, O. & Lorents, P. (2010). Cyberspace: Definitions and Implications., Cooperativa Cyber Defence Centre of Excellence, Tallinn, Estonia. 2010.

84Adolfo Arreola García. Ciberseguridad, la nueva cara de la seguridad internacional. Agosto 2015. Disponible en:http://www.academia.edu/36092683/Ciberseguridad_la_nueva_cara_de_la_seguridad_internacional

Las operaciones en una visión general, no distan mucho de la clasificación clásica de un conflicto bélico tradicional en su esencia. Pueden clasificarse de acuerdo al tipo de blanco e interés objetivo: ofensivas, acciones en búsqueda de la interrupción, negación, degradación o destrucción de la información y sistemas de control; defensivas, adoptadas en búsqueda de dar protección y respuesta inmediata ante la detección de actividades no autorizadas y por último, las de recolección de información asociadas normalmente a tareas de inteligencia.

Respecto de su ambiente de operación, así como existen los ambientes que dan característica al tipo de conflicto en cuanto a su medio de acción, aire, mar y tierra, la ciberguerra tiene el propio que es donde se amalgama y circunscribe el tipo de acciones mencionadas, el ciberespacio: dominio global que incluye el espectro electromagnético y electrónico, utilizado para el almacenamiento e intercambio y explotación de la información por medio de las redes informáticas.

Este entorno es el que impone la complejidad de no reconocer límites ni fronteras, actores estatales o grupos rebeldes, prácticamente velados por esta falta de condiciones. Los usuarios del ambiente tienen acceso prácticamente ilimitado para concluir en la búsqueda de intereses u objetivos. Aquí es donde se comprueba más que nunca que el manejo de la información es el origen del poder, y su control se traduce en el control del objetivo material[85].

Su alcance gracias a la constelación de satélites en órbita es casi ilimitado, y con esto deja bien planteado que su accionar coordinado y correctamente dirigido inutiliza entre otras cosas, sistemas de comunicación y la consiguiente capacidad de comando

85 Jesus REGUERA SANCHEZ. Aspectos Legales En El Ciberespacio. La Ciberguerra Y El Derecho Internacional Humanitario. 18 marzo 2015. Disponible en:http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario

y control de un estado, conllevando con ello a la desestabilización y por traslación a quebrar la voluntad de vencer del adversario, fin en si mismo de la guerra[86].

Este ciberespacio y la ciberguerra conforma de una arquitectura compleja, agrupa usuarios, redes y dispositivos que sirven como contenedores para el software y sistemas de procesamiento en general, los mismo que a su vez se utilizan para administrar y facilitar el flujo, entrada y salida de información que se encuentra almacenada en los distintos servidores, empleando aplicaciones, servicios y/o sistemas que se encuentran conectados de manera directa o indirecta a una red dada[87].

Los ataques cibernéticos ya sea por medio de computadoras o inclusive hasta por celulares pueden afectar a la totalidad del universo conectado a la red informática o de comunicaciones y con ello lograr la desestabilización de diferentes sectores tanto civil como militar, privado como estatal.

La información y capacidad para administrarla, se han transformado en factores relevantes para la coyuntura y avance social; han coadyuvado al desarrollo del ciberespacio como un medio y dimensión relevante para la defensa y la seguridad de los Estados y las personas, dando lugar así a su naturaleza, instaurada a partir del uso masivo del espectro informatizado y de la gran cantidad de vulnerabilidades que se encuentran presentes en él.

3.7 Actualidad de la Ciberguerra.

86 Richard A. Clarke, Robert K. Knake Guerra en la red: Los nuevos campos de batalla. Grupo Planeta Espana. Febrero 2011.50 Lourdes CIRLOT. Arte, arquitectura y sociedad digital. Ediciones Universidad Barcelona, 2007.

La ciberguerra seguramente no hubiese llegado a la escala actual de no haber sido por las redes y sobre todo por aquella que es la que impone un ritmo de crecimiento tecnológico veloz, el INTERNET.

Habiendo comenzado como un proyecto universitario[88], hoy se constituye en la red mundialmente accesible que permite y facilita el intercambio de datos e información entre diferentes tipos de usuarios, gubernamentales y no gubernamentales principalmente. A través de ella se puede ejercer el control del sistema financiero, como así también de distintos tipos de diligencias y acciones.

Este ambiente tan particular y al mismo tiempo común a todas las actividades o al menos su mayoría, realizadas por el ser humano, sufre constantemente amenazas y ataques que evolucionan e imponen una necesidad creciente de mantenerse a la vanguardia tecnológica a fin de poder desarrollar modos de acción que permitan contrarrestar las amenazas y ataques, como es el caso de los virus y otros tipos de operaciones ligadas a la disrupción de las redes que pudiera sufrir las un estado.

Un estado debe contar con la capacidad ininterrumpida de comunicación y control de sus sistemas, inclusive en aquellas ocasiones donde pudiera llegar a existir conflictos o crisis que atentaran contra su seguridad y defensa.

Las comunicaciones concisas y efectivas tanto a nivel doméstico como internacional son cruciales para mantener las relaciones entre los estados con un bajo nivel de conflicto y accesibles para mantener los canales de comunicación.

La redes de computadoras inmersas en un ambiente de Internet seguro y protegido gracias a las herramientas existentes para el cifrado, así como el sistema de

88 Stephanie Falla Aroche. La historia de Internet. Febrero 2006. Disponible en:http://www.maestrosdelweb.com/editorial/internethis/>

posicionamiento global (GPS), son la base técnica para una multiplicidad de innovaciones técnicas y estratégicas[89].

Este contexto brinda el escenario ideal para el desarrollo de las capacidades requeridas por la guerra cibernética y permite integrar la información de planificación y ejecución, tanto de orden civil como militar de las diferentes tareas, asegurando con ello su vital importancia en la acertada evolución efectiva de las mismas.

Asimismo, es el que presentan las redes sociales, como es el caso de Facebook, Instagram y Tweeter entre otras, sin dejar de lado las gran serie de aplicaciones que se utilizan para hacer más práctica la vida cotidiana y donde el usuario no se percata de la cantidad de información sensible que vuelca en estas como ser datos relacionados con sus tarjetas de créditos, finanzas e información personal[90].

Ahora bien, queda claro que los niveles de seguridad informáticos estarán asociados a las vulnerabilidades que pudieran encontrarse y de ello en cierta forma se desprenderán los tipos de acciones cibernéticas.

Este tipo de acciones cibernéticas tienen motivaciones intelectuales o económicas y políticas, dado que las consecuencias no se centran exclusivamente en un daño económico, sino en los conflictos entre países que demuestran y miden sus fuerzas.

En diciembre de 1995 los usuarios de Internet ascendía a 16 millones, para el 2001 pasó a ser de 458 millones y en enero de 2010 explotó 1.700 millones[91].

89 Richard A. Clarke, Robert K. Knake Guerra en la red: Los nuevos campos de batalla. Grupo Planeta Espana. Febrero 2011.

90 Edición del día.Ciberataques interrumpen servicio de Twitter, Spotify y otros sitios web en Estados Unidos Disponible en: https://www.laizquierdadiario.com/Ciberataques-interrumpen-servicio-de-Twitter-Spotify-y-otros-sitios-web-en-Estados-Unidos. Viernes 21 de octubre de 2016.

91 www.internetworldstats.com/stats.htm

Durante el año 2008, Symantec creó 1,6 millones de nuevas armas a fin de atacar los sistemas informáticos[92].

La Base de Datos Nacional de Vulnerabilidades de EEUU[93], ha sido la encargada de concentrar aquellas intrusiones a los sistemas informáticos y al 2010 tenia un aproximado de 45.000 casos.

Si hacemos una proyección estadística desde ese momento hasta la actualidad, se podría tener una perspectiva exponencial del crecimiento de ataques, intrusiones a las redes, sobre todo con la expansión que las mismas han tenido en la última década.

Tanto en el escenario político como militar los medios de comunicación se han constituido como necesidad primordial en la obtención de información. Ya fuera para sostener un mercado de valores, dar justificación a una guerra, imponerse en elecciones presidenciales o desestabilizar la economía o vida social de un estado, los líderes mundiales han recurrido constantemente a los planes de desinformación masiva buscando la modelación de la percepción pública[94].

Se podría llegar a sostener que todo medio que se utilice para la transferencia de información, administrado eficientemente constituye una parte fundamental del proceso sistemático de análisis durante el desarrollo de una situación dada en el escenario correspondiente, sea este parte o no de una crisis o conflicto.

Una información determinada, positiva o negativa, transforma inevitablemente el desenlace de una crisis haciendo que los objetivos buscados por los actores involucrados y sus intereses sean manipulados en pos de obtener resultados satisfactorios en

92 Enlace:www.symantec.com/business/resources/articles/article.jsp?aid=20090511_symc_malicious_code_ activity_spiked_in_2008.

93 National Vulnerability Data Base. U.S. Government.Disponible en: http://nvd.nist.gov/

94 Rosa Maria ARTAL. Adoctrinamiento: Nuevas técnicas para viejos fines. Disponible en: https://www.eldiario.es/zonacritica/Adoctrinamiento-Nuevas-tecnicas-viejosfines_6_752134800.html. 20 marzo 2018.

la negociación. Por ello resulta esencial lograr el dominio de la información en todo momento.

Nuevamente, a partir de la caída de la Unión Soviética y el fracaso del comunismo, sobrevino el final de la lógica que había dominado en cierta forma las Relaciones Internacionales con el fin de la Segunda Guerra Mundial; Estados Unidos se convirtió en la única superpotencia con capacidad de nuclear y proyección militar al frente del nuevo orden mundial[95].

Su poder durante la Guerra Fría, le permitió afianzarse y transitar un camino hacia la consolidación de la superioridad militar y alzarse con ello en el dominio absoluto sobre los espacios comunes, mar, aire, espacio exterior y ciberespacio[96].

Este dominio de los espacios comunes es precisamente lo que habría permitido a Estados Unidos su desarrollo económico a gran escala en las ultimas décadas, no obstante el cambio se esta aproximando y su hegemonía esta perdiendo balance a partir de la aparición de una China fuerte y decidida a ser imperante en la economía mundial[97], como así también con la firme idea de gobernar primero el ciberespacio, antes que combatir abiertamente en otros frentes; de allí surge su interés en gobernar las 5 G en muchos lugares del globo y la negativa americana a permitir esa acción.

Estos espacios comunes, Global Commons son entornos en donde ninguna persona o estado puede tener su propiedad o control y que son elementales para la vida; su potencial normalmente para el desarrollo de la sociedad, conocimiento y la vida es fabuloso.

Dado este escenario, cualquier enfrentamiento futuro deberá desarrollarse necesariamente y de manera primordial en el ámbito

95 FRIEDMAN, G.The next 100 years: A forecast of the 21st Century. Black Inc. 2011.

96 Alexander KUTT NEBRERA. LA IMPORTANCIA DE DOMINAR LOS GLOBAL COMMONS EN EL SIGLO XXI. Disponible en:http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM292015_Global_Commons_XXI_Alexander_Kutt.pdf 12 noviembre de 2015.

97 ZAKARIA, F. The Post American World. Norton. 2001.

de los espacios comunes, pues su dominio favorecerá el status de superioridad internacional[98].

En virtud de las crecientes tensiones entre las grandes potencias y la aparición y desarrollo de estos nuevos espacios como es el ciberespacio, resulta lógico observar nuevas tendencias geopolíticas por parte de los estados de la comunidad internacional[99].

3.8 El Ataque Cibernético, Técnicas y Efectos.

Inicialmente todo comenzó como un juego y en su gran mayoría, los actores que constituían las amenazas eran los hackers, intelectuales que no hacían otra cosa que buscar popularidad al arrogarse el haber evadido y quebrado los sistemas de protección contra intrusiones de organizaciones variadas[100].

Sin embargo, hubo un cambio radical y puede decirse que la ciberdelincuencia, ya no se trata de un juego, que las motivaciones pasaron a tener otros objetivos y en gran parte asociados al beneficio económico, sin necesidad de aclarar que de manera fraudulenta[101].

Lo importante y a destacar es que aquello que fue tomando fuerza con el transcurrir del tiempo y los avances tecnológicos como fue el robo de identidad, información, fraude bancario y violación de la privacidad, entre otros delitos, la amenaza que sirve de elemento coercitivo y alienta a los estados y organismos que precien su seguridad es sin duda el ciberterrorismo.

Bien conocida y flagelo de la comunidad internacional en general, la Yihad Global se sustenta en el plano operativo, ataques

98 LEJARZA ILLARO, E. Estados Unidos – China: Equilibrio de poder en la nueva Ciberguerra Fría. Instituto Español de Estudios Estratégicos. 2013.

99 LOWENTAL, A. F. The US in the Early 21st Century: Decline or Renewal? Real Instituto Elcano.2013.

100 History & Impact of Hacking: Final Paper. Disponible en:https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf. December 2006.

101 MADARIE, Renushka. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers Research and Documentation Centre (WODC), The Netherlands.June 2017. Disponible en: http://cybercrimejournal.com/Madarievol11issue1IJCC2017.pdf

suicidas de media y gran escala y en la gestión, en el ciberespacio a través de la Internet; por medio de este último es que logra administrar el mando, control y las comunicaciones de cualquier ataque terrorista que planifique perpetrar[102].

El ciberespacio es también la principal herramienta de propaganda, distribución de ideas, reclutamiento de voluntarios y recaudación de fondos de los terroristas islámicos[103].

Como no podría faltar y totalmente necesario en el ambiente político como empresarial, el ciberespionaje tiene su protagonismo, países como China[104] y Rusia[105] lo han transformado y abrazado como uno de sus métodos principales, obteniendo información sensible; Titan Rain es un ejemplo de cómo China intentó apoderarse de información de los gobiernos de Inglaterra y Estados Unidos[106].

Ahora bien, hasta aquí se puede observar que hay tres grandes grupos que concentran los ciberataques, si las consecuencias de un ciberataque son de alcance político gubernamental, se lo considera CIBERGUERRA. De manera similar si el ataque tiene un objetivo terrorista, se lo denomina CIBERTERRORISMO; si lo que se busca tiene connotaciones orientadas a la obtención ilegítima de información, se lo puede llamar CIBERESPIONAJE. Tanto el ciberterrorismo y el espionaje son ilegales, sin embargo, cuando se trata de delitos comunes que presentan características que apuntan a la manipulación de información

102 CARLINI, Agnese. ISIS: Una nueva amenaza en la era digital. Instituto Español de Estudios Estrategicos. Diciembre 2015. Disponible en:http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-2015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf

103 Idem.

104 BROWN, Kerry. Contemporary China. 2015.

105 Michael Connell and Sarah Vogler.Russia's Approach to Cyber Warfare March 2017.

106 Remembering Operation Titan Rain. Octubre 2016. Disponible en: https://cyware.com/news/remembering-operation-titan-rain-c54ad3e4.

bancaria, tarjetas de crédito, etc. el término empleado es el CIBERCRIMEN[107].

Es necesario en un principio focalizarse en cuales fueron los objetivos del ciberataque, dado que las acciones propias de este ambiente de guerra al emplear no solamente métodos progresivos, si no también secuenciales, hace que se dificulte la localización y clasificación de la fuente de emisión que lo generó y por consiguiente su agrupamiento.

A continuación se detallan algunos de los ciberataques más conocidos y perpetrados en la comunidad internacional[108]:

- 1982: Sabotaje gasoducto Siberiano
- 1983: "Juegos de Guerra"
- 1984: Virus de Ordenador Pakistaní "BRAIN"
- 1986: "El huevo del cuco" de Clifford Stoll, primer caso documentado de ciberespionaje en el Lawrence Berkeley National Laboratory
- 1988: Robert Morris crea el Gusano "Morris Worm", atacando más de 6000 ordenadores
- 1992: Creación Virus "Dark Avenger"
- 1997: Operación "Elegible Receiver", 1er ejercicio de ciberguerra de EE.UU.: Joint Task Force Computer Defense (Fuerza de Tarea Conjunta de Ciberdefensa)
- 1998: "MoonlightMaze": ciberpenetración en el pentágono, NASA y Departamento de Energia de los Estados Unidos
- 2003: Nace Anonymus

107 SÁNCHEZ MEDERO, Gema. LOS ESTADOS Y LA CIBERGUERRA . Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010

108 RUSSINOVICH, Mark. Trojan Horse: The Widespread Use of International Cyber-Espionage as a Weapon RSA Conference 2013. Disponible en:https://www.rsaconference.com/writable/presentations/file_upload/exp-r35.pdf

- 2005-2010: Primer Ataque Cibernético conocido de EEUU a Irán "STUXNET"
- 2006: WikiLeaks.
- 2006-2011: "ShaddyRat": penetración de 72 compañías e instituciones gubernamentales.
- 2007: Ataque al gobierno estoniano, denegación de servicios.
- 2008: Guerra de Osetia del Sur: ataque a Alania TV y denegación de servicios en sitios web de Georgia y Azerbaiyán.
- 2008: Ataques a sistema de información de campañas de Obama y McCain.2009-2012: "Flame": software malicioso, complejo y multi-componente dirigido a Irán.
- 2009-2012: "Gauss": Similar a Stuxnet, enfocado a ciberespionaje.
- 2009-2010: Operación Aurora, penetración para modificar código de fuente de Google y Adobe.
- 2009-2011: NightDragon, extracción de información de compañía energética.
- 2011-2015: Banda "Dragonfly", que se cree que es un grupo de patrocinio estatal que se focalizan en industrias estratégicas: empresas de suministro energético, principales empresas generadoras de energía, operadoras de oleoductos.2012: Penetración en medios de comunicación, New York Times, Wall Street Journal y Washington Post.
- 2012: Shamoon, ciberataque de borrado masivo contra SaudiAramco.
- 2013:

-"TeamSpy" (operación de ciberespionaje de una década de duración a través de Teamviewer, objetivos de perfil alto en países de Europa oriental y la comunidad de estados independientes (CEI).

-"MiniDuke" (vulnerabilidades avanzadas en Adobe Reader para recoger inteligencia geopolítica de objetivos de perfil alto, gobiernos e instituciones mundiales).

-"Red October" (Red de ciberespionaje avanzado con objetivos de agencias diplomáticas y gubernamentales).

-"NetTraveler" (red internacional principalmente china de ciberespionaje, cuyos objetivos son instituciones gubernamentales, embajadas, centros de investigación científica, complejos militares y empresas petrolíferas).

-"Icefog" (campaña de ciberespionaje centrada en ataques en la cadena de suministro para empresas occidentales a través de objetivos en Corea del Sur y Japón).

-"Kimsuky" (campaña de ciberespionaje con el objetivo de think-tanks surcoreanos). Junio 2013: Revelaciones de Edward Snowden sobre el programa de vigilancia global llevado a cabo por la NSA.

- 2014:

-"CosmicDuke" (dirigido a organizaciones diplomáticas, sector energético, operadoras de telecomunicaciones, contratistas militares e individuos implicados en el tráfico o venta de sustancias ilegales o controladas).

-"EpicTurla" (operación de ciberespionaje masivo apuntando a instituciones gubernamentales, embajadas,

ejército, educación, investigación y compañías farmacéuticas en 45 países).

-"TheMask" (atacantes hispanohablantes dirigidos hacia instituciones gubernamentales, empresas de energía, petróleo y gas y otras víctimas de perfil alto con instrumentos complejos)

-"Crouching Yeti" (campaña continua de espionaje con más de 2.800 objetivos de gran valor en todo el mundo)

-"Energetic Bear" (infiltrado en los ordenadores y sistemas de más de 1.000 organizaciones en el sector global de energía, acceso a datos sensibles y poder de interrupción del abastecimiento energético).

-Hackeo a Sony Pictures Entertainment.

- 2015: Ataques terroristas de Charlie Hebdo seguidos por unos 19.000 ciberataques a infraestructuras tecnológicas francesas llevados a cabo por hackers pro-islamistas. Anonymous lanza una campaña contra Daesh y sitios web yihadistas. También son objetivos, algunas cuentas de redes sociales del Mando Central de Estados Unidos. Intrusión rusa en la Casa Blanca. "APT30", para obtener datos de activos del sudeste asiático para China.

Estos ataques/intrusiones no autorizadas requieren además de una motivación, la selección de un blanco, un objetivo y una serie de técnicas básicas, que pueden aplicadas de manera individual o conjunta y obtener así el resultado buscado. Las más usuales y detectadas al momento podrían ser[109]:

- **VIRUS:** Los Virus Informáticos son esencialmente programas maliciosos, que tratan de infectar a otros archivos de un

109 BELTRÁN, Julián Ignacio. Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. Escuela Técnica Superior de Ingeniería Informática Universitat Politècnica de València . Septiembre 2015.

sistema, y producir con ello alteraciones al funcionamiento del mismo o daños al sistema infectado. Este introduce una secuencia de códigos maliciosos, que normalmente está dirigida a los archivos ejecutables del sistema atacado. A cada ejecución de estos archivos, se produce una propagación del virus, infectando de esta manera nuevos archivos y generando una expansión del mismo.

- **SPAMMING:** consiste en el envío de mensajes no solicitados, generalmente enviados en grandes cantidades por un remitente desconocido.

- **SPOOFING:** este tipo de ataque consiste en la simulación desde un equipo informático de la identidad de otro conectado a la red a fin de conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de seguridad basada en el nombre o la dirección IP del host suplantado. Esta técnica continua siendo un ataque peligroso y factible contra cualquier tipo de organización.

- **KEYLOGGERS:** es el envío o instalación de archivos, programas que registran y graban la pulsación de teclas y clics del ratón; una vez recopilada esta información será utilizada por la persona que lo haya instalado para la consecución de sus objetivos.

- **TROYANOS:** su empleo es muy común y son una clase de virus caracterizado por su capacidad de engaño a través de programas o archivos habituales con el objeto de infectar y causar daño. Este crea una puerta trasera con la que logra el acceso a la administración remota del equipo infectado y a partir de allí el robo de la información confidencial/personal.

- **BOT del IRC (Internet Relay Chat):** son programas empleados para que el sistema sea controlado remotamente sin el conocimiento ni consentimiento del usuario. En webs de

conversación on-line, chats, algunos son utilizados para simular una persona y hacer un uso maligno buscando mantener salas de chat abiertas indefinidamente, y que son utilizadas como canal de comunicación por lo que esa sala de chat nunca es clausurada.

- **ROOTKITS:** herramientas que ocultan un acceso no autorizado a un sistema informático. Se utilizan para esconder procesos y archivos que permiten al intruso el acceso con fines maliciosos; diseñados para ser inadvertidos.

Hasta aquí y con la sola mención de algunas de las herramientas o técnicas de ataque detectadas a la fecha, es lógico pensar que con el avance y la capacidad de desarrollo tecnológico y de software actual existan muchas más que no han sido detectadas aún.

Más del 40% de los programas maliciosos enviados por e-mail tienen como fin el robo de información. Muchos son dirigidos a empresas utilizando a partir del auge del comercio on-line, sus canales y sitios web para atacar y obtener información confidencial de los usuarios[110].

Recapitulando lo expresado hasta ahora, podemos asegurar que la ciberguerra evoluciona de manera permanente y rápida con una dinámica propia que construye su complejidad, sumando una sociedad directamente ligada al proceso de globalización tecnológica, transversal a todas las áreas y aspectos del ser humano como individuo y que en su conjunto forma el conglomerado de un estado-nación.

De esta manera, las operaciones en el ciberespacio no solamente son empleadas con objetivos generales y específicos positivos, también gracias a la amplitud del escenario, son capaces de

110 Redacción Silicon.El 40% de los programas maliciosos busca robar información personal. Agosto 2013. Disponible en: https://www.silicon.es/el-40-de-los-programas-maliciosos-busca-robar-informacion-personal-2247075.

afectar las redes y/o sistemas críticos o sensibles de los estados a nivel nacional, interfiriendo de manera directa o indirectamente en la vida cotidiana de la sociedad y sus instituciones, provocando daños significativos en sectores económicos, financieros, relacionados con la Seguridad y Defensa de un país, con lógicas y atendibles repercusiones nacionales e internacionales.

Si bien un ciberataque siempre aprovechará las vulnerabilidades de los sistemas informáticos del oponente, la naturaleza del conflicto condicionará la selección de los blancos u objetivos, entre aquellos vulnerables. Habrá coherencia entre medios y fines, así como entre causa y efectos, relaciones que son siempre difíciles de desentrañar tanto para los actores recíprocamente involucrados como para terceros.

La determinación de proveniencia de un ataque cibernético, es decir su detección, identificación, localización y seguimiento se constituye en un objetivo prioritario.

Finalmente, puede sostenerse que el ciberespacio y la ciberguerra, son una dimensión y ambiente que los Estados y la comunidad internacional a través de sus áreas vinculadas a la defensa y seguridad deben tener en cuenta, sobre todo con la importancia en la gestión de la información y capacidad para gestionarla, se han convertido en factores críticos para la articulación y progreso de las sociedades.

CAPÍTULO 4

4.1 Ciberdefensa, Ciberguerra y los Conflictos Modernos.

Internet se ha transformado en una revolución en todos los aspectos de la vida humana, es el medio de comunicación más empleado en la actualidad y en los últimos años ha sido evidente que ciertos países se encuentran en la vanguardia por su dominio y buscan su control logrando con ello poder acceder mediante la desestabilización de los sistemas informáticos en conseguir alcanzar sus intereses y objetivos.

La ciencia y la tecnología son las fuerzas productivas de la sociedad moderna, y el producido de estas constituye uno de los aspectos creativos del hombre, que por el contrario en vez de adaptarse al medio que lo contiene, es su esencia, funciona como un sistema que ejerce una fuerza transformadora sobre el escenario donde se desarrolla, para hacerlo adaptable a sus necesidades[111].

El uso cotidiano y sistemático del conocimiento científico y los nuevos materiales desarrollados en el sector tecnológico se han impuesto como condición para el desarrollo social; la tendencia indica con firmeza que esto es lo que caracteriza a la sociedad moderna y la impulsa con mayor énfasis.

A partir del proceso de globalización, para un estado el dominio del factor de poder científico/tecnológico[112], es el que le permitirá desarrollarse firmemente y poder cumplir con el objetivo de presentar a su nación un escenario fértil para el dar más oportunidades y capacidades para que la ciudadanía

111 CANEDO ANDALIA, Rubén. Ciencia y tecnología en la sociedad. Perspectiva histórico-conceptual. 2001. Disponible en: http://bvs.sld.cu/revistas/aci/vol9_1_01/aci051001.htm.

112 Jhoner Perdomo , Luis D. Álvarez, Sary Levy-Carciente, Mauricio Phélan C.La innovación científica y tecnológica como factor de progreso e integración. Febrero 2016. Disponible en: https://es.ictsd.org/bridges-news/puentes/news/la-innovación-cient%C3%ADfica-y-tecnológica-como-factor-de-progreso-e

promueva resultados que permitan el desarrollo humano. En este sentido, los países se integran en bloques para fortalecer sus políticas, dar respuestas a las demandas sociales y mejorar la calidad de vida de sus habitantes.

Hoy la sociedad ha consolidado una posición en el ciberespacio, usando la totalidad del espectro y concibiendo un escenario donde las posibilidades pueden llegar a ser infinitas y solamente están sujetas a la capacidad de imaginación y creación del ser humano.

La Ciberdefensa y Ciberguerra plantean una nueva situación estratégica, que impone el desarrollo de nuevas perspectivas y aproximaciones a la resolución de conflictos.

Ambos conceptos deben tomarse como una dimensión y manera de afrontar un conflicto o también de generarlo en pos de un objetivo ulterior y es relevante para la seguridad y defensa de los Estados, dada sus condiciones para afectar el desarrollo e inclusive generar crisis entre los mismos.

Las causas que dan contexto a un conflicto o crisis son variadas al igual que las dimensiones que estos pueden abarcar; sin embargo el resultado final no deja de ser otra cosa que la combinación de factores relacionados con[113]:

- **Factores político-institucionales:** Instituciones estatales débiles, exclusión política y debilitamiento de las clases sociales de elite, ruptura del contrato social, falta de identidad política y corrupción.
- **Factores socio-económicos:** ausencia o debilitamiento de la cohesión social, pobreza, exclusión y marginalización.

113 ADINOYI, Julius A. Causes Of International Conflicts And Insecurities: The Viability And Impact Of Conflict Management Mechanism In International Relations. Disponible en: http://www.academia.edu/10036496/CAUSES_OF_INTERNATIONAL_CONFLICTS_AND_INSECURITIES_THE_VIABILITY_AND_IMPACT_OF_CONFLICT_MANAGEMENT_MECHANISM_IN_INTERNATIONAL_RELATIONS

- **Factores del medio ambiente y recursos naturales:** escasez de recursos naturales nacionales, normalmente relacionados con el crecimiento descontrolado de la población y que a su vez generan impacto en el medio ambiente, explotación desmedida.

Cabe aclarar que si bien estos son factores tomados de acuerdo a la referencia señalada, no hay que dejar de lado aquellos que surgen históricamente en determinadas regiones debido a los aspectos religiosos o étnicos en relación al control de un territorio al que se consideran tienen derecho exclusivo.

Asimismo e independientemente que en los últimos años se ha dado como común el proceso de instrumentalización de la algunas independencias, generándose con ello la proliferación estatal y una fragmentación global con posibles consecuencias sobre la seguridad regional y/o internacional.

A continuación se describe una muestra de algunos conflictos Post-Guerra Fría en los que se han empleado capacidades de ciberguerra. Esta descripción permite observar el tipo de operaciones ejecutadas y sus efectos, teniendo en cuenta que las operaciones de ciberguerra han sufrido una evolución en función de los años donde se ha desarrollado y respecto de la cantidad e intensidad, siendo así sus etapas identificadas en[114]:

- **Temprana:** 1994-2006

  Esta etapa fue durante la que se llevaron a cabo una serie de movilizaciones políticas utilizando como medio el mundo digital y llevando a cabo un hacking de los sistemas de información de fuerzas militares. Los casos fueron: Chechenia, Kosovo, Israel y Palestina, teniendo entre ellos la característica común que todos los ciberataques fueron

114 SALAZAR, Juan Pablo. La Migración De La Guerra Al Espacio Digital. 2016. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20%20La%20migración%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf

desplegados en el marco de conflictos armados internacionales y que tuvieron como objetivo determinado dejar sin actividad sitios web y la conectividad de aquellos actores estatales con intereses contrapuestos con los del agresor.

- **Intermedia:** 2007-2009

  Durante esta etapa fue el inicio de las ciberoperaciones y primeras manifestaciones de ciberconflictos. Los ataques fueron muestra de un período para la prueba de ciberarmas y con objetivos claros sobre la seguridad y defensa de otros estados. Los afectados y atacantes fueron: China, Estados Unidos, Israel, Reino Unido, y Rusia.

- **Proliferación:** 2010-2016

  Esta etapa inicia en el 2010 con la aparición de nuevos actores en la dimensión cibernética y comenzó a introducirse nuevas ciberarmas. También, además de una mayor cantidad de ciberataques, los Estados comenzaron a trabajar en conjunto a los fines de preparara estructuras de Ciberdefensa y acuerdos para evitar los incidentes cibernéticos.

Habiéndose determinado e identificado etapas en la evolución y desarrollo de la ciberguerra es que se hace necesario adentrarse en algunos de los ataques y conflictos más significativos.

- **TEMPRANA**

  - CHECHENIA[115]

  Durante el conflicto armado de los noventas en Chechenia, representantes pro-Chechenos y pro-Rusos canalizaron sus confrontaciones a internet, principalmente difundiendo

115 KENNETH, Geers. Cyberspace and the Changing Nature of Warfare. The Nato Cooperative Ciber Defense Center of Excellence. Tallin, Estonia. 2008. Disponible en:https://ccdcoe.org/library/publications/cyberspace-and-the-changing-nature-of-warfare/

propaganda y utilizando la plataforma para la difusión de mensajes de relacionamiento público con la causa. En los mismos se publicaban imágenes, videos e información sobre los incidentes ocurridos, ataques contra caravanas militares rusas.

Aquí en este caso particular puede observarse como este tipo de accionar impacta directamente sobre la mente de las poblaciones; elemento central de las Guerras de Cuarta Generación

Este accionar por parte de los chechenos hizo que el gobierno ruso vislumbrara la necesidad de optimizar sus tácticas en el ciberespacio, aplicando ciberoperaciones que impidieran que contenido pro-checheno estuviera accesible en la web; esto fue un adelanto en términos de la introducción de medidas militares centralizadas de censura.

- **Kosovo**[116]

Hackers pro-Serbios durante 1999 se encargaron de llevar adelante una ofensiva por medio del empleo de ciberataques. Los mismos estaban dirigidos a buscar el desequilibrio de la infraestructura del internet y la red informática en general perteneciente a la Organización del Atlántico Norte (OTAN), los Estados Unidos y el Reino Unido.

La táctica empleada para perpetrar estos ataques fue la inyección de virus que eran enviados por medio de e-mail, llegando a registrarse en un día más de dos mil mails recibidos en las cuentas asociadas a las redes informáticas mencionadas anteriormente.

116 FUENTES, Julio. Guerra Informática en Serbia. 16 abril 1999. Disponible en: http://www.elmundo.es/navegante/99/abril/16/hackers.html

Asimismo y de manera general se llevaron a cabo aleatoriamente la denegación de servicio, ocasionando con ello la caída del sistema informático y redes que se empleaban para la coordinación de las operaciones y tráfico de información sensible.

Estos ataques ocasionaron que el sitio web de la OTAN estuviera sin servicio por días y que los servidores del correo electrónico se vieran colapsados por la inundación de mensajes electrónicos, dificultando con ello el normal curso de las acciones en el escenario de conflicto y las comunicaciones entre los actores involucrados.

- **ETAPA INTERMEDIA**

- Estonia[117]

Tan simple, pero a la vez complejo porque resultaba ser un interés para el gobierno ruso, una estatua con la figura de un soldado ruso instalada en Tallinn, Estonia y su reubicación, generó una rivalidad nacionalista entre esos dos estados, debido a que para muchos, es monumento simbolizaba la opresión soviética, mientras que para los rusos simbolizaba la victoria de la Unión Soviética sobre el nazismo.

Este accionar dio pie a fuertes protestas en dicha ciudad y también en la sede de la Embajada de Estonia en Moscú, y el escenario de conflicto fue trasladado de manera inmediata al mundo digital por medio de ataques que hackers.

Entre el 29 de abril y el 11 de mayo de dos mil siete, diversos sistemas de Estonia fueron afectados masivamente por un ataque de denegación de servicio. Las redes de Estonia fueron inundadas por

117 Richard A. Clarke, Robert K. Knake Guerra en la red: Los nuevos campos de batalla. Grupo Planeta Espana. Febrero 2011.

datos procedentes de Rusia, probablemente no por el Estado, sino por las organizaciones patrióticas.

La agresión provocó que Estonia pidiera la intervención de la OTAN y, en agosto de 2008, se puso en marcha el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD) de la OTAN en Tallinn, su capital.

Estos ciberataques hicieron que durante tres semanas, organizaciones gubernamentales e instituciones perdieran el control de sitios web y redes, caso entre otros del Despacho Presidencial, Parlamento, Policía, bancos y medios de comunicación en general.

La denegación de servicios ocasionó que unos cincuenta y ocho sitios web tuvieran dificultades o quedara anulado el acceso a los mismos; un caso ejemplar fue el Hansapank, el banco comercial más grande de estonia que solamente estuvo disponible por pocas horas.

Asimismo el SEB EestiÜhispank, otro de los más importantes bancos comerciales, estuvo fuera de línea algunas horas originando con ello todo tipo de inconvenientes en las transacciones financieras.

Se estimó que cerca de un millón de computadoras fueran empleadas para atacar estos sitios web y como resultado Estonia perdió 3 millones de euros lo que equivale aproximadamente a 4 millones de dólares y cifra que representaba en ese entonces el 1.85% de su PBI.

- **Ataques a Estados Unidos por China**[118]

Durante el año 2007 se constituyó un ciberataque contra el Departamento de Defensa de los Estados Unidos.

118 Michael RILEY/Ben ELGIN. Ciberespías chinos logran sortear a EE UU y robar secretos militares vitales. Washington. 04 MAY 2013.Disponible en:https://elpais.com/internacional/2013/05/04/actualidad/1367700469_570919.html

Militares chinos, perteneciente al Ejercito Popular de Liberación lograron ingresar en la red informática del Pentágono Americano, viéndose su personal obligado a desconectar parte del sistema informático de la oficina del Secretario de Defensa.

Durante el ataque se descargaron cantidades de información, que si bien no era sensible, obligo a que los responsables del sistema informático analizaran que información era enviada por mail o guardada en los diferentes nodos de acceso a la red.

No obstante a partir de ese año, los hackers chinos se introdujeron en las bases de datos de casi todos los grandes contratistas de defensa de Estados Unidos y lograron hacerse con varios de los secretos tecnológicos más protegidos del país y la valoración de daños de los incidentes sigue siendo información reservada.

Algunos de estos ataques han llegado a hacerse públicos, como el robo que sufrió Lockheed Martin Corp. de tecnología relacionada con el F-35, el avión de combate más avanzado de los Estados Unidos.

Asimismo entre los datos que han sido robados en general de tecnología militar muy confidencial, se estima que su volumen es equivalente a 1,3 millones de páginas de documentos o más de 3,3 millones de páginas de tablas en Microsoft Excel.

Si bien al día de hoy no se cuentan con pruebas fehacientes respecto de las reales competencias para irrumpir en sistemas críticos y producir desequilibrio de las operaciones por parte del Gobierno Chino, si se tiene noción que articulan constantemente métodos para infiltrarse en las redes y romper las barreras de defensa de aquellos gobiernos o sectores de interés.

- **Ataques a Siria Suprimen Defensa Aire - Tierra**[119]

Siria e Israel han estado en conflicto desde 1967. A partir de ello sucesivos ataques se han desencadenado, pero durante septiembre 2007 un ataque de aviones de combate israelíes bombardearon instalaciones militares estratégicas sirias.

Los motivos del ataque siempre estuvieron en el velo, no obstante aparentemente buscaban un objetivo relacionado con el desarrollo de armas nucleares, fruto de la alianza establecida entre Siria y Korea del Norte.

Las defensas antiaéreas sirias nunca detectaron la intrusión de las aeronaves y de acuerdo a los especialistas esto fue gracias al empleo de un sistema de ataque informático desde el aire, "Suter", por medio del cual se hackean las defensas del enemigo.

Esta tecnología permite al usuario invadir la red de comunicación es y ver lo que el enemigo ve en sus sensores e inclusive tener acceso como administrador a su sistema y manipularlo a posiciones donde no puedan detectar la aproximación del enemigo.

Asimismo por medio de este programa se pueden insertar blancos falsos, generando con ello confusión y distracciones mientras la operación real se lleva a cabo.

- **Ataques a Georgia por Rusia**[120]

Durante el mes de agosto del 2008 el estado de Georgia fue blanco de ciberataques que afectaron sus sistemas informáticos, en su mayoría pertenecientes al gobierno, medios de comunicación y logística. La denegación de

119 LEYDEN John. Israel suspected of hacking Syrian air defences. 04 octubre 2007. Disponible en: https://www.theregister.co.uk/2007/10/04/radar_hack_raid/

120 SMITH, David J. Russian Cyber Strategy and the War Against Georgia. 17 enero 2014. Disponible en: http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia

servicio (DDoS) fue por excelencia el método seleccionado.

Rusia atacó poniendo en práctica por primera vez su doctrina de ciberguerra y aplicando las mismas técnicas y sistemas informáticos empleados cuando atacara a Estonia.

Todo el evento fue registrado tiempo antes que Rusia comenzara su avanzada para la invasión por tierra, impidiendo con ello que la población de Georgia pudiera acceder a los mensajes que el gobierno intentaba enviar como alerta o las acciones de coordinación que necesitaban hacerse; aquí se muestra claramente lo anteriormente mencionado, que un ataque inicial de un conflicto puede darse o generarse empleando como escenario el ciberespacio.

- **Ataques a Kirguistán**[121]

Ataques similares a los que hicieron impacto en Georgia durante el 2008 fueron detectados de manera masiva en Kirguistan, los cuales afectaron y sacaron de línea a través de la denegación de servicio a los dos proveedores Internet con los que contaban la víctima.

Los objetivos de estos ataques fueron de acuerdo a las opiniones de los especialistas una manera de silenciar la retorica de una oposición cuyo principal blanco era remover al gobierno oficial y generar una fisura en las políticas administrativas.

Por otra parte algunos sostuvieron que estos ataques fueron parte de una campaña rusa para presionar al gobierno y que este procediera al cierra de una base aérea clave para Estados Unidos, la cual resultaba ser una

121 Counter Threat Unit Research Team. Kyrgyzstan Under DdoS Attack From Russia. 27 enero 2009. Disponible en: https://www.secureworks.com/blog/research-20957.

fuente importante de despliegue en la guerra contra el Islam en Afganistán.

La denegación de servicio por parte de Rusia constituyó la manera ideal para dificultar al gobierno opositor de hacer publicidad de sus alternativas y obtener apoyo, ocasionando por otro lado una oposición diplomática de parte de los Estados Unidos y sus aliados.

- **PROLIFERACION**

  - **Irán**[122]

Stuxnet[123] era el nombre del gusano (malware) que materializó el ciberataque a los sistemas de supervisión, control y adquisición de datos pertenecientes a las centrifugadoras nucleares en la instalación de Natanz, Irán. Fue el primer virus informático específicamente diseñado para causar daño físicamente y no de manera virtual a como se esta acostumbrado.

Cabe señalar que este tiene la forma de programa con la capacidad de capaz de propagarse activamente a otros sistemas, explotando sus vulnerabilidades, específicamente del sistema Windows.

Según los especialistas, Stuxnet era dirigido con un objetivo particular, sabotear un programa específico de la marca Siemens utilizado en el control de oleoductos, plataformas petroleras, centrales eléctricas y otras instalaciones industriales reprogramar las centrifugadoras para hacerlas fallar sin que se detectara.

122 ESPINOSA, Angeles. Irán sufre un ataque informático contra sus instalaciones nucleares. Septiembre 2010. Disponible en:https://elpais.com/diario/2010/09/28/internacional/1285624808_850215.html

123 Top Ten Most-Destructive Computer Viruses. Available. 28 julio 2012.Disponible en: http://www.smithsonianmag.com/science-nature/Top-Ten-Most- Destructive-Computer-Viruses.html

La operación inició en el año 2005 y llevada adelante principalmente por Agencia de Seguridad Nacional conjuntamente con la Central de Inteligencia de los Estados Unidos.

Stuxnet fue introducido por un doble agente, quien mediante una unidad USB infectada alteró el funcionamiento de los controladores lógicos de las máquinas centrifugadoras de uranio marca SIEMENS.

Su forma de operar consistía en permanecer inactivo eludiendo los sistemas de monitoreo durante períodos reglados y que alcanzaban hasta un mes, para imprevistamente y durante breves minutos gracias a la información que había obtenido el programa creaba un código que permitía acelerar los rotores de las centrifugas hasta el límite de la destrucción o desacelerarlo hasta llegar prácticamente a la inactividad ocasionando su destrucción.[124]

El ataque destruyó casi mil de un total de seis mil centrifugadoras, afectando las posibilidades de Irán de continuar con su avance y progreso hacia la construcción de una bomba atómica y por ende sus posibilidades de fortalecer su presencia y poder militar en la región[125].

A pesar que este suceso no se enmarca en una guerra formal entre dos Estados, si se puede sostener que se da a partir de las relaciones de poder y fuerza en el marco de un conflicto entre dos o más estados, como lo es el que sostiene Irán, en relación a su programa

124 Top Ten Most-Destructive Computer Viruses. Available. 28 julio 2012.Disponible en: http://www.smithsonianmag.com/science-nature/Top-Ten-Most- Destructive-Computer-Viruses.html

125 Anónimo. El virus que tomó control de mil máquinas y les ordenó autodestruirse.11 octubre 2015. Disponible en:https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

tecnológico nuclear, con Naciones Unidas y Estados Unidos e Israel.

Si bien se podría continuar desarrollando una extensa lista de ataques cibernéticos conocidos, es evidente que se esta presente a solamente una parte de lo que ocurre, dado que podría sostenerse que por cuestiones de seguridad nacional por parte de los distintos estados, muchos de estos ataques no se dan a conocer, pero no dejan de impactar en las relaciones entre los integrantes de la comunidad internacional.

Desde luego, Estados Unidos y sus aliados tienen la capacidad, los recursos y la motivación para lanzar con mas virulencia ataques cibernéticos, y de acuerdo a la opinión de los expertos existe una "guerra fría cibernética"[126] entre los Estados Unidos y China donde redes civiles y militares han sido objetivos principales para los chinos, como así también las empresas fabricantes de armas.

Washington y Beijing pese a que siempre han estado tratando de mantener una estabilidad y promover cambios positivos en sus relaciones bilaterales, durante los últimos años no pudieron escapar a la tirantez de sus relaciones; tirantez que tiene asistencia a partir de las constantes discrepancias en los fines e intereses de cada uno de ellos.

Estas discrepancias suscitaron se materializaran sucesivos ataques e intromisiones en los distintos sistemas informáticos de Estados Unidos, donde se han llegado a registrar más de 117.000 ataques a sus equipos

126 Anónimo. La guerra fria cibernetica. 25 febrero 2013. Disponible en: http://www.iriartelaw.com/la-guerra-fria-cibernetica.

y sistemas, buscando con ello hacer llegar un mensaje de descontento a su competidor[127].

A pesar que ambos países deben cooperar y mantener una agenda compartida respecto de los asuntos internacionales y sobre todo en aquellos donde mas influyen sus acciones, no hay duda que las tensiones cibernéticas están creciendo, y lo hacen al mismo ritmo que las tensiones en los mares cercanos a China[128].

Puede observarse que en el ciberespacio la velocidad y el sigilo con el que una acción de ciberguerra puede llevarse adelante, resulta ser un factor predominante en cuanto al impacto a lograr y respecto del resultado buscado, tanto que desequilibra notoriamente en cantidad y eficiencia los que pudieran obtenerse en el tradicional espacio físico de aire mar y tierra.

Estas cualidades son determinantes al momento de diseñar e implementar barreras defensivas, dado que el poco además de la capacidad de desarticular a un actor dado, también puede lograr romper con las relaciones de fuerza y poder de un que este pueda sostener con otros actores.

Ante la creciente dinámica del ciberespacio y las acciones de ciberguerra, las capacidades y vulnerabilidades de los integrantes de la comunidad internacional, y de acuerdo a los casos hasta aquí aportados, deben ser tomadas como elementos cruciales en el desarrollo de los niveles de protección adecuados a fin de poder explotar y auto protegerse.

Desde la globalización el alcance y la profundidad de esta dimensión, el ciberespacio, no ha hecho otra cosa

127 Idem.

128 STEVENS, Tim, BETZ, David.Cyberspace and The State. Toward a Strategy for Cyber-Power. 2013. Disponible en: https://assemblingsecurity.files.wordpress.com/2013/05/betz_stevens_cyberspace-and-the-state-2011.pdf

que ampliarse y de manera pareja también ha hecho lo propio la ciberguerra, transformándose ésta en un multiplicador, que alienta a líderes políticos y militares con visión estratégica a considerar las ciberarmas como elementos validos para desarticular al enemigo.

En las distintas fases y casos desarrollados en este capítulo, se puede observar que si bien existe cierta diversidad en las operaciones involucradas en un ataque cibernético, como ser las ligadas a la región donde se desarrollan, características y nivel tecnológico de los actores involucrados y el fin ulterior, casi en su totalidad los ataques conciben medios y métodos técnicos similares.

Del análisis de los casos planteados, es posible concebir que las capacidades de ciberguerra con que cuente un Estado, harán que este aumente o disminuya el status quo de su potencial bélico respecto de otro estado y por supuesto respecto de sus capacidades convencionales, siendo así que lo virtual pasa a tener durante la estada de crisis y escalada del conflicto mayor preponderancia que las capacidades reales.

Estos casos también han permitido materializar la forma en como las operaciones de ciberguerra se han hecho presente de acuerdo al escenario y contexto de cada conflicto e identificar la forma en como puede afectar la seguridad y la defensa, como así también el poder nacional de un Estado.

Se hace imperioso entonces, que actores estatales y organismos responsables de la seguridad y defensa, deban asumir que la ciberguerra está en una constante evolución, y por ende que los esfuerzos de vigilancia y reconocimiento del ciberespacio sean

constantes, sobre todo en atención a que cada vez un conflicto entre estados en esta dimensión es más significativo.

CAPÍTULO 5

Conclusiones.

Los resultados de este trabajo de investigación y su interpretación, son un aporte que permite a través del estudio y una perspectiva actual del alto grado de interconexión presente en la Comunidad Internacional, comprender como ha evolucionado la naturaleza, el desarrollo y alcance de las crisis y conflictos modernos entre los estados.

El conflicto o la guerra en sentido amplio como se trató el tema a lo largo de este trabajo, ha ido mutando a lo largo del tiempo. Se hizo un rápido recorrido por las distintas generaciones de guerra, para detenerse en la IV Generación, hoy en curso y presente globalmente. Conflicto multidimensional que contempla la presencia de actores estatales como paraestatales, medios y herramientas modernas desde lo tecnológico pero también elementos tradicionales y hasta antiguos.

En la actualidad, la principal característica quizás sea que el resultado de las acciones no se mida en avances en el terreno, sino en el control de la mente de los pobladores, el dominio de la voluntad de los mismos y el control de sus pensamientos; por ello es que los aspectos vinculados al control del ciberespacio cobran un peso relevante a la hora de abordar un conflicto de IV Generación.

Los estados con ambición de mantener o acrecentar su estatura estratégica, son conscientes del alcance e importancia del ciberespacio como escenario del conflicto moderno y como antes, evaluaban el tamaño de sus ejércitos, sus flotas y sus escuadrones aéreos, luego su red y despliegue satelital y de armas de destrucción masiva, hoy miden sus capacidades cibernéticas, procurando mantener a las mismas en el nivel que su apetencia de poder les obligue.

De esta manera actores como Estados Unidos, China, naciones de la Unión Europea y Rusia entienden que el liderazgo positivo en materia del uso del ciberespacio, marca un nuevo estrato para alcanzar la jerarquía como potencia y autoridad mundial.

El ciberespacio, por sus características y siempre novedosas implicaciones, debe ser tenido en cuenta no solamente a la hora de evaluar posibles conflictos entre actores estatales, sino también por los alcances que conlleva el accionar de actores internos que interactúan en la cotidianeidad social. Allí el estado y sus habitantes pueden observar claramente que los límites entre seguridad y defensa son notoriamente indefinidos y se requiere ser más hábil al momento de operar y desarticular las maniobras de ataques en este nuevo escenario.

Las actividades que un estado ejerce en este terreno virtual son variadas y su potencialidad orientada siempre será hacia el servicio de sus intereses nacionales, pudiendo tomarse ello como una rama del poder blando, que un actor estatal puede aplicar a fin de influir en la esfera internacional de manera convincente, persuasiva y hasta disuasiva.

Por otra parte se pudo alcanzar un nivel de comprensión sobre la Ciberguerra, especialmente a partir de su perspectiva como práctica moderna de las operaciones, que permitiría comprender y aceptar en virtud de los aportes de casos y ataques presentados, que lentamente se está constituyendo como instrumento predominante para disparar y desarrollar crisis y conflictos, actuales y futuros entre los diferentes actores tanto estatales como privados.

Así como en el pasado un actor pensaba en un ataque sorpresa para anular las capacidades centrales de su oponente, hoy ese primer impacto tendiente a debilitar la capacidad de combate del oponente es altamente probable que se desarrolle en el ciberespacio.

El uso de internet como herramienta generalizada para el manejo y la transferencia de información permite que cada vez sea más común y constante la transgresión de los límites de lo permitido y que cada minuto se sumen nuevos actores al conglomerado informático presente entre estados, ampliando con ello la cantidad y tipos de ataques que se pueden llevar a cabo.

Los ciberatacantes no entienden de fronteras ni legislaciones y con su accionar individual o coordinado afectan la totalidad de los ámbitos políticos internacionales y por consiguiente sus relaciones internacionales.

La inexistencia de una legislación a nivel internacional que contemple al ciberespacio con su conglomerado de aspectos, que van desde los delitos informáticos hasta un ciberataque entre estados dificulta el tendido de lazos de cooperación internacional.

Estados como Rusia, China y Estados Unidos, potencias a nivel mundial, han logrado comprender rápidamente la importancia que tiene poder dominar y controlar el ciberespacio, haciendo de ese control una herramienta de sus relaciones internacionales para coaccionar o disuadir a sus oponentes de llevar adelante ciertas acciones en ese mismo o en diferente ámbito. Por ello se han encargado de incluir dentro de sus estrategias para la política exterior, apartados explicando su postura respecto al desarrollo de capacidades que permitan afrontar los desafíos del ciberespacio, informatizando sus ejércitos y creando comandos para la defensa y seguridad nacional.

Los casos de ataques enunciados muestran un ciberespacio activo y militarizado, donde el control de la información busca ser preciso y totalmente restrictivo a filtraciones de información sensibles y confidenciales para la seguridad y defensa de los intereses del estado; la presencia actual del gobierno en el ciberespacio de manera activa, hace que la ciberguerra se pueda

tomar como una herramienta más de las relaciones internacionales.

Asimismo se pudo observar que las operaciones de ciberguerra dependiendo de las capacidades que hayan desarrollado los actores, son empleadas con mayor o menor intensidad en una situación de crisis o conflictos entre partes, afectándole de distintas maneras los intereses de un Estado al mismo tiempo de alcanzar objetivos estratégicos y llegando a dificultar o impedir el sostenimiento bélico; aseguran una relación costo - beneficio eficiente y con una escala de riesgo menor.

Las distintas operaciones de ciberguerra explicitadas en el trabajo dan cuenta de la enorme variedad de herramientas, amenazas, escenarios de empleo, actores involucrados, motivaciones de origen, magnitud de capacidades, etc.; diversidad de abordajes que obliga a todos aquellos interesados en dotarse de capacidad de ataque o defensa en el ciberespacio a estar siempre a la vanguardia en investigación, desarrollo, vigilancia y sobre todo fomentar en su personal la iniciativa, flexibilidad y pensamiento creativo.

En relación a los efectos de la ciberguerra, fue posible determinar su capacidad de poder afectar en diversas maneras y gracias al empleo de diferentes estrategias y tácticas, el poder nacional, sus instrumentos e instituciones, generando impactos cuyas magnitudes pueden ir desde lo más bajo hasta la desarticulación completa de un estado y con ello generar un daño aun mayor, más trasversal y diseminado.

Las acciones de ciberguerra como pudo verse afectan y tienen el potencial para alterar el normal funcionamiento de los organismos del Estado y sistemas tan sensibles para la sociedad como el sistema financiero, logístico y sus comunicaciones; atentan contra las capacidades de sostenimiento del esfuerzo de guerra propiciando una sensación de

vulnerabilidad ante amenazas desconocidas, complejas de identificar y de un alcance global.

El trabajo de investigación también permitió determinar que las capacidades de ciberguerra en coordinación con las operaciones convencionales que tenga un Estado, permiten desequilibrar las relaciones de poder que existan entre dos o más estados, favoreciendo con ello la consecución de los intereses y objetivos políticos de un determinado conflicto. Es decir, el desafío del futuro no es sólo dotarse de capacidades de ciberguerra sino articular y coordinar las mismas con las otras capacidades del estado, defensivas, ofensivas, militares, policiales, económicas y políticas.

La posibilidad de un conflicto es permanente y que el mismo se desencadene en el ciberespacio casi una certeza. Por ello, los Estados y organismos responsables de su seguridad y defensa deben asumir que esta dimensión está en constante evolución y que los esfuerzos deben asegurar la protección de los sistemas, junto a garantizar la libertad de acción.

Es menester entonces que los estados que busquen libertad de acción para su desarrollo integral necesariamente deban mantener una vigilancia permanente del ciberespacio, dotándose de instrumentos de alerta temprana flexibles y sólidos; la vinculación entre inteligencia y ciberguerra es más profunda que lo que se podría pensar en un principio.

El ciberespacio es un escenario tan crítico como la tierra, el mar, el aire y el espacio, de no controlarse de manera adecuada una nación puede ver amenazada su libertad de acción y seguridad.

A partir del uso generalizado de este escenario, la Estrategia de Seguridad y defensa de un estado cambiará su paradigma y deberá incluir soluciones y aproximaciones a las problemáticas, gestión de crisis y resolución de conflictos.

Es destacable que tanto la localización, como obtención, clasificación y capacidad para su gestión son y serán factores cuya relevancia y dominio es cada vez más importante para la articulación y progreso de la sociedad y preservación de la soberanía, defensa y seguridad de un Estado.

Es por ello, que se considera que pese a la resistencia que pudiera surgir a tomar estos temas como parte de una agenda internacional, los Estados indefectiblemente deben comenzar a estructurar capacidades y competencias para la ciberguerra a fin de, afrontar los desafíos de constituir redes de defensa integradas, convencionales, coherentes y coordinadas con el potencial de contribuir de manera relevante en el desarrollo y consecución de una crisis o conflicto.

La ciberseguridad es un desafío que cada vez cuenta con mayor presencia en cuestiones de inteligencia, como también en relación a las políticas de seguridad y defensa de todos los países; sobre todo con el creciente nivel de informatización que se ha alcanzado desde el advenimiento del Internet.

Se ha podido observar que la ciberguerra es un elemento vertebral para la seguridad y defensa del estado, que debe afrontarse como un asunto de interés nacional alentando la sinergia entre el sector privado y gubernamental, no tan sólo para el desarrollo de capacidades tecnológicas, sino también para definir doctrinas en el empleo de medios y desarrollo de actividades de inteligencia.

Para finalizar, se considera que el auge y preeminencia de la temática planteada en el presente trabajo de investigación hacen que sea necesario continuar profundizando con estudios asociados, sacando conclusiones acerca de cuáles son las capacidades y competencias que un estado debería tener dentro de su Instrumento Militar y de seguridad, determinando un diseño estructural a fin de, poder afrontar amenazas o posibles

hipótesis de conflicto en el marco regional y global dentro del ciberespacio, nuevo ámbito de la defensa.

BIBLIOGRAFÍA

A. Documentos electrónicos.

- Air War College. Battlefield of the future. 21st Century Warfare Issues. Studies in National Security Nro.3 Air University. Maxell Aire Force Base. 1998.
- ANÓNIMO. History & Impact of Hacking: Final Paper. Disponible en: https://courses.cs.washington.edu/courses/csep590a/06au/projects/hacking.pdf. December2006.
- ANÓNIMO. "Tallin Manual on the International Law applicable to Cyber Warfare". International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence. Cambridge University. Gran Bretaña. 2013.
- Anónimo. Oficina de las Naciones Unidad contra la Droga y el Delito. "El uso de internet con fines terroristas".NuevaxYorkx2013.Disponiblexen:https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf
- BELTRÁN, Julián Ignacio. Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad. Escuela Técnica Superior de Ingeniería Informática Universitat Politècnica de València. Septiembre 2015.
- BROWN, Kerry. Contemporary China. 2015.
- CIRLOT, Lourdes. Arte, arquitectura y sociedad digital. Ediciones Universidad Barcelona, 2007.
- CLARKE, Richard A., KNAKE, Robert K. Guerra en la red: Los nuevos campos de batalla. Grupo Planeta España. Febrero 2011.

- CLAUSEWITZ, Karl von. De la Guerra. http://www.biblioteca.org.ar/libros/153741.pdf.
- CLARKE, Richard A., KNAKE Robert K. Guerra en la red: Los nuevos campos de batalla. Grupo Planeta España. Febrero 2011.
- COHEN, Fred. "InfluenceOperations". U.S.A. 2011. Disponible en:http://all.net/journal/deception/CyberWar-InfluenceOperations.pdf.
- Cyberspace & Information Operations Study Center. Disponible en http://www.au.af.mil/infoops/cyberspace.htm#cyber. Fecha de captura, 01 de mayo 2013.
- DALLANEGRA PEDRAZA, Luis, Realismo - Sistémico-Estructural: La Política Exterior como "Construcción" de Poder, (Córdoba, Edición del Autor, 2009) ISBN: 978-987-05-6072-2
- FOJÓN CHAMORRO, Enrique y SANZ VILLALBA, Ángel F. Real Instituto Elcano-España. Ciberseguridad en España: una propuesta para su gestión. Disponible en: www.realinstitutoelcano.org/2010.
- FRIEDMAN, G.Thenext 100 years: A forecast of the 21st Century. Black Inc. 2011.
- HERNÁNDEZ, Campos Augusto. Los Conflictos Internos: Naturaleza y Perspectivas. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6302462.pdf.1999.
- KENNETH, Geers. Cyberspace and the Changing Nature of Warfare.The Nato Cooperative Ciber DefensexCenterxofxExcellence.xTallin,xEstonia.x2008.xDisponiblexen:https://ccdcoe.org/library/publications/cyberspace-and-the-changing-nature-of-warfare/

- KUTT NEBRERA, Alexander. LA IMPORTANCIA DE DOMINAR LOS GLOBAL COMMONS EN EL SIGLO XXI. Disponible en: http://www.ieee.es/Galerias/fichero/docs_marco/2015/DIEEEM29-2015_Global_Commons_XXI_Alexander_Kutt.pdf 12 noviembre de 2015.
- LEJARZA ILLARO, E. Estados Unidos – China: Equilibrio de poder en la nueva Ciberguerra Fría. Instituto Español de Estudios Estratégicos. 2013.
- LEJARZA ILLARO, Eguskiñe. Instituto Español de Estudios Estratégicos. Ciberguerra: Los escenarios de Confrontación.21 de febrero de 2014. http://www.ieee.es.
- LOWENTAL, A. F. The US in the Early 21st Century: Decline orRenewal? Real Instituto Elcano. 2013.
- LUKASIK, S., GOODMAN, S., LONGHURST, D. Protecting Critical Infraestructures Against Cyber-Attack. Oxford University Pressfor The International Institute for Strategic Studies. London, UK. 2003.
- MEDERO, Gema Sánchez. LOS ESTADOS Y LA CIBERGUERRA Profesora de Ciencias Políticas en la Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010.
- MORENO, Andrés Simón TEORÍA DEL CAOS SOCIAL / Cap.: 7 Crisis,conflictos y Caos Social /http://www.oxigeme.com /wpcontent/uploads/2014/10/Teoria_caos_social.pdf.
- Ponemon Institute LLC. (2010). First Annual Cost of CyberCrime Study: Benchmark Study of U.S. Companies. Traverse City, Michigan: Ponemon Institute LLC. Baskerville, R. L., & Portougal, V. 2003.
- Ponemon Institute LLC. "Possibility Theory Framework for Security Evaluation in National Infrastructure

Protection. Journal of Database Management". Baskerville, R. L., & Portougal, V. A. Traverse City, Michigan, USA. 2003.

- Ponemon Institute LLC. "2011 Cost of Data Breach Study: United States". Benchmark Research sponsored by Symantec Independently Conducted by Ponemon Institute LLC. Traverse City, Michigan, USA. 2012.
- PONS Luis. Claves del Siglo XXI. IUN-Dunken, Buenos Aires 2000.
- RUSSINOVICH, Mark. Trojan Horse: The Widespread Use of International Cyber-Espionage as a Weapon RSA Conference 2013. Disponible en:https://www.rsaconference.com/writable/presentations/file_upload/exp-r35.pdf.
- SÁNCHEZ MEDERO, Gema. LOS ESTADOS Y LA CIBERGUERRA . Universidad Complutense de Madrid https://dialnet.unirioja.es/descarga/articulo/3745519.pdf 2010.
- SANCHEZ MEDERO, Gema - La ciberguerra: los casos de Stuxnet y Anonymoushttps://dialnet.unirioja.es/descarga/articulo/4331298.pdf 2012.
- STEVENS, Tim, BETZ, David. Cyberspace and TheState. Toward a Strategy for Cyber-Power. 2013. Disponible en: https://assemblingsecurity.files.wordpress.com/2013/05/betz_stevens_cyberspace-and-the-state-2011.pdf
- SUN TZU. El arte de la Guerra. 2003. http://www.biblioteca.org.ar/libros/656228.pdf.
- The Comprehensive National Cybersecurity Initiative. The Executive Office of the President of UnitedState. http://www.fas.org/irp/eprint/cnci.pdf. 22 junio de 2012.
- TRITZ, Gerald L. "Cyberspace and the Operational Commander". Naval WarCollege. New Port. USA. 2010.

- ZAKARIA, F. The Post American World. Norton. 2001.

B. Artículos de Internet.

- ANÓNIMO. "El Pentágono se asocia con la OTAN para crear un sistema de guerra ciberspacial global". 15 de octubre de 2010. Disponible en http://rebelion.org/noticia.php?id=114884 .
- ANÓNIMO. El virus que tomó control de mil máquinas y les ordenó autodestruirse. 11 octubre 2015. Disponible en: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
- ANÓNIMO. La guerra fría cibernética. 25 febrero 2013. Disponible en: http://www.iriartelaw.com/la-guerra-fria-cibernetica.
- ANÓNIMO. "EEUU e Israel crearon el virus Flame para espiar y atacar instalaciones de Irán". 20 junio .2012Disponibleenhttp://www.elmundo.es/elmundo/2012/06/20/navegante/1340173299.html.
- ANÓNIMO. Que es un ciberataque y tipos. 2018. Disponible en:https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos.
- ANÓNIMO. Remembering Operation Titan Rain. Octubre 2016.Disponible en:https://cyware.com/news/remembering-operation-titan-rain-c54ad3e4.
- ANÓNIMO. Redacción Silicon.El 40% de los programas maliciosos busca robar información personal. Agosto 2013.Disponible en: https://www.silicon.es/el-40-de-los-programas-maliciosos-busca-robar-informacion-personal-2247075.
- ANÓNIMO. Ciberataques interrumpen servicio de Twitter, Spotify y otros sitios web en Estados Unidos. 21 octubre 2016. Disponible en:https://www.laizquierdadiario.com/C

iberataques-interrumpen-servicio-de-Twitter-Spotify-y-otros-sitios-web-en-Estados-Unidos.

- ANÓNIMO. Research and Documentation Centre (WODC), The Netherlands. June 2017. Disponible en: http://cybercrimejournal.com/Madarievol11issue1IJCC2017.pdf.
- ANÓNIMO. CounterThreatUnitResearchTeam.KyrgyzstanUnderDdoSAttackFromRussia. 27 enero 2009.Disponible en: https://www.secureworks.com/blog/research-20957.
- ANÓNIMO. Top Ten Most DestructiveComputerViruses. Available. 28 julio 2012. Disponible en: http://www.smithsonianmag.com/science-nature/Top-Ten-Most-Destructive-Computer-Viruses.html
- ARREOLA, García Adolfo. Ciberseguridad, la nueva cara de la seguridad internacional. Agosto 2015.Disponible en: http://www.academia.edu/36092683/Ciberseguridad_la_nueva_cara_de_la_seguridad_internacional.
- ARTAL, Rosa María. Adoctrinamiento: Nuevas técnicas para viejos fines. 20 marzo 2018.Disponible en: https://www.eldiario.es/zonacritica/Adoctrinamiento-Nuevas-tecnicas-viejos-fines_6_752134800.html.
- BARTOLOMÉ, Mariano Cesar. Un abordaje general a la Teoría de las RelacionesnInternacionales.mDisponiblefen:chttp://repositorio.ub.edu.ar/bitstream/handle/123456789/3505/4104%20%20teoria%20de%20las%20relaciones%20internacionales%20-%20bartolome.pdf?sequence=1&isAllowed=y
- CARLINI, Agnese. ISIS: Una nueva amenaza en la era digital. Instituto Español de Estudios Estratégicos. Diciembre 2015. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO1292015_ISIS_AmenazaEraDigital_AgneseCarlini.pdf.

- CONNELL, Michael and VOGLER, Sarah. Russia's Approach to Cyber Warfare March 2017.
- DERGARABEDIAN, César. "La guerra cibernética "sale" de las computadoras y llega a la economía "real". San Francisco, April 2013. Disponible en Iprofesional.com.
- ESPINOSA, Ángeles. Irán sufre un ataque informático contra sus instalaciones nucleares. Septiembre 2010.Disponible en: https://elpais.com/diario/2010/09/28/internacional/1285624808_850215.html.
- FALLA AROCHE, Stephanie. La historia de Internet. Febrero 2006. Disponible en: http://www.maestrosdelweb.com/editorial/internethis/>
- GOODMAN LUKASIK, S, LONGHURST,D. ProtectingCriticalInfraestructuresAgainstCyberAttack. Oxford UniversityPressforThe International InstituteforStrategicStudies. London, UK. 2003.
- LEYDEN John. Israel suspected of hacking Syrian air defences.04 octubre 2007. Disponible en: https://www.theregister.co.uk/2007/10/04/radar_hack_raid/
- MADARIE, Renushka. Hackers' Motivations: Testing Schwartz's Theory of Motivational Types of Values in a Sample of Hackers.
- MORENO ARRECHE, Andrés. Crisis, Conflicto y Caos Social. 11 junio 2009.Disponible en:https://teodulolopezmelendez.wordpress.com/2009/06/11/crisis-conflictos-y-caos-social/.
- PÉREZ CALDENTEY, Ignacio. El Realismo y el final de la Guerra Fría. Disponiblemen:frevistas.pucp.edu.pe/index.php/agendainternacional/article/viewFile/7164/7364.

- PUGLIESE, Silvia Viviana. Pensando en la crisis y sus efectos en la sociedad actual. 18 abril 2018.Disponible en: https://apop.es/en-la-crisis-y-los-efectos-en-la-sociedad/.
- RAIN, O., LORENTS, P. (2010). Cyberspace: Definitions and Implications., Cooperativa CyberDefence Centre of Excellence, Tallinn, Estonia. 2010.
- REGUERA SANCHEZ, Jesús. Aspectos Legales En El Ciberespacio. La Ciberguerra Y El Derecho Internacional Humanitario. 18 marzo 2015.Disponible en: http://www.seguridadinternacional.es/?q=es/content/aspectos-legales-en-el-ciberespacio-la-ciberguerra-y-el-derecho-internacional-humanitario.
- RILEY, Michael /ELGIN, Ben. Ciberespías chinos logran sortear a EE UU y robar secretos militares vitales. Washington. 04 MAY 2013. Disponible en: https://elpais.com/internacional/2013/05/04/actualidad/1367700469_570919.html
- ROZOFF RAMÍREZ, Gustavo. "Prepara EU ofensiva cibernética con 4 mil nuevos miembros en su Cibercomando". CiberPoliticos.com. 28 de enero de 2013.Disponibleen:http://ciberpoliticos.com/?q=EUofensivacibernetica4milCibercomando.
- SMITH, David J. Russian Cyber Strategy and the WarAgainst Georgia. 17 enero 2014.Disponible en: http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

C. Sitios Web.

- www.internetworldstats.com/stats.htm
- http://www.eumed.net/diccionario/definicion.php?dic=3&def=220 23 julio 2018

- www.symantec.com/business/resources/articles/article.jsp?aid=20090511_symc_malicious_code_activity_spiked_in_2008.

- http://nvd.nist.gov/. National Vulnerability Data Base. U.S. Government.

DANIEL EDUARDO GIUDICI
CAPITÁN DE FRAGATA
M.R.013537-3/D.N.I. 22.489.601