LA RELACIÓN DE LA CIBERGUERRA CON LA GUERRA INTERESTATAL CLÁSICA: ESTUDIO DE CASO ESTONIA, GEORGIA E IRÁN

LAURA MILENA ECHEVERRI MARTÍNEZ

Código 0901591

Director:

Mgr. Andrés Gaitán Rodríguez

Trabajo de Grado para optar por el título de Profesional en Relaciones Internacionales y Estudios Políticos

UNIVERSIDAD MILITAR NUEVA GRANADA

Facultad de Relaciones Internacionales, Estrategia y Seguridad

Programa de Relaciones Internacionales y Estudios Políticos

Julio, 2016

Bogotá D.C

TABLA DE CONTENIDO

Introducción

El proyecto de investigación “La relación de la Ciberguerra con la Guerra Interestatal Clásica: estudio de caso Estonia, Georgia e Irán” busca construir y presentar una perspectiva desde la cual se pueda analizar la ciberguerra como nueva capacidad de los Estados para alcanzar intereses nacionales a través del uso de la fuerza (cibernética e informática), y a su vez, cómo éste fenómeno propio del ciberespacio se encuentra alineado a las premisas clásicas de la guerra interestatal. La ciberguerra se ha convertido en un concepto de gran relevancia debido a los fenómenos que se han desarrollado en la era de la información y los avances científicos frente a las tecnologías de la información y la comunicación; y claramente, su aplicación en los ámbitos militares, así como gubernamentales.

En muchos casos, y producto de los efectos que se han constatado a partir del empleo de la ciberguerra, se ha considerado necesario crear un marco teórico diferente para comprender este nuevo escenario de conflagración entre Estados debido al grado exponencial al que se ha llevado el desarrollo tecnológico y científico en torno a dicho campo. No obstante, al tratarse de igual manera del ejercicio de la guerra, sólo que, a partir de diferentes medios, esta apreciación no es necesariamente correcta; la ciberguerra surge del deseo y naturaleza perenne del hombre por resolver los conflictos políticos a partir de la violencia, y esto, según Boutol, es considerado como guerra, bajo el enfoque de la polemología. En otras palabras, hablar de guerra ciberespacial no implica el surgimiento de una nueva clase de guerra, se trata de la misma práctica hostil, sólo que a partir del uso de tecnologías que implican un cambio cualitativo en la manera de llevar a cabo las operaciones y tácticas dentro de la guerra o en un acto de hostilidad unilateral.

No obstante, también sería desacertado establecer que por el hecho de que la ciberguerra emerge de la guerra clásica esta no demanda formas específicas de exploración y comprensión como fenómeno, así como le necesidad de entenderlo a partir de las disciplinas que pueden explicarlo desde su valor político; es decir, cómo su uso impacta las relaciones políticas internacionales. Es por esto que, el presente proyecto de investigación busca explorar esos paralelos en los cuales se encuentra la comprensión de la ciberguerra, y así, establecer la tesis de que este fenómeno en su naturaleza misma no se desliga de la guerra clásica, pero si debe aceptarse como una forma de confrontación con cualidades y alcances únicos y diferenciales al empleo del armamento convencional y el pie de fuerza.

Por tal motivo, es imperativo para el desarrollo de esta investigación hacer un análisis de las hostilidades, a partir del empleo de la ciberguerra, que se desarrollaron en Estonia en 2007, Georgia durante 2008 y para 2010 en Irán. La teoría clásica de la guerra interestatal, permitiría encontrar las similitudes entre ambos conceptos que pueden dar explicación a los acontecimientos contemporáneos en el ciberespacio para determinar las particularidades de la ciberguerra y qué efectos pueden tener.

El presente trabajo de indagación se diseñó a partir de una estructura argumentativa de capítulos, lo cual por supuesto, busca un construir enfoque lógico de exposición de la temática. En primer lugar, se encuentra el desarrollo del apartado en donde se explora el fenómeno de la guerra clásica, y se lleva a cabo una cronología de la evolución conceptual y teórica como concepción. En el segundo capítulo, y de manera intencionada, se exponen los casos ocurridos en Estonia (2007), en Georgia (2008) e Irán (2010) con el fin de comprender en la práctica cómo se presenta la ciberguerra y la manera en la cual se llevaron a cabo las acciones de agresión a través

del ciberespacio. En tercer lugar, se podrá encontrar una disertación en torno a las particularidades que presenta el ciberespacio como escenario y la ciberguerra como fenómeno y cuál puede ser su alcance en el contexto global actual. En el último capítulo de la monografía, se analizan las características comunes que se presentan entre la guerra convencional y la ciberguerra debido a su semejanza presentada en su naturaleza como práctica humana.

Por supuesto, el lector podrá encontrar al final del documento unas consideraciones a manera de conclusión. De igual manera, y con el ánimo de apoyar futuras investigaciones en esta materia, además de ser requisito metodológico, se presenta el marco de referencia que sustentó la presenta investigación.

Planteamiento del Problema

Actualmente, la ciencia política y la disciplina de las Relaciones Internacionales se encuentran en la búsqueda constante de nuevos conceptos que logren explicar con la mayor claridad el comportamiento de sus actores, los medios que usan y el entorno en el cual actúan al momento de construir y seguir dando vida al sistema internacional y la política exterior. El análisis de las trasformaciones y nuevos paradigmas que se originan el Sistema Internacional permiten, por un lado, la adaptación de antiguos enfoques teóricos, que más que haber sido consignados en los anales de la historia, adquirieron el título de clásicos y hoy siguen siendo pertinentes para explicar fenómenos. Y por otro lado, este tipo de coyunturas o escenarios de cambio también dan paso al surgimiento de teorías novedosas que permitan complementar el proceso a partir del entendimiento de los fenómenos desde otros enfoque y perspectivas; así como apelando a otro tipo de métodos de observación.

El concepto “ciberguerra” se encarga de unir las visiones preexistentes y aquellas que aparecen de manera más reciente. Es la unión de la “guerra” como característica inherente que ha acompañado la humanidad en su constante evolución, y el prefijo “ciber”, haciendo referencia a una nueva ciencia, la cibernética, comprendida como el estudio de las interacciones entre el hombre y los aparatos electrónicos, y los tipos de sistemas de control y comunicación (Mindell, 2000); la cual surge de la creación de nuevos instrumentos por parte de la raza humana, en su afán de ejercer control sobre todo aquello que lo rodea.

Esta nueva temática ha empezado a ocupar un lugar importante en la literatura de las Relaciones Internacionales; situación justificada en la realidad cada vez más interconectada de sus actores y las acciones que se desplazan al entorno cibernético por una gran cantidad de ventajas que él ofrece. Pero, a pesar de aparecer de forma recurrente en los últimos años del desarrollo de conocimiento, y una gran cantidad de intentos, aún es un tema que no se trata con toda la libertad y del cual no existe un consenso teórico a nivel internacional.

La guerra en el entorno cibernético puede llegar a distar en ciertos aspectos de la guerra tradicionalmente conocida, y por tanto, es necesario en primera instancia conocer la guerra interestatal y la ciberguerra como conceptos, sus respectivas características y cómo han tomado protagonismo en el escenario internacional.

Acontecimientos como los sucedidos en las plantas de uranio de Irán durante 2010, aquello que se desarrolló tras la crisis política en Estonia y la guerra de Georgia con Rusia en 2007 y 2008 respectivamente reflejan el surgimiento de acciones en el nuevo entorno, pero la falta de un análisis juicioso de los fenómenos recientes, y cómo se adaptan al concepto de guerra tradicional,

hace necesario cuestionarse si los escenarios de ciberguerra acontecidos en Georgia, Irán y Estonia pueden calificarse como guerra interestatal.

Pregunta de Investigación

Asumiendo como estudio de caso los actos de ciberguerra ejercidos en contra de Estonia (2007), Georgia (2008) e Irán (2010) ¿Cómo se puede comprender en la actualidad el fenómeno de la ciberguerra a partir del enfoque clásico de la guerra interestatal, y, a partir de su propia teorización?

Justificación

El proyecto investigativo es de vital importancia, por el tipo de sociedad que se ha construido en la modernidad, vivir en un contexto en el cual los avances tecnológicos y la interconexión permite acortar distancias, llevar a cabo tareas de forma sencilla y veloz, que antes eran tediosas y prolongadas, disminuir los esfuerzos y los recursos, para cumplir los mismos objetivos con mayor eficiencia, entre otras cosas, hacen del entorno cibernético un espacio con grandes ventajas y proyección al futuro. Pero, al igual que toda creación humana, tiene pros y contras, los últimos representados por los ciberataques, el ciberespionaje, el robo de información, y demás tipos de agresiones; que, en manos de los actores equivocados, puede representar un gran riesgo para la sociedad internacional. Estos efectos negativos se vuelven un tema que exige su estudio y una aproximación que constituya este nuevo escenario como un contexto con oportunidades de aprovechamiento de las capacidades particulares que ofrece.

El trabajo puede ser llevado a cabo, pues existe información suficiente para la construcción de análisis; es de alta exigencia, pero los elementos para realizarlos son accesibles al aplicarse la metodología de investigación. Por lo tanto, se cuenta con fuentes de información que permiten una indagación profunda y de los cuales se puede extraer los datos necesarios para el desarrollo investigativo.

Para las Relaciones Internacionales como disciplina, tratar temáticas innovadoras es muy enriquecedor, y la pertinencia de la investigación se basa en la posibilidad de comprender un fenómeno, que puede llegar a ser complejo y algo distante, pero que se hace cada vez más visible en la realidad contemporánea, como lo es la ciberguerra y sus características; y de igual forma, enlazarlo con las teorías ya existentes que han permitido el entendimiento de los contextos vividos en tiempos pasados. Tomar casos de estudios específicos permite aplicar la teoría existente de tal forma que sea comprensible y es un método que permite resaltar los aspectos más importantes que aportan al desarrollo de conocimiento.

Los fenómenos que han acaparado la realidad internacional en lo transcurrido del siglo XXI tienen nuevas características de las cuales no existen antecedentes, por las particularidades y las herramientas con las que se cuenta. Los acontecimientos en Irán, Georgia y Estonia son el ejemplo claro de las nuevas formas de actuar de los actores internacionales; y convierte al ciberespacio en un entorno con gran proyección y que exigirá a todos los Estados el manejo profesional, profundo, constante y prudente de los nuevos instrumentos con los que se cuenta. El proyecto permite identificar las acciones que se han cometido, cuáles han sido los errores y las respuestas, y cuál es la nueva propuesta que presenta la ciberguerra y genera el interrogante de cómo enfrentarlo.

Objetivo General

Construir una posición actualizada del fenómeno de la ciberguerra a partir del enfoque clásico de la guerra interestatal, a partir de su propia teorización; tomando referencia los casos de ciberguerra ejercidos en contra de Estonia (2007), de Georgia (2008) e Irán (2010)

Objetivos Específicos

- Definir y explicar el concepto de guerra y guerra interestatal clásica.
- Presentar, a partir de la lógica y naturaleza de la ciberguerra, los acontecimientos ocurridos en Estonia (2007), Georgia (2008) e Irán (2010).
- Exponer la estructura argumentativa conceptual y teórica del fenómeno de la ciberguerra.
- Analizar, cómo a partir de la teoría clásica de la guerra interestatal, así como de la teoría de la ciberguerra, se puede llegar a la construcción de una posición o comprensión más acertada de este fenómeno propio de las Relaciones Internacionales.

Marco Conceptual

El proyecto exige el desarrollo de dos conceptos claves: Guerra Interestatal Clásica y Ciberguerra. La guerra, en su sentido clásico, es un concepto ampliamente difundido y de los más usados a nivel académico, y puede variar de un autor a otro. Ha sido usado para describir un conjunto enormemente diverso de condiciones y comportamientos a lo largo de la historia, y grandes teóricos han construido su definición propia. En su conceptualización, tal vez la más conocida, la guerra es definida como “un acto de fuerza que se lleva a cabo para obligar al

adversario a acatar nuestra voluntad" (Clausewitz, 2005, pág. 7); y asociada de forma directa al escenario político; es "un instrumento político, una continuación de la actividad política, una realización de ésta por otros medios" (Clausewitz, 2005, pág. 19). Por su parte, Sun Tzu afirma que la guerra es "el dominio de la vida o de la muerte, el camino hacia la supervivencia o la pérdida del Imperio: es forzoso manejarla bien" (Sun Tzu, 1999, pág. 5).

Van der Dennen (1995), autor mucho más contemporáneo, precisa que la guerra es "una especie del género de la violencia; más específicamente es colectiva, directa, manifiesta, personal, intencional, organizada, institucionalizada, instrumental, sancionada, violenta y, a veces ritualizada y regulada" (pág. 69), y agrega que solo se puede llevar a cabo entre Estados, característica que comparte con Clausewitz y Sun Tzu.

Para el presente trabajo se tendrán en cuenta los conceptos clásicos que se conocen, y además los que poseen mayor aceptación a nivel internacional para los estudiosos del tema, y algunos aportes de autores contemporáneos, con el fin de construir una definición de guerra convencional pertinente y con la mayor cantidad de elementos propios posibles. Para cumplir este objetivo, la guerra se definirá como un acto que exige la participación de actores estatales, que expresen sus capacidades para proteger su soberanía de los peligros y amenazas externas, y que busque y propenda por la consecución de un objetivo político claramente determinado.

Como segundo concepto esencial, aparece la ciberguerra. Esta noción se ha definido de distintas maneras, probablemente más veces que la guerra en si misma; debido a una razón fundamental: La guerra cibernética no es fenómeno que la sociedad ya haya presenciado en su máxima expresión, por lo tanto, la teoría se ha construido a partir de las capacidades que los

actores hacen visibles, el manejo de los avances tecnológicos y la penetración que pueden tener en el ciberespacio, y la proyección del ciberespacio como futuro escenario de enfrentamientos. Con esto en mente, la ciberguerra se definirá por varios autores, para agrupar las características comunes del concepto que se pueden aplicar al proyecto.

Para Kevin Coleman (2008), la guerra cibernética se define como "un conflicto que utiliza transacciones hostiles o ataques a ordenadores y redes en un esfuerzo por interrumpir las comunicaciones y otras piezas de la infraestructura, como un mecanismo para infligir daño económico o alterar y atacar las defensas". Según el Departamento de Defensa de los Estados Unidos (2006), el objetivo es interrumpir, denegar, degradar o destruir la información almacenada en los equipos y maquinas que la contienen y sus redes informáticas, o los equipos y las redes en sí mismas. Y Nils Melzer (2011) afirma que la ciberguerra, en su definición más básica es "la guerra llevada a cabo en el ciberespacio a través de medios y métodos cibernéticos" (pág. 4).

Otra definición afirma que la ciberguerra es toda acción por parte de un Estado con el fin de penetrar en los ordenadores o redes de otra nación buscando causar daños o molestias, siendo esta real, global, y capaz de ocurrir a la velocidad de la luz (Clarke & Knake, 2010). La RAND Corporation (s.f.), tanque de pensamiento estadounidense en constante trabajo conjunto con las Fuerzas Militares norteamericanas, define la ciberguerra como aquella que "involucra las acciones de una organización del Estado nacional o internacional para atacar y tratar de dañar las computadoras de otra nación o redes de información a través de, por ejemplo, virus informáticos o ataques de denegación de servicio".

Las conceptualizaciones ofrecen características similares, que permiten concatenarlas y afirmar que la ciberguerra es un fenómeno que exige la participación de actores estatales o sus instituciones, y se genera a partir de las acciones en las cuales el Estado pretende generar daños, interrupciones, denegaciones de servicios, entre otras agresiones; basado en un objetivo determinado, a través de medios cibernéticos.

Marco Teórico

Si bien el desarrollo académico ha permitido la construcción de teorías específicas para el estudio de la guerra y la ciberguerra, las Relaciones Internacionales permiten que algunos enfoques que no estudian exclusivamente el fenómeno de las acciones bélicas, aporten de manera importante al estudio del mismo En este caso, las teorías más pertinentes son el realismo y la interdependencia, sin convertirlas en posiciones contradictorias, sino en marcos de referencia; unidas a la visión de Manuel Castells y su concepto de era de la información. La intención en este proyecto de investigación es que, a través del uso de enfoques ya existentes, se comprenda el fenómeno de la ciberguerra y se construya una perspectiva que incluya el contexto moderno y las teorías clásicas de la disciplina.

Con referencia al realismo, está más que claro, que se seguirá considerando al Estado como actor protagónico: "único actor digno de consideración en un medio de carácter político y (…) [como] la forma histórica de organización del ejercicio del poder en las relaciones internacionales" (Barbé, 1987, pág. 155). Morgenthau (1986) presenta en su teoría los seis principios del comportamiento de los Estados en un sistema anárquico, y estos explican el porqué de las acciones contra Estonia, Georgia e Irán. Se demostrará que el proceder de los

Estados atacantes estaba motivado por el deseo de poder y la consecución de los intereses nacionales, es decir, que a pesar del cambio de medios y de escenario, la ciberguerra mantiene los objetivos políticos. Además la guerra en el ciberespacio refleja el comportamiento egoísta de los Estados, porque son acciones que no representan enfrentamiento directo y se pueden realizar de forma unilateral.

En cuanto a la interdependencia compleja, se tendrá en cuenta su concepto teórico: "Interdependencia en la política mundial se refiere a situaciones caracterizadas por efectos recíprocos entre los países o entre actores de diferentes países" (Keohane & Nye, 2011, pág. 8). El cambio de paradigma en las últimas décadas del siglo XX representó el deseo de los Estados por generar una sociedad más conectada, donde el desarrollo, principalmente económico, y el proceso de globalización requerían una herramienta para alcanzar sus fines de forma más efectiva, y presentó la oportunidad para proponer el ciberespacio como el escenario adecuado para desarrollar el sueño global. Pero no todo fue perfección y el ciberespacio surgió como contexto, no solo para facilitar el trabajo del sistema internacional, sino también como un teatro de alta peligrosidad para los Estados con mayor conexión a él.

Al convertirse en un nuevo riesgo para la estabilidad de los Estados, los aspectos de sensibilidad y vulnerabilidad de la teoría de interdependencia pueden jugar un papel vital. La sensibilidad, entendida como "el efecto (que) tiene sobre un actor una acción ejecutada por otro" (Pardo & Tokatlian, 1990, pág. 347); empezó a surgir como concepto dentro de los planes de seguridad de los Estados, pues la amenaza cibernética podría alcanzar efectos antes desconocidos. Y la vulnerabilidad, definida como "los costos reales que afectan a un actor por la acción de otro, teniendo en cuenta su relativa disponibilidad o carestía de recursos alternativos

para responder" (Pardo & Tokatlian, 1990, pág. 347); es vital, porque la ciberguerra representa un nuevo entorno en el cual los Estados deben fortalecerse defensivamente y aprender a atacar, y enfrentarán mayores costos que probablemente no se habían contemplado.

Una vez queda clara la conveniencia del uso del realismo político y la interdependencia compleja como marco para la comprensión del fenómeno cibernético, la sociología hace su contribución con el español Manuel Castells (2006), quien expone el concepto de la sociedad red y la define como:

> Aquella cuya estructura social (está) compuesta de redes potenciadas por tecnologías de la información y de la comunicación basadas en la microelectrónica. Entiendo por estructura social aquellos acuerdos organizativos humanos en relación con la producción, el consumo, la reproducción, la experiencia y el poder, expresados mediante una comunicación significativa codificada por la cultura. (pág. 27)

La obra de Castells, si bien no hace referencia directa a la guerra y ciberguerra como fenómenos, es el punto de enclave, al resumir cómo funciona la sociedad en la actualidad y lo que representa la cibernética y las conexiones para los actores, como individuos y como Estados; es decir, que con el devenir de la tecnología y su impacto en el comportamiento político y social, se reafirma la indispensabilidad del ciberespacio para el comportamiento de la comunidad global como es conocida en la actualidad y la disponibilidad de elementos vitales para los Estados que ahora pueden ser encontrados en la red, lo que permite concluir que se convierte en un escenario vulnerable, y que puede ser explotado y aprovechado por los actores.

Las teorías precedentes abren paso a los enfoques que se han especializado exclusivamente en estudiar la guerra y la ciberguerra y los ubican como objeto de estudio. De la guerra se encarga la polemología y la teoría de la ciberguerra, novedosa, se ha construido con el paso de las últimas décadas. La primera surge de la necesidad del sociólogo francés Gastón Bouthoul, de "elaborar y aplicar métodos científicos al estudio de las guerras, como medio o receta, para luchar por su desaparición" (Franco Suanzes, 2000, pág. 59), con la clara pretensión de crear marcos y espacios académicos dedicados a la investigación de las causas reales de los conflictos, para poder enfrentarlas. Esta corriente ideológica se convierte al poco tiempo, en una disciplina conocida a nivel global, que ha permitido la construcción de un acercamiento mucho más analítico y profundo de lo que es la guerra y su impacto como fenómeno social.

Por otro lado, si bien aún no se conoce un neologismo, se ha dado la construcción de la teoría de la ciberguerra, que la explique fenomenológicamente. Martin Libicki (2009), apoyado por la RAND Corporation, construye un marco, en el cual explica que la ciberguerra puede ser "la interrupción o daño deliberado por parte de un Estado a un sistema de interés a otro Estado" (pág. 23); y se extiende al afirmar que la ciberguerra sucede cuando otros tipos de disuasión no han funcionado; además de agregar conceptos como ciberataques y ciberdefensa como ejes para el comportamiento de los Estados en el ciberespacio.

Paul Rosenzweig (2013), en su obra *Cyber Warfare How Conflicts in Cyberspace Are Challenging America and Changing the World*, se encarga de presentar no solo el concepto de ciberguerra, y avanza al describir la naturaleza del fenómeno y de su escenario, además de exponer los riesgos que representa la guerra ciberespacial para los Estados y cuales deberían ser las cuestiones primordiales que estos actores deben enfrentar para no sufrir perjuicios severos.

A pesar de la dificultad para crear una teoría única que cobije todos los aspectos de la guerra en el ciberespacio, tal vez la aproximación más aceptada a nivel internacional para la conceptualización, la regulación y el reconocimiento de los impactos que puede generar este fenómeno, es el Manual de Tallin, el cual se desarrolló con el objetivo de crear "la ley que rige la guerra cibernética" (Schmitt, 2013, pág. 16); y puede ser el acercamiento teórico más importante, porque reunió a los expertos más importantes sobre el tema en la actualidad.

El proyecto será enriquecido por un marco teórico integral, al usar las teorías clásicas de las Relaciones Internacionales y unirlas a los enfoques específicos de la guerra y la ciberguerra, que permitirán el desarrollo y la profundización en el tema de investigación.

Diseño Metodológico

La investigación que se llevará a cabo es de carácter cualitativo - interpretativo, a través del método de estudio de caso y de investigación evaluativa; con técnicas de análisis documental y observación del fenómeno. La investigación de tipo interpretativa, permite la comprensión y el posterior análisis de los acontecimientos sociales.

El método de estudio de caso permite conocer una situación específica, sus características propias y su impacto generando un objeto de estudio a partir de un caso en particular. Por otro lado, la investigación evaluativa se enfoca en determinar si los conceptos y las teorías son aplicables a una situación determinada.

La recolección de datos se hará a partir de la observación no participante del fenómeno y se recogerá información a partir de los procesos tomados como estudios de caso. Igualmente a

través de un análisis documental de fuentes primarias y secundarias, desde el cual se tomarán los datos más pertinentes para contestar la pregunta problema. Al obtener los datos, se realizará un análisis que permita hacer un proceso sistemático, selectivo y reflexivo de la conveniencia de la información obtenida.

El desarrollo del proyecto se llevará a cabo en tres etapas, siendo la primera meramente descriptiva, abordando los acontecimientos sucedidos en Georgia, Estonia e Irán. En segundo lugar, se propondrá un escenario en el cual la ciberguerra ofrece características específicas que pueden llegar a ser beneficiosas o perjudiciales al contexto de conflicto en la actualidad. Por último, se tomarán los conceptos claves de la guerra interestatal y se construirá un análisis que permita descubrir la pertinencia de la aplicación de los mismos en la guerra cibernética.

1. ¿Qué es la guerra?

Como una gran cantidad de conceptos acerca de los fenómenos sociales, la guerra no puede ser puntualizada con facilidad. La pluralidad es la principal característica del contenido creado por una serie de autores que se han atrevido a definir el término. Con el objetivo de definir qué es la guerra es indispensable hacer un recorrido por una cantidad prudente de concepciones que permitan reconocer los elementos comunes y generen un marco conceptual definitivo acerca de dicho fenómeno. Para cumplir con esta tarea de una forma organizada, el recorrido se hará con un carácter cronológico.

Para iniciar, etimológicamente, el término guerra "se deriva del alemán antiguo *werra*, lo que significa confusión, discordia o contienda" (Van der Dennen, 1995, pág. 69). Sun Tzu (1999), militar chino, se encargó de emprender el camino de la construcción de teorías acerca de la guerra mucho antes que cualquier otro. Es reconocido como el pionero en esta temática y a pesar la antigüedad de sus escritos, mantiene vigencia. El autor chino definió la guerra como "el dominio de la vida o de la muerte, el camino hacia la supervivencia o la pérdida del Imperio" (pág. 5).

El otro autor que es mundialmente reconocido por su desarrollo teórico sobre la guerra, de una forma mucho más contemporánea, es Carl von Clausewitz, militar que vivió entre los siglos XVIII y XIX las Guerras Napoleónicas, y dada su vasta experiencia, dedicó su tiempo a la construcción de su obra sobre temas militares. Clausewitz (2005) define la guerra como "un acto de fuerza que se lleva a cabo para obligar al adversario a acatar nuestra voluntad" (pág. 7). El autor asocia de forma directa la guerra al escenario político; pues se refiere a ella como "un

instrumento político, una continuación de la actividad política, una realización de ésta por otros medios" (Clausewitz, 2005, pág. 19).

El siglo XX se convierte en el periodo de auge, en la época dorada de la teorización de la guerra. Es aquí donde surge una cantidad significativa de pensadores alrededor del mundo que pretenden poner fin al conflicto sobre la universalidad de un concepto de guerra y construyen los propios. Georges Sorel (1912) define 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 la más fuerte e imponer la voluntad de quien gane.

Para Carl Schmitt (2014), en su obra *El concepto de lo político*, de 1932, conceptualiza la guerra como "el combate armado entre unidades políticas organizadas" (pág. 20). Y toda su teoría se construye desde los actores que él define como amigos y enemigos:

> La guerra proviene de la enemistad puesto que ésta es la negación esencial de otro ser. La guerra es solamente la enemistad hecha real del modo más manifiesto. No tiene por qué ser algo cotidiano, algo normal; ni tampoco tiene por qué ser percibido como algo ideal o deseable. Pero debe estar presente como posibilidad real si el concepto de enemigo ha de tener significado. (Schmitt, 2014, p. 20)

Horacio Kallen (1939) reitera la parte política de la guerra: "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" (pág. 373) Por otro lado agrega nuevos componentes a los conceptos ya

conocidos, y acaba con la exclusividad del aspecto militar en la guerra, al afirmar que la organización de las fuerzas armadas se extiende más allá de sí mismas, y afecta las actividades civiles, como la industria, la producción y el comercio, así como los aspectos sociales y las actitudes individuales (Kallen, 1939).

Los sociólogos jugaron un papel muy importante al construir teorías sobre la guerra. Por su parte, el inglés Bronisław Malinowski (1941) definió la guerra como un concurso armado entre dos unidades políticas independientes, por medio de una fuerza militar organizada, en búsqueda de una política nacional. Y L. L. Bernard (1944), de misma profesión, pero en este caso, estadounidense, propuso una definición de uso múltiple. Para él, la guerra es un conflicto organizado y continuo de carácter transitorio entre dos o más colectividades, capaces de armarse y organizarse para una lucha violenta, llevada a cabo por los ejércitos sobre la tierra, o en su defecto unidades navales en agua. Pero además, se contaba con el apoyo de los civiles o la población, que si bien no estaba completamente militarizada, se encontraba respaldando desde atrás. La guerra siempre se constituía con el fin de conseguir algún objetivo político o casi político bien definido.

Al acercar la sociología con los conceptos políticos, el resultado fue identificar que la guerra sólo puede tener lugar entre entidades políticas soberanas. Y además otorga una condición legal que igualmente permite que estos actores lleven a cabo un conflicto por la fuerza (Wright, 1965). Las guerras exigen la implicación directa del Estado y sus instituciones, ya que se desarrolla en un contexto internacional, lo que genera riesgos de desaparecer como unidad estatal (Aron, 1966); y es claro que el principal interés de los Estados es su supervivencia, y llegaran a las últimas consecuencias para mantenerse con vida.

Del mismo modo y manteniendo la connotación social del concepto, Otterbein (1970) define la guerra como una lucha armada entre las comunidades políticas; entendiendo una comunidad política como un grupo de personas definidas en términos de la ocupación de un territorio común y una institución que se encargue de liderar a la población y defienda su soberanía (Naroll, 1964).

En la década de los 70's vuelve a brillar la evocación a la política. Barringer (1972) considera que la guerra es un modo de la actividad política dirigida a resolver de manera efectiva y favorablemente un conflicto de intereses. Pero en ese sentido, la guerra no es un único método, sino uno de los numerosos procedimientos junto a la negociación, la conciliación, la mediación, el arbitraje y la adjudicación. Este tipo de soluciones solo se pueden llevar a cabo por parte de las fuerzas armadas de dos o más facciones políticas reconocidas, organizaciones, naciones, gobiernos o Estados. Este estatus de beligerancia implica soberanía. Una lucha se puede considerar una guerra sólo si los contendientes son unidades políticas soberanas (Lider, 1977).

Para Gaston Bouthoul, sociólogo francés de fama internacional, reconocido por la creación de la polemología, es decir, "la sociología científica de las guerras, consagrada al estudio de sus causas presuntas, de su periodicidad y de su previsión y prevención" (Molina Cano, 2014, pág. 199); la guerra convencional se trataría de:

> Un fenómeno que abarca las siguientes características: tiene un carácter colectivo y de lucha a mano armada; requiere de un enemigo activo e implica un enfrentamiento recíproco; en la acción bélica y dentro del grupo, se necesita de ayuda mutua y cooperación; por último, la guerra es una manifestación de violencia organizada entre grupos que se baten para zanjar una discusión o conflicto. (Franco Suanzes, 2000, pág. 62)

En este punto, si la concepción es meramente social, se podría decir que la guerra es tan antigua como la humanidad misma, pues se incluyen los actos esporádicos de violencia entre familias o las pequeñas bandas igualitarias que carecen de liderazgo definido (Harrison, 1973). Si, por otro lado, se afirma que los actos de hostilidad, a fin de ser definidos como actos de guerra, deben exhibir algún tipo de liderazgo y un poco de planificación, es decir, la existencia de una entidad política, así como el uso de la fuerza armada, la guerra será vista como una actividad social cuya génesis si bien no se puede determinar con precisión, surge a partir del desarrollo, la organización y los avances de la humanidad, y se adapta a sus respectivos cambios, es decir, es el resultado de las actividades o condiciones relacionadas con la procesión de la evolución sociocultural del hombre (Harrison, 1973).

Johan M.G. Van der Dennen (1995) autor contemporáneo, precisa que la guerra convencional es "una especie del género de la violencia; más específicamente, es colectiva, directa, manifiesta, personal, intencional, organizada, institucionalizada, instrumental, sancionada, violenta y, a veces ritualizada y regulada" (Pág. 69). Al afirmar esto, asegura, al igual que los demás, que estas características distintivas y las respectivas delineaciones dimensionales no son limitativas, y pueden adaptarse a los cambios que se presenten con la evolución de la sociedad. Van der Dennem termina su definición, al aseverar que la guerra interestatal, sólo puede tener lugar entre las entidades políticas soberanas, es decir, los Estados, lo que la convierte en un medio para resolver las diferencias entre las unidades del orden más alto de la organización política (Van der Dennen, 2016, pág. 3).

Con el fin de sintetizar un poco los distintos rasgos que presentan las definiciones presentadas, se puede decir que la guerra clásica interestatal requiere organización y recursos,

que debe darse entre dos adversarios o más, que si bien implica a las fuerzas armadas como eje principal, también exige la legitimidad que otorga la población civil, y que puede afectar no solo a los que se encuentran enfrentes de batallas, sino a las instituciones públicas y privadas, que solo alcanza el estatus de guerra cuando los actores son Estados, pues son las únicas unidades capaces de ofrecer todos los requisitos para el desarrollo de la misma. Y probablemente la característica esencial, y sin importar la época, los autores concuerdan en ello, siempre tiene como objetivo sobreponer la voluntad sobre el vencido y por lo tanto su fin es siempre político.

2. ¿Qué sucedió? Estonia, Georgia e Irán

Durante la última década, las agresiones por medios cibernéticos que constituyen la ciberguerra han aumentado de una forma abrumadora, y es sencillo descubrir por qué. Los avances tecnológicos le han permitido a los Estados actuar sobre entornos que antes ni siquiera existían, y tal como se alcanzó soberanía sobre la tierra, el mar y el cielo; el ciberespacio se convierte en el nuevo escenario de acción. Para que exista una visión más precisa, que permita la comprensión de lo que puede representar la ciberguerra dentro de la guerra interestatal clásica, los estudios de caso se vuelven una valiosa herramienta; al convertirse en una reflejo de los alcances de la guerra cibernética.

Dentro de las acciones cibernéticas realizadas durante los últimos años, resaltan algunas que, si bien no han sido las únicas, si han generado efectos dramáticos que han quedado marcados como hitos, y que probablemente por otros medios, no hubiesen alcanzado los mismos resultados obtenidos por los mecanismos cibernéticos. En orden cronológico se encuentran: Estonia en 2007, Georgia en 2008 y en Irán mientras transcurría el año 2010, siendo casos donde la guerra ciberespacial figura como protagonista ante los respectivos contextos.

2.1 Estonia

En primer lugar, surge la situación que se vivió durante el primer semestre de 2007 en territorio estonio. Transcurridas dos semanas entre abril y mayo, Estonia fue víctima de agresiones cibernéticas en forma masiva sobre su infraestructura, considerado el primer asalto cibernético dirigido a la seguridad nacional de un país (Ashmore, 2009). El contexto en el cual se

genera la guerra en el ciberespacio es de vital importancia para identificar las causas, los medios y el atacante.

Estonia es una de las repúblicas bálticas, que se incorporaron a la Unión Soviética en 1940. En 1989, tras la disolución de la URSS, Estonia recuperó su independencia y comenzó un proceso que puede denominarse como de "occidentalización", rápidas reformas económicas, políticas y sociales; acompañadas de la adhesión a la Unión Europea y la OTAN en 2004 con el fin de garantizar su seguridad (Kozlowski, 2014). Para 2007, en Estonia había una minoría rusa, y un conflicto cultural y político de vieja data, explotó por una decisión del gobierno estonio, lo que produjo una tensión interna, que desencadenó las acciones en el ciberespacio:

> Estonia se compone de 1,3 millones de personas, donde el 25,6% de la población es rusa (…) Estonia ha visto la presencia de Rusia como una ocupación ilegal (…) Los rusos, por otro lado ven a los estonios como una población ingrata porque se salvaron de los fascistas nazis gracias a Rusia (…) Los hechos reales se centraron en el monumento soviético "Soldado de Bronce", monumento que conmemoraba a los soldados soviéticos que murieron durante la Segunda Guerra Mundial y sus respectivas tumbas. Sin embargo, con el tiempo los rusos étnicos habían utilizado el monumento como un sitio de reunión para las manifestaciones y otras formas de protesta contra el gobierno estonio. Esto condujo que el gobierno de Estonia moviera el monumento a un área menos pública. (Ashmore, 2009, pág. 6)

La decisión del traslado de la escultura generó un malestar en la minoría rusa, que se encargó de manifestarlo a través de protestas en Tallin y frente a la embajada de Estonia en Moscú el 27 de abril, donde causaron daños a la propiedad pública, y del mismo modo, el gobierno ruso se pronunció al afirmar que el gobierno estonio estaba "rompiendo las leyes humanas y exigió la

renuncia del primer ministro" (Kozlowski, 2014, pág. 238). Tras dar por terminadas las manifestaciones físicas, se consideró el final de la controversia; pero lo que sucedió durante las dos semanas siguientes, sorprendería no solo al gobierno del país báltico, si no al planeta en general.

Para el 29 de abril, si bien ya no habían protestas en escenarios públicos, se propagaba por internet una campaña de interrupción y denegación de servicios a lo largo de la infraestructura electrónica de Estonia, usando paquetes de sobrecarga, desconfiguración de páginas web y avalanchas de correos no deseados y cargados de virus (Ruef, Shakarian & Shakarian, 2013). Durante tres semanas, Estonia vio cómo su infraestructura de servicios y su red de internet pasaban de sufrir algunos tropiezos, a estar bajo tutela de otros y perdía su poder para defender sus intereses como Estado.

Lo que había comenzado como un problema mínimo de seguridad en sus Tecnologías de la Información (TI), se convirtió en una situación que amenazaba la seguridad nacional y que tomó un nivel de seriedad altísimo, cuando el 28 de abril, el jefe de relaciones públicas del Ministerio de Defensa de Estonia declaró "Estamos bajo ciberataque. Su superior, el Ministro de Defensa estonio Jaak Aaviksso dijo: Resultó ser una situación de seguridad nacional" (Schdmit, 2013, pág. 8). La infraestructura se vio tan afectada, que fueron cerrados los sitios web de todos los ministerios, varios partidos políticos, algunos bancos y portales de medios de comunicación; y se llegó a desactivar por completo el servicio de internet y correo electrónico del parlamento.

Los daños a los medios de comunicación hicieron que fuera imposible para los lectores, dentro y fuera del territorio, ingresar a los portales web, lo que generó aún más desconocimiento

sobre la situación que vivían los estonios. Y las violaciones de seguridad que sufrieron las entidades financieras como HansaBank, produjeron pérdidas por casi un millón de dólares, pues los clientes tanto dentro de Estonia, como fuera, no pudieron disponer de sus cuentas ni sus recursos; a pesar de estar fuera de circulación por tan solo una hora y media (Schdmit, 2013).

Si bien en algún punto se pudo llegar a pensar que una ofensiva de tipo cibernético no tendría un efecto relevante y menos en un país tan pequeño, tras lo sucedido en Estonia, es una teoría que se queda sin fundamentos. Estonia puede ser visto como un modelo para los demás Estados en el futuro. Los estonios, como casi todos los países desarrollados y con capacidades en el sector tecnológico, se han aprovechado de los grandes beneficios que tienen los avances científicos en esta área y usan el Internet para las elecciones, al usar votación automatizada, la educación, la seguridad y el sector bancario:

> Estonia basa el funcionamiento de su infraestructura crítica en la Internet; las redes electrónicas son esenciales para la labor de las operaciones gubernamentales, redes de energía eléctrica, servicios bancarios, e incluso el suministro de agua de Tallin. En Estonia, el 97% de las transacciones bancarias se producen en línea; y para 2007, 60% de la población del país utiliza Internet a diario. Además (…) el Estado estonio es tan dependiente de la Internet que su modelo de operaciones del gobierno se conoce como "gobierno sin papel". (Herzog, 2011, pág. 51)

Un Estado, desconcertado por la dimensión que alcanzó la guerra en el ciberespacio, buscó cursos de acción, y la mejor manera era obteniendo el apoyo internacional para mitigar las consecuencias negativas de la guerra ciberespacial. El gobierno fue capaz de emplear su Equipo de Respuesta a Emergencias Informáticas (CERT) para defenderse y, con la ayuda de los aliados, superar los peligros. Alemania, Israel, Eslovenia y Finlandia proporcionaron asistencia para

restaurar las operaciones de redes normales, mientras que el OTAN Computer Emergency Response Team también ayudó a las reparaciones de los sistemas (Ashmore, 2009). Aunque el daño pude ser mitigado, el mundo fue testigo de una situación de la cual había escuchado, y tal vez imaginado, pero que hasta ese momento no había visto nunca, la guerra cibernética apagó la infraestructura de información de un país entero (Iasiello, 2013).

Respecto a la asignación de responsabilidades, si bien por la naturaleza de los fenómenos cibernéticos, es difícil determinar culpabilidades con precisión, existen rastros que implican al gobierno ruso como autor de lo sucedido. En primer lugar, las direcciones IP de donde nacieron las acciones fueron rastreadas hasta territorio ruso. Por otro lado, antes del inicio de la ciberguerra, el gobierno ruso protestó por el movimiento del monumento ruso y advirtió lo desastroso que podría ser para Estonia si se realizaba la reubicación (Ashmore, 2009).

Además que el grupo pro-Kremlin “Nashi”, acusado con anterioridad de trabajar en nombre de Moscú, se adjudicara la responsabilidad de los daños, y que este grupo fuera financiado por entidades que a su vez financian al gobierno ruso, hizo pensar que Rusia bien podría estar detrás de la guerra en el ciberespacio aplicada a Estonia. Se puede agregar a estos argumentos que durante las acciones cibernéticas, el día con mayor intensidad fuese el 9 de mayo “Día de la Victoria”, en el cual se conmemoraba el triunfo para Rusia sobre el ejército alemán en la Segunda Guerra Mundial, además el hecho de que no hicieron propuestas para detener o frenar la ciberguerra que se estaba gestando desde su territorio (Iasiello, 2013). Por supuesto los dirigentes estonios tomaron los argumentos existentes, y asumieron que las autoridades rusas eran responsables; situación que condicionó el comportamiento de las relaciones diplomáticas entre ambos países, que se mantienen tensas hasta el día de hoy.

2.2 Georgia

En 2008 “lo que comenzó como un asalto encabezado por Georgia en contra del régimen separatista de Osetia del Sur, rápidamente se convirtió en un conflicto armado entre Rusia y Georgia” (Bonstra, 2008, pág. 1). La guerra que inició en agosto, representó la condensación de una larga historia de conflictos geoestratégicos entre las dos naciones, como lo fueron la Guerra de Osetia del Sur en 1992 y la Guerra de Abjasia en 1993. El enfrentamiento comenzó oficialmente el 7 de agosto de 2008 después de varias semanas de tensión por las crecientes posiciones disidentes sobre el futuro del territorio de Osetia del Sur propuestas por Rusia y Georgia (Hollis, 2011).

Tropas georgianas iniciaron un ataque militar contra Osetia del Sur y comenzaron un bombardeo masivo de la ciudad de Tsjinvali, en respuesta a la supuesta provocación de Rusia. Rusia desplegó tropas de combate adicionales a Osetia del Sur y respondió con bombardeos en territorio georgiano (Bonstra, 2008). La derrota militar táctica de Georgia en la batalla de Tsjinvali, la derrota operativa a través de la invasión sin oposición de la parte occidental de Georgia, el bloqueo naval a Georgia y la dificultad para conseguir que su mensaje fuera conocido por los medios de comunicación al mundo, llevó a la derrota estratégica de Georgia en la guerra.

Pero el caso de Georgia presenta una cuestión interesante: La ciberguerra que se presentó contra el Estado en el Cáucaso, se produjo al mismo tiempo que los enfrentamientos bélicos de forma física:

> A pesar del hecho, de que la guerra era clásica y el comportamiento de los ejércitos en el campo de batalla recordaba lo que se vivió en el siglo XX, un aspecto era una novedad completa. Fue la

> primera guerra que tuvo lugar en el aire, en la tierra, en el mar y en el nuevo dominio: el ciberespacio. (Kozlowski, 2014, pág. 239)

En este caso, los problemas cibernéticos para Georgia se dieron con anticipación a los enfrentamientos bélicos: "El 19 de julio de 2008, una empresa de seguridad de Internet informó de un ataque cibernético por medio de una denegación de servicio contra los sitios web en el país" (Kastenberg & Korns, 2009, pág. 60); pero se fortalecieron e intensificaron con la llegada de las tropas terrestres y los bombardeos rusos, durante la segunda semana de agosto.

Entre el 8 y el 12 de agosto, fechas de intenso combate hasta alcanzar el cese de hostilidades, la guerra en el ciberespacio aumentó en número de ataques, en la especificidad de los sitios web como destinos y también en sofisticación. "El 9 de agosto el foro *StopGeorgia.ru* estaba en marcha (…) No sólo era un grupo de hackers experimentados, contaba con una lista de los 37 objetivos de alto valor en la web, para acceder desde direcciones IP de Rusia o Lituania" (Carr, 2009, pág. 15). El tiempo demostró que existieron mejoras para el desarrollo y el alcance de la guerra en el ciberespacio, para hacerla más dañina, en este caso, sobre la infraestructura crítica de Estonia.

La ciberguerra se produjo en dos fases. En un primer momento, estuvo dirigida principalmente a los sitios web del gobierno y a los medios de comunicación de Georgia, y al no tener estructuras de defensa más fuertes, fue más fácil de atacar y dejar inoperable por periodos más largos. En la segunda fase se buscó infligir daños a una lista de objetivos más amplia, incluyendo instituciones financieras, empresas, instituciones educativas, medios de comunicación occidentales (BBC y CNN), y un sitio web de hackers en Georgia (Ruef, Shakarian & Shakarian, 2013).

En este caso, los asaltos no se quedaron exclusivamente en la denegación de servicios. Se usaron nuevos métodos que generaban desconfiguración de redes, donde desaparecía el mensaje real y aparecía alguno alusivo al gobierno de Rusia; además lograron que las fallas fueran mucho más duraderas y más difíciles de solucionar (Cyber Committee of AFCEA, 2012). Y un avance de suma importancia, se apoderaron de correos electrónicos y consiguieron una gran cantidad de información valiosa para el gobierno georgiano; utilizado en la inteligencia militar rusa, que les servía también para su accionar en tierra.

Aunque Georgia no es un país dependiente de las infraestructuras cibernéticas, en este caso específico la información que obtuvieron los rusos a partir de sus inmersiones en las redes georgianas, les permitió actuar de forma más precisa durante los enfrentamientos bélicos. Kenneth Corbin (2009) escribió que los fines que motivaron la guerra en el ciberespacio por parte de los rusos, eran aislar y silenciar a los georgianos. La ciberguerra logró silenciar los medios de comunicación y aislar al país de la comunidad global. La lista de objetivos que fueron atacados dan fe de la opinión de Corbin, y además, la población georgiana sufrió un impacto psicológico al dejarse llevar por un sentimientos de derrota, ya que no fueron capaces de comunicar lo que estaba pasando con el mundo exterior y mantener la soberanía sobre un entorno que no consideraban valioso, y que al final, demostró su importancia.

Responsabilizar a Rusia de la guerra en el ciberespacio llevada a cabo contra Georgia puede llegar a ser un poco más sencillo en este caso, pues se encontraban en conflicto, lo que permite pensar que el interés ruso era ganar en todos los escenarios posibles. Además, es claro que las mejoras visibles de los acciones ofensivas en el ciberespacio exigen inversiones económicas importantes, y que los beneficios que recibirían las Fuerzas Militares rusas pagarían la inversión

dl uso de la guerra cibernética. “Dicha coordinación con las fuerzas militares y negar al adversario cualquier medio de comunicación podría sugerir que el gobierno ruso y sus militares estaban detrás de la andanada de ataques cibernéticos. Habrían sido el mayor beneficiario de la situación” (Cyber Committee of AFCEA, 2012, pág. 13).

Si bien, y como en todos los casos donde se lleva a cabo la guerra a través del ciberespacio, establecer que Rusia fue el culpable es un tanto difícil, pero la coincidencia del actuar coordinado entre las fuerzas terrestres rusas y las fuerzas cibernéticos invisibles está lejos de ser un evento aleatorio. Además de las posibles conexiones con un proveedor principal en las redes de Rusia, los patrones de la guerra cibernética también sugiere que debió existir algún tipo de comunicación con el ejército ruso. Dicha asistencia táctica y operativa en el ciberespacio puede ser beneficiosa cuando coincidió perfectamente con la ubicación y el destino de los militares rusos (Cyber Committee of AFCEA, 2012).

2.3 Irán

Está más que claro que las plantas de refinamiento de uranio que posee Irán se convirtieron en una amenaza para la hegemonía nuclear de los países con este tipo de energía, un peligro para la estabilidad mundial, la prueba de una realidad muchas veces negada, haciendo referencia a la existencia de plantas que producen energía y bien podrían producir armas nucleares en manos de países que no tienen autorización ni supervisión de la OIEA, y una razón de conflicto y tensión con los Estados vecinos. El propósito inicial del programa nuclear iraní fue generar electricidad y reducir la dependencia de las energías no renovables y los combustibles fósiles. Los Estados Unidos, Francia y Alemania apoyaron este esfuerzo durante el gobierno del Sha, pero la ayuda se

detuvo debido a los temores de que Irán desarrollara en algún momento un arma nuclear (Gamero Garrido, 2014).

Actualmente existe un acuerdo con las seis potencias mundiales sobre el manejo de la energía nuclear en Irán, pero hace algo más de seis años la situación no era tan armónica ni se resolvía por vías diplomáticas, y la planta de refinamiento de uranio en Natanz sufrió una irrupción que significó retrasar el programa nuclear de Irán y que se llevó a cabo por medios cibernéticos:

> El 17 de junio de 2010, investigadores de seguridad en una pequeña empresa bielorrusa conocida como VirusBlockAda identificaron un software malicioso (malware) que infectaba las memorias USB. En los meses siguientes, hubo una oleada de actividades en la comunidad de seguridad informática, revelando que este descubrimiento identificaba un nuevo gusano informático conocido como Stuxnet. Este software fue diseñado específicamente para afectar equipo industrial. Una vez que se reveló que la mayoría de las infecciones fueron descubiertas en Irán, junto con un inexplicable retiro del servicio de centrífugas en la planta de enriquecimiento de combustible iraní en Natanz, muchos en los medios de comunicación especularon que la meta final de Stuxnet era atacar las instalaciones nucleares iraníes. (Shakarian, 2011, pág. 50)

El software fue bautizado como Stuxnet, un gusano informático diseñado exclusivamente para generar daños en los controles industriales, específicamente sobre los sistemas SCADA (Sistemas de Control, Supervisión y Adquisición de Datos). En primer lugar, es importante definir que es un gusano informático: Es un programa que realiza copias de sí mismo, para infectar a otros ordenadores y se propaga automáticamente en una red, independientemente de la acción humana (Sáez Collantes, 2012). Como segundo punto, surge la necesidad de aclarar que

es un Sistema SCADA: "Estos sistemas están diseñados para la recopilación, control y vigilancia de datos en tiempo real de infraestructuras críticas, incluyendo plantas de energía, oleoductos, gasoductos, refinerías, sistemas de agua u otras aplicaciones que requieren equipo controlado por computadoras" (Shakarian, 2011, pág. 51). Este sofisticado programa informático estaba diseñado para penetrar y establecer control sobre estos sistemas remotos, no se podía enviar desde las redes públicas y requirió dispositivos intermedios que permitieran su tránsito. Usando vulnerabilidades desconocidas para los ingenieros que manejaban las centrifugadores de enriquecimiento, y que por lo tanto no tienen protección, fue capaz de atacar y reprogramar por completo el ordenador en Irán (Farwell & Rohozinski, 2011).

El gusano parecía estar focalizado en las refinerías iraníes, ya que este tipo de malware está diseñado de forma muy específica para atacar una industria determinada y exige cierta disposición en las instalaciones físicas y electrónicas para poder ser corrompidas (Mueller & Yadegary, 2012). Esta teoría fue confirmada por un estudio realizado durante 2010, por Symantec, empresa encargada de la construcción y comercialización de software, principalmente de seguridad, en el cual se afirmó que la concentración de infecciones en Irán indicaba que éste era el objetivo inicial para las infecciones y donde se sembraron en un primer momento (Kerr, Rollins, & Theohary, 2012)

La guerra cibernética contra Irán, además de ser una de los más penetrantes y poderosas, tiene una característica que la identifica y convierte en una pionera para las guerras en el ciberespacio que se pueden presentar en el futuro: Fue una guerra que, usando medios cibernéticos, causó daños físicos. El alcance implica que la guerra ciberespacial ataca tres capas distintas: La capa de Tecnologías de la Información, que se usa para propagar el malware, la capa del Sistema de

Comando y Control que se usa para manipular los procesos de control y, finalmente, la capa física, donde se produce el daño real sobre las infraestructuras (Langner, 2013).

La innovación en este caso, es la capacidad de hacer daño a infraestructuras físicas, "reales". El incidente dañó casi 1.000 tubos de centrífuga en la instalación iraní de Natanz. Esta cifra es representativa si se compara con el número total de tubos instalados, que alcanzaba los 9000 y la porción de aquellos que estaban al servicio exclusivo y eran alimentados con uranio, que era un total de 4000. Se produjo una disminución del 23% en el número de centrifugadoras en funcionamiento desde mediados de 2009 hasta mediados de 2010 debido a Stuxnet (Gamero Garrido, 2014).

Una agresión como esta, forja una controversia importante respecto a la autoría de los hechos, y es por una cuestión muy sencilla, a pesar que casi todo apunta que fueron los Estados Unidos en colaboración con Israel, ambos Estados niegan de forma categórica su participación, y pretender acusar a uno de los países más poderosos en el Sistema Internacional y enfrentarse a él, es casi imposible. Algunos argumentos que apoyan y fortalecen la tesis sobre la responsabilidad por parte del país norteamericano, afirman que se generaron denuncias anteriores de los esfuerzos de Estados Unidos y otros gobiernos, incluido Israel, para sabotear el programa de centrifugado de Irán, socavando los sistemas eléctricos, sistemas informáticos y otras redes en las que se apoya a Irán, esto dicho por altos funcionarios de Estados Unidos y de gobiernos extranjeros (Kerr, Rollins, & Theohary, 2012).

Por otro parte, los reporteros Nakashima y Warrick (2012) al indagar con algunos funcionarios estadounidenses, afirman que la ciberguerra fue trabajo de Estados Unidos y

expertos israelíes bajo las órdenes secretas del presidente Obama, quien necesitaba frenar el progreso iraní frente a la construcción de una bomba atómica sin lanzar un ataque militar tradicional. Para un grupo de autores, el único Estado con los recursos económicos y tecnológicos y en la capacidad de llevar a cabo la guerra cibernética, la cual exige de la más alta ingeniería hasta la fecha, incluyendo creaciones como Stuxnet, es Estados Unidos (Geers, et. al, 2014).

David Sanger (2012) periodista estadounidense, a través de una búsqueda minuciosa de datos y entrevistas, se encargó de plasmar en su libro *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, la posibilidad de que el gobierno estadounidense haya estado detrás de toda la operación en la cual se llevó a cabo Stuxnet. Afirma que la idea era que las centrifugadoras quedaran fuera de servicio por un buen tiempo, y que las fallas fueran atribuidas al desgaste propio de los aparatos, al no ser de última tecnología, y ser propensos a dañarse. Para cumplir este objetivo se construyó una operación denominada Juegos Olímpicos, con dos intenciones básicas:

> La primera fue para paralizar, al menos por un tiempo, el progreso nuclear de Irán. La segunda, igualmente importante, era convencer a los israelíes de que había una forma más inteligente y elegante de lidiar con el problema nuclear iraní que lanzar un ataque aéreo, que podría escalar rápidamente en otra guerra en Oriente Medio, elevar los precios del petróleo e involucrar a todos los actores más volátiles de la región. (Sanger, 2012, pág. 190)

Si bien es claro que la relación entre Irán y Estados Unidos se encontraba bastante deteriorada y que la que existe con Israel es claramente tensa y conflictiva, ninguno de los dos Estados permite vislumbrar la menor posibilidad de aceptar las acusaciones, pues afirman que este tipo

de herramientas cibernéticas, más adelante pueden ser utilizadas en su contra, y no se prestarían para llegar a atmósferas de tal nivel.

El anterior, fue el recorrido de los principales escenarios de guerra cibernética que se han presentado en los últimos años, fueron escogidos precisamente porque fueron los de mayor alcance, representan los pasos más grandes en cuanto a innovación tecnológica y permitirán, de una forma ilustrativa, construir una relación con el concepto tradicional de guerra interestatal.

3. La Ciberguerra como una forma inédita de confrontación

La ciberguerra ofrece un escenario de innovación que si bien, está constituido por medios no tradicionales, permiten mejoras sustanciales para los Estados que estén en capacidad de manejar los avances en el entorno cibernético y retos para los que se encuentren bajo la influencia de la guerra en el ciberespacio.

Partiendo de la premisa de Clausewitz (2010) “La guerra es un verdadero camaleón, por el hecho de que en cada caso concreto cambia de carácter” (pág. 21), la ciberguerra es sencillamente la adaptación a los medios tecnológicos provistos por el ser humano en su afán de gobernar todos los medios a los cuales tiene acceso.

“Las guerras se libran en el contexto de su edad. Las armas que se utilizan para luchar en la guerra están determinadas a menudo por la tecnología prevaleciente” (Mehan, 2014, pág. 41); y en un mundo donde prevalece la interdependencia en todos los aspectos y donde la revolución tecnológica ha avanzado de forma descomunal, las armas cibernéticas sobresalen sobre las demás, por todas las prerrogativas que acarrean.

El ciberespacio se define como “un dominio global dentro del entorno de la información, cuyo carácter distintivo y único está enmarcado por el uso del espectro electrónico y electromagnético para crear, almacenar, modificar, intercambiar y explotar la información a través de redes interdependientes e interconectadas” (Kuehl, 2009, pág. 27); por lo que presenta particularidades que lo diferencian de otros dominios, y algunas de esas características hacen que este entorno sea muy llamativo para la guerra en él.

La guerra cibernética puede lograr la parálisis total de los sistemas de información de destino, funcionamiento intermitente de los mismos, errores acerca de la veracidad y robo de

información, vigilancia a través de sistemas invisibles, la toma de los centros de mando y control (Rattray, 2001), entre muchos otros daños, únicamente mediante medios magnéticos. La ciberguerra se puede llevar a cabo a través de operaciones en el ciberespacio, que tienen distintos fines y cada uno otorga ventajas excepcionales, que por otros medios, no se alcanzarían de una forma tan precisa.

Se clasifican en operaciones ofensivas, defensivas y de explotación (Turns, 2012). Las operaciones ofensivas son acciones que pretenden interrumpir, negar, degradar o destruir la información y los sistemas de control, en este caso, se habla de las acciones que pueden ejercer daño físico a la infraestructura crítica de un Estado. Las operaciones defensivas se adoptan para proteger, controlar, analizar, detectar y responder a actividades no autorizadas dentro de los sistemas cibernéticos públicos y privados de los Estados. Por último, las operaciones de explotación comprenden las capacidades de inteligencia, es decir, la recolección de información del contrario.

La guerra en el ciberespacio tiene el potencial de producir una gran perturbación social, económica y política, de una forma mucho menos cruel y desastrosa que las guerras anteriores. Además es inherentemente transfronteriza, al usar herramientas que desubican y hacen que las señales reboten, en un intento por ubicar la señal de origen; frustrando en muchos momentos, la asignación de culpabilidad en función de factores geográficos (Schmitt, 2012). Por otro lado, se salta el campo de batalla, es decir, como ahora casi todos los componentes institucionales y estructurales de los Estados están interconectados al ciberespacio y son accesibles desde él, se pueden atacar sin llegar a un campo de batalla físico y conseguir la derrota de las defensas tradicionales de un país (Clarke & Knake, 2010).

La ciberguerra no es perceptible a los sentidos, por lo que muchas veces no se alcanza a percibir su dimensión, alcance y peligrosidad, ya que todo transcurre en un entorno que no puede ser recorrido como los demás, y lo que se alcanza a distinguir es a través de códigos y fórmulas matemáticas, que impiden dimensionar su tamaño (Stel, 2014). El control del armamento que se usa en esta clase de guerra en el ciberespacio está, por supuesto, en manos de aquellos Estados en capacidad de desarrollar tecnologías para manejarlos, pero esa misma cualidad se convierte en un riesgo, los convierte en los actores más vulnerables, pues toda su infraestructura está conectada y los consecuencias de las ofensivas cibernéticas pueden ser mucho más dañinas al alcanzar más sectores esenciales para su correcto funcionamiento como Estado.

La guerra ciberespacial permite que el campo de batalla llegue a ser el corazón de un Estado, es totalmente posible llegar a la información y a las infraestructuras, sin necesidad de movilizar tropas a través de tierra, mar o aire. Y siendo la información un elemento clave en las guerras, la guerra cibernética ofrece ventajas sobre esta que no se pueden subestimar y sobrepasan las ya existentes: “La información es inmaterial, no pesa, carece de masa, no ocupa más que el espacio que ocupa en sus sistema de almacenamiento, se puede modificar, alterar o convertir en decimas de segundos” (López de Turizo y Sánchez, 2012, pág. 139). Manejar la información se convierte entonces, en una fuente de poder, y esta se transforma en un objeto primordial para atacar y conseguir.

La responsabilidad es otro de los aspectos que hacen llamativa la ciberguerra al ofrecer carácter de anonimato, lo que hace que sea muy difícil identificar a los actores detrás de los las acciones en el ciberespacio (Cyber Defense & Network Security, 2013), por lo tanto, la

atribución de culpabilidad a un determinado Estado sigue siendo uno de los retos más difíciles para quien se encuentra bajo los efectos del mismo y exige que los Estados mejoren sus capacidades de identificación y rastreo (Heintschel Von Heinegg, 2012).

Aparte de las características exclusivas mencionadas, además la ciberguerra ofrece un acceso desde cualquier lugar del mundo, siempre y cuando se cuente con la tecnología adecuada, la dificultad de la localización proporciona seguridad para el atacante, es tremendamente eficiente y tienen un rango de rendimiento muy alto, pues los avances tecnológicos permiten que los elementos tecnológicos que se usen se puedan reproducir y reemplazar con facilidad y a bajos costos y se pueden lanzar muchos acciones perjudiciales desde un solo equipo operativo. El alcance de la ciberguerra en la actualidad es casi ilimitado, gracias a los satélites de cobertura global que alcanzan todos los rincones del planeta; coordinar para los encargados de caminos que van a tomar a través del ciberespacio es mucho más fácil gracias a la conectividad y a las características propias de la comunicación en la era moderna (López de Turizo y Sánchez, 2012).

"Una acción en el ciberespacio bien organizada, coordinada y dirigida puede dejar inutilizado los sistemas de comunicación, sus infraestructuras críticas, su capacidad de mando y control; lo que produciría una desestabilización" (pág. 143), y qué puede llegar a ser más importante que desestabilizar y acabar con la voluntad del adversario de la forma más eficiente posible, es el fin mismo de la guerra.

4. La Ciberguerra en un contexto de Guerra Interestatal Clásica

Si definir guerra interestatal ha generado dificultades al existir una multiplicidad de definiciones, siendo una realidad que acompaña a las sociedades desde su aparición, evolución y

organización; la ciberguerra se convierte en un fenómeno un tanto más complejo, pues se refiere a un escenario que no es palpable ni cercano como escenario de enfrentamientos para la gran mayoría de personas, además, como temática no ocupa la realidad mundial hace más de un siglo e implica un espacio que es bastante novedoso.

Si bien la construcción teórica especializada en el ciberespacio se viene realizando desde hace menos de 30 años, en una forma juiciosa, muchos de los acontecimientos, en este caso, lo que sucedió en Estonia, Georgia e Irán; pueden encajar en los conceptos tradicionales de guerra, haciendo la salvedad en ciertas adaptaciones a las particularidades que presenta el ciberespacio, como se han hecho a su vez, con los demás contextos en los que se ha desarrollado la guerra. Esta aclaración es trascendental, porque la ciberguerra presenta rasgos muy característicos que por supuesto no pueden ser catalogados dentro de la guerra convencional, pero que no obligan a los conceptos, por ningún motivo, a estar en oposición.

La ciberguerra, desde una conceptualización teórica, puede ser definida por una gran cantidad de autores que se han apropiado de los asuntos cibernéticos. Maness y Valeriano (2012) definen la ciberguerra como "las capacidades y acciones ofensivas en el ciberespacio de un Estado (…) El uso de las tecnologías computacionales en el campo de batalla militar y diplomática de los asuntos y la interacción internacional" (pág. 142). Para Schreir (2012) la guerra cibernética "se refiere a un asalto digital coordinado de forma masiva de un gobierno a otro. Es la acción de un Estado-nación para penetrar las redes y los ordenadores de otra nación con el fin de causar daños o molestias" (pág. 16).

La noción política se incluye, al afirmar que:

> La guerra cibernética es una extensión de la política a través de las acciones tomadas en el ciberespacio por parte de actores estatales que o bien constituyen una grave amenaza para la seguridad de una nación o se llevan a cabo en respuesta a una amenaza percibida contra la seguridad de una nación (Ruef, Shakaraian & Shakarian, 2013, pág. 2).

Estas definiciones, comparadas con las características de la guerra interestatal clásica, son de gran semejanza; siguen siendo determinadas por actores estatales, exigen la profesionalización de las Fuerzas Militares y el apoyo de la población civil, su fin principal es ejercer la voluntad propia sobre el otro y su principal motivación es meramente política, tal vez la principal diferencia son los medios por los cuales se alcanza el objetivo principal. Y estas semejanzas las afirman Friedman y Singer (2014) pues los elementos clave de la guerra en el ciberespacio, tienen sus paralelismos y conexiones a la guerra en otros dominios. Sea la guerra en tierra, en el mar o en el aire, o ahora en el ciberespacio, siempre tiene un objetivo político, que la distingue de la delincuencia.

La ciberguerra que alcanzó a Estonia, Georgia e Irán, cabe en las características de la guerra interestatal. A continuación se explica el porqué. En primer lugar, los acontecimientos que tuvieron lugar en estos Estados fueron motivados por cuestiones absolutamente políticas; como segundo punto, las singularidades de la guerra en el ciberespacio potencializan las características ya determinadas de la guerra interestatal tradicional.

Con respecto al primer punto, el fin político, dicho por Clausewitz (2010) “la guerra entre naciones enteras, y particularmente entre naciones civilizadas, surge siempre de una circunstancia política, y no tiene su manifestación más que por un motivo político. Es, pues, un acto político” (pág. 19). Es claro que el fin es el logro político, el medio la guerra.

Lo que sucedió en Estonia “parece ser la primera vez en que [la ciberguerra] estuvo dirigida contra de una nación, como instrumento coercitivo en un conflicto político” (Schdmit, 2013, pág. 1); pues la situación entre Rusia y su excompañero de la URSS ya era bastante tensa, y la guerra en el entorno cibernético se produjo en un entorno de crecientes divergencias entre el gobierno y la minoría étnica rusa que habita Estonia, exacerbado por el problema generado por el movimiento del monumento ruso.

La guerra clásica debe tener un objetivo político claramente definido, decisivo y alcanzable, el cual se alcanzará a través de los elementos que constituyen el poder de una nación y las distintas acciones y decisiones que se tomen con el transcurrir del conflicto (Sohr Biss, 2003). Entre los tres casos presentados anteriormente, no existe mejor ejemplo de lo mencionado, que Georgia. El objetivo era muy claro: Resolver los conflictos territoriales, frente a la invasión de Osetia y mostrar al gobierno georgiano como incompetente; y en este caso, fue la ciberguerra que acompañó el enfrentamiento físico, por lo que el tinte político resalta aún más:

> Las operaciones en el dominio cibernético realizadas por la cibermilicia rusa apoyaron el esfuerzo por negar y degradar la capacidad del gobierno de Georgia para comunicarse, tanto internamente como con el mundo exterior. A través de este esfuerzo, combinado con otros esfuerzos en el dominio físico, por ejemplo la invasión indiscutible del terreno en el oeste, el bloqueo naval y de bombardeo de áreas alrededor del oleoducto; los rusos fueron capaces de demostrar que el gobierno de Georgia fue incapaz de defender su soberanía territorial, tanto en los dominios físicos como en el ciberespacio. (Hollis, 2011, pág. 5)

En el caso específico de Irán, las plantas de tratamiento de uranio representaban en su momento, una amenaza tanto para la estabilidad política de la región y un contrincante serio en

la carrera de la energía nuclear para las potencias nucleares; en este caso, la relación de fricción con Israel es más que conocida, además de la renuencia del país hacía el manejo de las tecnologías nucleares por parte de Irán; y además Estados Unidos no podía perder el control sobre el manejo de una de las energías más peligrosas y valiosas, en regiones contrarias a su pensamiento político y de vital importancia geoestratégica como fuente de petróleo. “La crisis entre EE.UU. e Irán tiene su origen en el programa nuclear de la República Islámica” (RT, s.f.). EE.UU. siempre sospechó que Teherán utilizaba el programa como cortina de humo para fabricar armas nucleares en secreto y por su parte, Irán rechaza estas acusaciones, al defender los fines pacíficos de su programa.

Reconociendo que la esencia de la guerra clásica interestatal es su objetivo político, un segundo momento permitirá exponer que existen otras características de la guerra interestatal que son claramente visibles en las acciones de guerra cibernética. Por supuesto es más que obvio, que debe ser llevada a cabo exclusivamente entre Estados; y en los tres casos sucedió de tal manera. Los Estados, en su afán de conseguir los objetivos que establecieron decidieron actuar, en esta ocasión por medios cibernéticos.

La constante evolución de los enfrentamientos bélicos que se han presentado entre Estados y sus alcances, han obligado a la humanidad a buscar formas más eficientes y menos crueles que las anteriores, pero que igual tengan el efecto de sobreponer la voluntad propia sobre las demás. La ciberguerra es un muy buen medio de conseguir esto; si bien, puede llegar a ser altamente destructiva, otorga mayor precisión y se adapta mejor a las necesidades del atacante. Por ejemplo, si el interés en Estonia era ejercer presión, un ataque terrestre estaría completamente sobredimensionado, y habría generado aún más problemas que posibles soluciones; mientras que

las actuaciones contra las páginas web de sectores importantes y valiosos para el gobierno y los sectores económicos más importantes, fue el precedente que querían sentar, y un abrebocas de lo que puede llegar a suceder si se enfoca en una estructura aún más crítica.

En el caso Stuxnet, Israel siempre se ha mostrado contrario a la proliferación del armamento cibernético en su región, pues considera amenazada su existencia como país. Buscando detener estos procesos de enriquecimiento nuclear, ha llevado a cabo ataques aéreos preventivos por sorpresa contra reactores en Irak, Siria y Sudán, entre otros. El problema con Irán era que su ruta área era mucho más larga, además debería sobrevolar naciones neutrales y sus instalaciones de enriquecimiento se encuentran bajo tierra. Si bien era una operación militarmente posible, podría tener más costos que beneficios, dado el riesgo operativo y el coste político. (Sánchez Medero, 2012); por lo tanto, el gusano cibernético se convirtió por supuesto en su mejor opción, a menores costos, siendo la primer acción de guerra ciberespacial que realmente causo daños físicos; en muchos casos, es más eficiente que un ataque terrestre, marítimo e incluso aéreo.

La característica del daño físico es vital, pues si con anterioridad no se había alcanzado, el perjuicio a las centrifugadoras demostró la capacidad de interferir en el funcionamiento de infraestructuras reales, exclusivamente por medios cibernéticos. Desde Sun Tzu (1999) se habla del ataque a los sectores críticos y vitales de los otros Estados, para ganar las guerras: “Ataca inesperadamente, haciendo que los adversarios se agoten. Interrumpe sus provisiones, arrasa sus campos y corta sus vías de aprovisionamiento. Aparece en lugares críticos y ataca donde menos se lo esperen” (pág. 18). Por lo tanto, y viviendo en una época como la actual donde casi todos los países desarrollados tienen sus principales industrias y entidades públicas y privadas conectadas a través de medios cibernéticos, el ataque a las infraestructuras críticas puede generar

efectos devastadores. Queda claro cuando un país como Estonia, ve todas sus redes desmoronarse por algún tiempo, desajustadas exclusivamente a través de medios cibernéticos, y pierde económicamente, al encontrar colapsados sus principales entidades financieras; e Irán, ve como, a través de una USB, meses, e incluso años de avances tecnológicos en el enriquecimiento de uranio se ven retrasados.

La información ha sido siempre un componente vital de las guerras interestatales, y de nuevo Sun Tzu (1999) lo recalca. Afirma que no conocer la situación de los adversarios por economizar gastos en investigar y estudiar al otro es extremadamente inhumano, y no es típico de un Estado victorioso. Por lo tanto, para vencer a los demás y lograr triunfos extraordinarios la información es esencial y no se deben escatimar gastos para obtenerla. Y la guerra cibernética mejora el proceso de consecución de la información, ya sea a través del ciberespionaje o de la inteligencia.

El ciberespionaje utiliza ordenadores o sistemas relacionados que recogen información o realizan ciertas operaciones. A diferencia de la delincuencia cibernética, en la que los incidentes normalmente están motivados financieramente, el espionaje cibernético es más probable que tengan efectos estratégicos que amenazan franjas más amplias de la sociedad. Las motivaciones pueden variar, pero incluyen el logro de ventajas militares, políticas, industriales o tecnológicas. (Lord & Sharp, 2011, pág. 17)

El caso perfecto para ejemplificar el uso de herramientas cibernéticas en la búsqueda de información es Georgia. La ciberguerra que se lanzó no fue diseñada solamente para controlar el flujo de información en las páginas web nacionales o deformar la percepción de las personas respecto a lo que encontraban en Internet, también ayudaron a la filtración de información sobre

inteligencia militar y política georgiana, para las autoridades rusas (Cyber Committee of AFCEA, 2012)

La sociedad civil juega un papel vital en la guerra interestatal clásica, pues representa legitimidad para la misma, y su participación es transcendental como soporte a las acciones realizadas en el ciberespacio por los Estados, y estos han comenzado a usar grupos civiles con amplios conocimientos en cibernética, les otorgan apoyo económico y obtienen un accionar en nombre de sus gobiernos (Andres, 2012). Estonia es la realización de esta característica en su máxima expresión, pues la responsabilidad fue asumida por un grupo de jóvenes que había sido respaldada con anterioridad por el gobierno ruso.

La guerra clásica está compuesta por dos actividades que deben trabajar en conjunto: la táctica y la estrategia. La primera se refiere a "preparar y conducir individualmente los enfrentamientos, y la segunda a combinarlos unos con otros para alcanzar el objetivo de la guerra" (Clausewitz, 2010, pág. 54). Las acciones en la guerra cibernética lanzada por Rusia a Georgia vuelven a sobresalir en este caso, al unir las acciones en tierra y mar, con aquellas realizadas en el entorno cibernético, siendo cada una preparada por los profesionales de su área, mostraron un avance tanto táctico como estratégico por parte de los rusos.

Una característica transcendental de la guerra, reconocida tanto por Clausewitz como por Sun Tzu es la sorpresa al momento de atacar. La sorpresa para el autor prusiano es "la base de todas las iniciativas, porque sin ella no cabe concebir que se cree una superioridad en el punto decisivo" (Clasewitz, 2010, pág. 118). Es un medio que debe ser secreto y rápido, lo que permite alcanzar superioridad, tanto física como moral al permitir la generación de daños inesperados en

las infraestructuras, confundiendo y desalentando a los enemigos y minando su resistencia y fuerza de voluntad.

Por su parte Sun Tzu (1999) afirma que la victoria puede crearse a partir de un actuar sorpresivo, ya que si el adversario no sabe ni la fecha ni el lugar donde se realizará el ataque, no tendrá la menor idea de cómo afrontarlo. Su pensamiento se basa en que el atacante no tenga forma, es decir, que sea tan sutil y silencioso que no exista la menor posibilidad de ser descubierto, porque no saben cómo es ni cómo pretende atacar. Ambos autores concuerdan con que la sorpresa debe ser rápida y secreta para alcanzar sus objetivos.

Por supuesto los tres casos son un fiel reflejo de qué es la sorpresa y lo influyente que puede ser al realizar la guerra por medios cibernéticos. Irán, Estonia y Georgia jamás esperaron ver sus infraestructuras virtuales o físicas bajo un contundente desbarajuste cibernético. La sorpresa encuentra en la ciberguerra una serie de ventajas sin precedentes, pues su capacidad de sigilo y rapidez ha sido nunca antes vista. Las acciones en el ciberespacio se producen de un momento a otro y solo se necesita un par de segundos para viajar a través de las redes, y la interdependencia a nivel global, facilita su viaje. Además si llega a producir algún ruido, será a través de las alarmas de protección de software, y si está muy bien diseñado o encuentra vulnerabilidades desconocidas para el programador que será atacado, puede pasar completamente desapercibido, y solo será notorio cuando haya logrado su cometido.

Por supuesto la constante evolución de la tecnología también hace mella, y aún más en el siglo XXI, donde los avances son cada vez más rápidos y constantes; gracias a la curiosidad del ser humano y a todos los pasos que ha dado para facilitar su supervivencia. La tecnología es un

factor de primera línea en los conflictos (Sohr Biss, 2003); y las necesidades de las guerras han conducido a los hombres a efectuar invenciones particulares con el fin aprovechar sus ventajas. Como consecuencia de estos hallazgos, el combate ha experimentado grandes cambios (Clausewitz, 2010). Este argumento reafirma que la guerra, en su esencia y en sus características no ha variado; y que los acontecimientos en la ciberguerra se amoldan a la guerra interestatal.

Conclusiones

La principal característica de la humanidad es que se encuentra en constante evolución, y está siempre acompañada de fenómenos y estructuras que la ayudan en su ardua tarea de estructurarse como sociedad. La guerra, es sin lugar a dudas, una de las realidades que más ha permitido al ser

humano conocerse, identificar sus alcances y esculpirse de tal manera que sus operaciones ofensivas sean cada vez sea más contundente, pero menos atroces.

Los progresos tecnológicos de la modernidad, le presentaron a los hombres, hace menos de 100 años, un escenario completamente nuevo, pero que, como los demás, exigía toda su capacidad intelectual y de innovación para manejarlo. El ciberespacio se convirtió en el nuevo dominio, que si bien representaba un reto, significó lo mismo que los demás, una inmensa curiosidad que le permitiera construir herramientas a la sociedad para actuar sobre él, como cuando tuvo que construir carruajes, carretas, automóviles y tanques para recorrer la tierra; barcos, buques y submarinos para alcanzar soberanía sobre el entorno marítimo; y una gran variedad de aeronaves para surcar el cielo.

Es claro que no se puede hablar del mismo tipo de instrumentos para la administración del ciberespacio, porque el hombre no pueda caminar, nadar o volar a través de él; pero si puede manejarlo, y se convierte en un escenario donde la precisión, el sigilo y la velocidad reinan y la guerra encuentra un aliado que le permitirá actuar de una forma mucho más libre, precisa y eficiente.

Los acontecimientos de guerra cibernética que se han presentado en los casos mencionados son el fiel reflejo de la voluntad humana para mejorar sus capacidades y conseguir mayores beneficios a menores costos. Estonia refleja el primer intento plausible de lo que puede llegar a ser la ciberguerra; si bien no hubo destrucción de estructuras físicas, es una primera advertencia de la capacidad de manejar, de forma remota, sus redes y de presentar mensajes que pueden ejercer presiones económicas y sociales.

El caso de Georgia presentó novedades que pueden ser lecciones para el futuro. Acompañar las campañas terrestres de maniobras en el ciberespacio, fue una forma muy inteligente de, en primer lugar, mostrar que los georgianos no estaban en capacidad de protegerse en ninguno de sus dominios y que su soberanía se veía totalmente destruida, acción que no solo tendría efecto físico, también alcanzaría la moral tanto del gobierno, como de la población, pues crecería la incertidumbre y la vulnerabilidad a la cual se encontraban sometidos sería un gran golpe sicológico.

Irán es un caso memorable, porque es el primero en el cual se alcanza un daño físico real por medios exclusivamente tecnológicos a través del ciberespacio. Aquí es donde se alcanza un poco a dimensionar lo que realmente es capaz de hacer la ciberguerra y los Estados empiezan a reconocer la extensión de la nueva amenaza a la que se enfrentan. La infraestructura deja de ser simplemente un componente del Estado, y se vuelve un centro de gravedad, para los Estados en su necesidad de defenderla y en su posibilidad de atacarla.

Hablar de guerra cibernética es hablar de guerra interestatal por otros medios, por medios que demuestran el avance en las capacidades del ser humano para manejar los fenómenos que lo acompañan. Son conflictos entre actores estatales, que ponen a disposición de la ciberguerra todos sus recursos y que lo único que pretenden es sobreponer su voluntad sobre el otro. Donde la política sigue jugando un rol fundamental y mientras más crecen las competencias, lo hacen a su lado las vulnerabilidades.

Es claro que no se pueden desestimar las novedades que acarrea hablar de guerra cibernética, pero no alcanza la connotación de un nuevo tipo de guerra, simplemente es el uso de nuevos

métodos, para conseguir los mismo fines; y está claro, que la guerra tiene permitido el uso de las técnicas que sean necesarias, con el fin de conseguir su propósito, siempre político. Los acontecimientos en Estonia, Georgia e Irán presentan elementos comunes, que se pueden considerar propios de las guerras interestatales, y la teoría de guerra convencional es pertinente para la evaluación de las causas, los efectos y las consecuencias que puede generar la ciberguerra; esta persigue el mismo fin último, y potencializa muchas de las particularidades propias de la guerra.

REFERENCIAS

Andres, R. (2012) The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence. En: *D. Reveron. Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World (pp. 89 – 104)* Washington, Estados Unidos: Georgetown University Press.

Aron, R. (1966) Peace and war; a theory of international relations. New York, Estados Unidos: Praeger.

Ashmore, W. (2009) Impact of Alleged Russian Cyber Attacks. En: *Baltic Security & Defence Review 11,* pp. 4 – 40.

Barbé, E. (1987) El papel del realismo en las Relaciones Internacionales. En: *Estudios Políticos (57),* pp. 149 – 176.

Barringer, R. (1972) War: patterns of conflict. Cambridge, Massachusetts: MIT Press.

Bernard, L.L. (1944) War and Its Causes. New York, Estados Unidos: Henry Holt.

Bonstra, J. (2008) Georgia y Rusia: Una guerra corta con consecuencias prolongadas. Comentario FRIDE. Recuperado el 15 de Febrero de 2016, de http://fride.org/download/COM_Georgia_Rusia_ESP_agust08.pdf

Carr, J. (2009) Inside Cyber Warfare. California, Estados Unidos: Mike Loukides.

Castells, M. (2006) La sociedad red: Una visión global. Madrid, España: Alianza Editorial.

Clarke, R. & Knake, R. (2010) Cyber War: The Next Threat to National Security and What to Do About It. New York, Estados Unidos: Harper-Collins Publishers.

Clausewitz, C. (2005) De la Guerra. Madrid, España: La esfera de los libros.

Coleman, K. (2008, Enero 28) Coleman: The Cyber Arms Race Has Begun. *CSO.* Recuperado el 20 de Enero de 2016, de http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html

Corbin, K. (2009, Marzo 12) Lessons From the Russia-Georgia Cyberwar. InternetNews.com Recuperado el 10 de Marzo de 2016, de http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm

Cyber Committee of AFCEA (2012) The Russo-Georgian War 2008: The Role of the cyberattacks in the conflict. Fairfax, Virginia, Estados Unidos: AFCEA.

Cyber Defence & Network Security (CDANS) (2013) Cyber Defence & Network Security 2013 Post Show Repost. Londres, Inglaterra: Cyber Defence & Network Security (CDANS).

Departamento de Defensa (2006) The National Military Strategy for Cyberspace Operations. Washington D.C., Estados Unidos: Charmain of the Joint Chiefs of Staff.

Farwell, J. & Rohozinski, R. (2011, Febrero – Marzo) Stuxnet and the Future of CyberWar. En: *Survival 53(1),* pp. 23 – 40.

Franco Suanzes, F. J. (2000) Gaston Bouthoul. La guerra como función social. En: *Cuadernos de Estrategia (111),* pp. 57 – 91.

Friedman, A. & Singer, P. W. (2014) Cybersecurity and Cyberwar: What everyone needs to know. New York, Estados Unidos: Oxford University.

Gamero Garrido, A. (2014) Cyber Conflicts in International Relations: Framework and Case Studies. Massachusetts, Estados Unidos: Universidad de Harvard.

Geers, K., Kinlund, D., Moran, N. & Rachwald, R. (2014) WORLD WAR C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. California, Estados Unidos: FireEye.

Harrison, R. (1973) Warfare. Minneapolis, Estados Unidos: Burgess Publ. Co

Heintschel Von Heinegg, W. (2012) Legal Implications of Territorial Sovereignty in Cyberspace. En: *C. Czosseck, R. Ottis & K. Ziolkowski (eds.) 4th International Conference on Cyber Conflict. (pp. 7 – 20).*Tallin, Estonia: NATO CCD COE Publications.

Herzog, S. (2011, Junio) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. En*: Journal of Strategic Security 4(2),* pp. 49 – 60.

Hollis, D. (2011, Enero) Cyberwar Case Study: Georgia 2008. En*: Small Wars Journal 6(1)*

Iasiello, E. (2013) Cyber Attack: A Dull Tool to Shape Foreign Policy. En: *M. Maybaum, K. Podins & J. Stinissen, (Eds.) 2013 5th International Conference on Cyber Conflict (pp. 451 – 468)* Tallin, Estonia: NATO CCD COE Publications.

Kallen, H. (1939, Septiembre) Of war and peace. En: *Social Research: An International Quarterly 6(3),* pp. 361 – 391.

Kastenberg, J. & Korns, S. (2009) Georgia's Cyber Left Hook. En: *Parameters,* pp. 60 – 76.

Keohane, R. & Nye, J. (2011) Power and Interdependence, 4ta edición. Londres, Inglaterra: Longman.

Kerr, P.; Rollins, J. & Theohary, C. (2012, Diciembre) The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. En: *CRS Report for Congress*. Washington D.C., Estados Unidos: UNT Digital Library.

Kozlowski, A. (2014, Febrero) Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. En: *European Scientific Journal 3,* pp. 237 – 245

Kuehl, D. (2009). Cyberspace and Cyberpower. En *F. Kramer, S. Starr, & L. Wentz, Cyberpower and National Security (págs. 26 - 43).* Washington D.C., Estados Unidos: Potomac Books.

Langner, R. (2013) To Kill a Centrifuge A Technical Analysis of What Stuxnet's Creators Tried to Achieve. Arlington, Estados Unidos; The Langner Group.

Libicki, M. (2009) Cyberdeterrence and Cyberwar. Santa Mónica, California: RAND Corporation.

Lider, J. (1977) On the Nature of War. Westmead, Australia: Saxon House.

López de Turizo y Sánchez, J. (2012, Febrero) La evolución del conflicto hacia un nuevo escenario bélico. En: *El Ciberespacio: Nuevo escenario de confrontación 126,* pp. 117 – 167.

Lord, K. & Sharp, T. (2011) America's Cyber Future. Security and Prosperity in the Information Age Volume I. Washington, D.C., Estados Unidos: Center of New American Security.

Malinowski, B. (1941) An anthropological analysis of war. En: *Amer. J. Sociol (46),* pp. 521-550.

Maness, R. & Valeriano, B. (2012) Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare. En: D. *Reveron. Cyberspace and National Security: Threats, Opportunities and Power in a Virtual World (pp. 139 – 157)* Washington, Estados Unidos: Georgetown University Press.

Mehan, J. (2014) Cyberwar, Cyberterror, Cybercrime and Cyberactivism. (2 ed). Cambridge, Massachusetts: IT Gobernance.

Melzer, N. (2011). Cyberwarfare and International Law. Ginebra, Suiza: United Nations Institute for Disarmament Research.

Mindell, D. A. (2000). Cybernetics: Knowledge domains in Engineering systems. Massachusetts, Estados Unidos: Massachusetts Institute of Technology.

Molina Cano, J. (2014) Gaston Bouthoul y el fenómeno-guerra. En: *Revista Brasileira de Estudos Políticos (109),* pp. 197-224

Mueller, P. & Yadegary, B. (2012) The Stuxnet Worm. Informe Computer Security. Arizona, Estados Unidos; The University of Arizona.

Nakashima, E. y Warrick, J. (2012, Junio 2) Stuxnet was work of U.S. and Israeli experts, officials say. The Washington Post. Recuperado el 15 de Marzo de 2016, de https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Naroll, R. (1964) On ethnic unit classification. En: *Current Anthropol (5),* pp. 283-312

Otterbein, K.F. (1970) The Evolution of War: A Cross-Cultural Study. New Haven, Estados Unidos: HRAF Press

Pardo, R. & Tokatlian, J. G. (1990). La teoría de la interdependencia: ¿Un paradigma alternativo al realismo? En: *Estudios Internacionales*, pp. 339-382.

RAND Corporation (s.f.) Cyber Warfare. RAND Corporation. *www.rand.org.* Recuperado el 10 de Febrero de 2016, de http://www.rand.org/topics/cyber-warfare.html

Rattray, G. (2001) Strategic Warfare in Cyberspace. Massachusetts, Estados Unidos: The MIT Press.

Rosenzweig, P. (2013) Cyber Warfare How Confl icts in Cyberspace Are Challenging America and Changing the World. California, Estados Unidos: PRAEGER.

RT (s.f.) EE. UU. vs. Irán. RT.com Recuperado el 20 de abril de 2016, de https://actualidad.rt.com/themes/view/44189-eeuu-vs-iran

Ruef, A., Shakarian, J. & Shakarian, J. (2013) Introduction to Cyber-Warfare: A multidisciplinary approach. Massachusetts, Estados Unidos: Elsevier.

Sáez Collantes, L. F. (2012) La ciberguerra en los conflictos modernos. Santiago de Chile, Chile. Recuperado el 15 de Marzo de 2016, de https://www.academia.edu/9339213/LA_CIBERGUERRA_EN_LOS_CONFLICTOS_MODERNOS

Sanger, D. (2012) Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power. New York, Estados Unidos: Brodway Books.

Schdmit, A. The Estonian Cyberattacks. (2013) En: *J. Healey (Ed.). The fierce domain – conflicts in cyberspace 1986-2012.* Washington D.C., Estados Unidos: Atlantic Council.

Schmitt, C. (2014) El concepto de lo político (2da. edición). Madrid, España: Alianza Editorial.

Schmitt, M. (2012) Classification of Cyber Conflict. En: *Journal of Conflict & Security Law 17(2)*, pp. 245–260

Schmitt, M. (2013) Tallinn Manual on the International Law applicable to Cyber Warfare. Cambridge, Inglaterra: Cambridge University Press.

Schreier, F. (2012) On Cyberwar. Ginebra, Suiza: DCAF.

Shakarian, P. (2011, Abril) Stuxnet: Cyberwar Revolution in Military Affairs. En: *Air & Space Power Journal*, pp. 50 – 59.

Sohr Biss, R. (2003) Claves para entender la guerra. Santiago de Chile, Chile: Random House Mondadori S.A.

Sorel, G. (1912) Réflections sur la violence. Paris, Francia: Rivière.

Stel, E. (2014). Seguridad y Defensa del Ciberespacio. Ayacucho, Perú: Editorial Dunken.

Tzu, S. (1999) El Arte de la Guerra. Bogotá D.C., Colombia: Editorial Panamericana.

Van der Dennen, J. (1995) The origin of war: the evolution of a male-coalitional reproductive strategy. Michigan, Estados Unidos: Universidad de Michigan.

Van der Dennen, J. (2016) On war: Concepts, Definitions, Research Data: A short literature review and bibliography. Recuperado el 15 de Abril de 2016, de https://www.researchgate.net/publication/30469766_On_war_Concepts_Definitions_Research_Data_A_short_literature_review_and_bibliography

Wright, Q. (1965) A Study of War. Chicago, Estados Unidos: University of Chicago Press.