UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES
RELACIONES INTERNACIONALES

Ciberguerras en el siglo XXI:
El conflicto ruso-georgiano y sus efectos en la reconfiguración de la noción de seguridad.

T E S I S

QUE PARA OBTENER EL GRADO DE

Licenciado en Relaciones Internacionales.

P R E S E N T A:

LUIS GUILLERMO LARA ESTRADA

DIRECTOR

MTRO. MARCO ANTONIO LOPÁTEGUI TORRES

MÉXICO, D.F., ABRIL DE 2014.

"Me fui a los bosques porque quería vivir sin prisa. Quería vivir intensamente y sorberle todo su jugo a la vida. Abandonar todo lo que no era vida, para no descubrir, en el momento de mi muerte, que no había vivido." ***H.D. Thoreau***

Dedicatoria

A mi familia: amorosa, *paciente* y de extraordinarios consejos…

A mis profesores, hombres y mujeres que retribuyen a la sociedad con sus *excepcionales* conocimientos…

A los *verdaderos* amigos, esos que se cuentan con los dedos de las manos…

Agradecimientos

A la máxima casa de estudios: "*Por mí raza hablará el espíritu*"…

A la Facultad de Ciencias Políticas y Sociales, *cuna de los grandes pensadores sociales del país…*

Ciberguerras en el siglo XXI:

El conflicto ruso-georgiano y sus efectos en la reconfiguración de la noción de seguridad.

Índice

Introducción.

> *"Las guerras del futuro se librarán mediante expertos en telecomunicaciones en habitaciones como esta y no con soldados desfilando por las calles o tanques o aviones de combate."* Philip Hammond, Ministro de Defensa de Reino Unido, en entrevista con *The Mail.*[1]

Hasta hace poco tiempo, las batallas en el ciberespacio parecían estar relegadas a películas y libros de ciencia ficción; sin embargo, recientemente estos conflictos comienzan a consolidarse como un instrumento capaz de dañar significativamente a la población e infraestructura de un Estado, convirtiéndose así en una amenaza palpable digna de atención nacional e internacional.

En este sentido, este trabajo parte de la hipótesis de que este nuevo tipo de fenómeno bélico es posible a partir de dos grandes hechos que se han desarrollado en los últimos tiempos: en primer lugar, encuentra una explicación en los grandes avances que ha experimentado la tecnología en los últimos años, en específico en aquellos campos relacionados con la computación, el desarrollo de aplicaciones, la Internet y con los dispositivos de comunicación, así como con el uso y sentido que le ha conferido el ser humano a estas herramientas; en segundo lugar, se debe también al nuevo ambiente alentado por el último modelo de conflicto conocido, el de las nuevas guerras, mismo que es producto de las diversas mutaciones que ha sufrido este portento a lo largo de la historia debido a las cambiantes condiciones del entorno social, político, económico y hasta técnico. Ambos elementos confluyeron de manera explícita en el conflicto librado entre Georgia y Rusia en el año 2008, durante el cual se emplazó una batalla virtual directa que puso en evidencia la capacidad destructiva de este nuevo tipo de agresiones, hecho que a

[1] Simon Walters, *Hammond's £500m new cyber army: as he reveals top-secret Whitehall bunker for the first time, Defence Secretary says future wars will be fought with viruses*, [en línea], The Mail Online, 28 de septiembre de 2013, Dirección URL: http://www.dailymail.co.uk/news/article-2436946/Hammonds-500m-new-cyber-army-As-reveals-secret-Whitehall-bunker-time-Defence-Secretary-says-future-wars-fought-viruses.html, [consulta: 15 de noviembre de 2013]. Traducción propia.

su vez repercutió en la noción de seguridad –nacional e internacional- que se tenía hasta aquel entonces: a partir de ese momento, los Estados comenzaron a agregar a su agenda el tema de la ciberseguridad, ampliando así al espectro de amenazas que tradicionalmente eran consideradas como críticas para su supervivencia en el entorno internacional.

Con esto aclarado, huelga decir que tras el conflicto de 2008 este novedoso método bélico - conocido entre los especialistas como ciberguerra- y su múltiple arsenal de armas y técnicas virtuales de agresión se han convertido en un instrumento estándar para utilizarse dentro de los conflictos actuales, generando un enorme ahorro de recursos –económicos y humanos- al Estado agresor así como una gran cantidad de daños políticos, estratégicos y materiales al país agredido. De la misma forma, y como ya se mencionó, es justamente a partir de este año cuando comienzan a surgir alrededor del mundo diversos planteamientos, tanto nacionales como mundiales, que intentan contener la dispersión de nueva forma de guerra o cuando menos regularla para evitar la total militarización de un terreno que hasta hace poco era utilizado de forma totalmente pacífica por todas las personas que habitan en la Tierra: el ciberespacio.

Debido a todo este escenario y a la enorme trascendencia que éste representa para Relaciones Internacionales, este trabajo tiene por objetivo analizar a fondo a este nuevo fenómeno de guerra -el de las ciberguerras- así como el impacto que el mismo ha provocado sobre la concepción que hasta el momento se tenía sobre la seguridad, término de gran relevancia para esta misma disciplina, sin perder de vista en todo momento la hipótesis antes planteada. Para lograr su cometido, este escrito se estructura en 4 capítulos que se entretejen para dar una explicación sobre este nueva amenaza virtual que se tiende sobre el mundo así como los alcances que tuvo hasta el momento en que se concluyó esta investigación.

El primer capítulo, titulado “La evolución histórica de la guerra y la transformación del Estado”, ofrece al lector un marco referencial para comprender el escenario donde se desarrollan actualmente estas ciberbatallas, es decir, el de las nuevas guerras. Sin embargo, para llegar hasta este último modelo de conflicto se realiza un recorrido a través de la historia de la guerra con el fin de comprender las mutaciones que ha sufrido a través del tiempo y que desembocaron en lo que diversos especialistas llaman *new wars*. Dicho trayecto analítico comprende diversas etapas, entre las que destacan la de los conflictos premodernos, la de la Guerra Clásica, la de la Guerra Total y, finalmente, la de las nuevas guerras: en este sentido, las características y autores más relevantes de cada uno de estos periodos es explicado de forma breve en cada subsección. Asimismo, paralelo a este análisis se agregan las diversas transformaciones que ha sufrido el Estado a partir del desarrollo de las diversas formas que han tomado los fenómenos bélicos, pues baste recordar que el ente estatal es producto de la guerra misma.

En el segundo apartado, intitulado “De batallas virtuales: concepto y características esenciales de las ciberguerras”, se procede a analizar con profundidad a este fenómeno conflictivo limitado al uso del ciberespacio. Para esto, se citan y confrontan diversas definiciones sobre ciberguerra de distintos especialistas con el fin de ampliar el espectro analítico que rodea a este novedoso fenómeno bélico. Posteriormente, se enumeran y explican a todos los actores capaces de intervenir en los enfrentamientos en el ciberespacio, escenario que comienza a mostrar las inusuales particularidades de los mismos. Para complementar esta sección, se enlistan de igual forma las técnicas y armas virtuales más utilizadas durante un ciberconflicto, al tiempo que se cita un breve ejemplo que involucró el uso de cada una de éstas con el fin de reafirmar la presencia real de los enfrentamientos cibernéticos en el mundo actual.

En el tercer capítulo, llamado “El otro campo de batalla: el emplazamiento de una ciberguerra a gran escala durante el conflicto ruso-georgiano de 2008”, se describe y analiza a profundidad uno de los casos con más trascendencia en el

terreno de las ciberbatallas con el fin de brindarle una base sólida a los planteamientos establecidos en este trabajo. En concreto, se revisa el caso de la ciberguerra librada entre Rusia y Georgia dentro del conflicto tradicional que estalló en el año 2008. En este sentido, para comprender a bien el marco en el que se desató este fenómeno bélico atípico, en dicha sección se desarrolla una breve trayectoria histórica sobre las relaciones que ambos países han tenido desde su constitución como nación; en seguida, se realiza un análisis sobre el punto de inflexión que llevó a que el conflicto comenzará a gestarse, es decir, cuando el presidente Mijeíl Saakashvili llegó al poder en el pequeño país de Eurasia y; tras todo esto, se realiza una descripción general de la guerra tradicional que se dio entre ambos Estados. Finalmente, y de forma más específica y detallada, se dedica toda una subsección a describir el conflicto informático que se dio entre ambos beligerantes, se hace mención de sus atípicos participantes así como de las tácticas y armas utilizadas durante el desarrollo del conflicto. Bajo esta misma idea, se hace una descripción completa de los daños que el ataque virtual ruso causó en la infraestructura física y cibernética de Georgia, además de las estrategias defensivas que adoptó este último país para protegerse de algo que hasta el momento no conocían. Todo este escenario es revisado bajo el marco de referencia establecido en el primer capítulo de este trabajo y con el orden conceptual definido en la segunda sección del mismo.

En la última sección de este escrito, nombrada “Ciberguerras y la reconfiguración de la noción de seguridad”, se revisan a detalle los efectos que ha tenido este nuevo fenómeno bélico sobre la concepción clásica de seguridad, en su nivel nacional como internacional, así como en los cambios en los campos que hasta hace poco abarcaba. Esto se explica a través de una serie de 4 argumentos que dan cuenta de este nuevo escenario: en primer lugar, se habla sobre el empoderamiento que las redes le han dado al individuo, convirtiéndolo en una amenaza letal para todos los Estados y trayendo consigo efectos secundarios como la expansión del espionaje digital; después, se analiza cómo este ambiente ha dado pie al surgimiento o reconfiguración de unidades militares estatales encargadas de

resguardar el ciberespacio, hecho que ha alentado la cooperación internacional en este mismo ramo; de igual forma, se analiza cómo esta situación repercutirá en las guerras del futuro pues, derivado de la creación de ciberejércitos alrededor del mundo, siempre habrá la posibilidad de que el vector informático se encuentre presente durante las próximas batallas, situación que a su vez acentuará el panorama de los conflictos asimétricos y; por último, se describe cómo todo este ambiente ha dado pie a la búsqueda de Tratados y leyes que intenten contener la dispersión de estos conflictos anómalos antes de que se conviertan en un método estándar de agresión.

Finalmente, es importante mencionar que este estudio de ninguna manera pretende generar una visión apocalíptica sobre el alcance destructivo del fenómeno, más bien busca aportar categorías, instrumentos y un enfoque de análisis que permita ampliar y robustecer al marco de comprensión que actualmente existe sobre las ciberguerras, portento que despierta cada vez más atención en el plano académico.

Capítulo 1. La evolución histórica de la guerra y la transformación del Estado.

> *"No puedes decir que la civilización no avanza, porque, en cada nueva guerra te asesinan de una nueva forma."*
> Will Rogers, *The New York Times*.[2]

La guerra ha estado presente en el mundo desde la génesis del Estado; no obstante, aun cuando el término es bastante antiguo, no existe una definición clara ni un modelo de identidad determinado para el fenómeno debido a los grandes cambios que ha experimentado a lo largo de la historia. En parte, dichas transformaciones encuentran su impulso en los diversos actores, medios, objetivos e ideales que alentaron a los conflictos en un lugar y momento dado: por ello, en el presente capítulo se realiza una breve periodización del fenómeno de la guerra a lo largo del tiempo destacando las características más relevantes de lo que a decir de Martin van Creveld son sus grandes etapas históricas, éstas son las referentes a los conflictos premodernos, a la guerra clásica, a la guerra total y a las nuevas guerras.

De forma paralela a este análisis, se realiza también una investigación sobre la evolución y transformación del Estado partiendo de los efectos que el fenómeno de la guerra provoca sobre él y viceversa, pues es menester recordar que el ente estatal es el principal actor que participa en los fenómenos bélicos.

Con todo, dicho marco de estudio permitirá comprender al lector el entorno político, social, militar, tecnológico, estratégico e histórico que posibilitó el surgimiento y emplazamiento de los diversos enfrentamientos actuales a través del ciberespacio, identificados por los estudiosos del tema con el nombre de Ciberguerras.

[2] Citado en Jeffrey Carr, *Inside Cyber Warfare: mapping the Cyber underwold*, Estados Unidos, O'Reilly, 2010, p. 1. Traducción propia.

1.1 Los conflictos premodernos y la génesis del Estado: los orígenes de la guerra.

El fenómeno de la guerra encuentra sus orígenes en los conflictos antiguos; no obstante, éstos últimos no son, *stricto sensu*, guerras. Aún cuando se especificará más adelante las distintas tónicas que ha adquirido el concepto a través del tiempo, es necesario recurrir a algunas definiciones estándar para confirmar la veracidad de la frase antes escrita.

La palabra guerra, en su sentido más amplio, indica una "lucha armada entre dos o más naciones o entre bandos de una nación," según indica el diccionario de la Real Academia Española. No obstante, es necesario aclarar que dicha lucha, por lo general, tiende a tener "[…] cierto grado de organización, sistematización y continuidad […]."[3]

Si se atiende bien a la definición antes citada, se notará que destacan tres elementos esenciales: la nación (o Estado en sentido lato) y la organización así como la sistematización (representadas por el ejército). Ahora bien, la afirmación de que en la antigüedad no existían las guerras tal y como las conocemos parte precisamente de la inexistencia de estos tres elementos; sin embargo, antes de continuar, es necesario recalcar que aquellos conflictos sí tenían el carácter violento que identifica a cualquier batalla del orden bélico.

Recordemos que, en el tiempo antaño, los conjuntos humanos se reducían a pequeños ducados, comunidades religiosas, reinos feudales, pueblos independientes y pequeños principados. Gran parte de estos conjuntos, según Bruce D. Porter, no tenían una autoridad central fuerte, una jurisdicción efectiva ni mucho menos una administración plenamente organizada: carecían, pues, de

[3] Edmundo Hernández-Vela, *Diccionario de Política* Internacional, México, Porrúa, Tomo I, 2001, p. 540.

soberanía[4]. En este sentido, la guerra, por lo menos entre Estados, no estaba presente durante este periodo histórico.

Por lo que a la organización y a la sistematización –o a los ejércitos- se refiere, no existía la noción de disciplina militar, por lo tanto, las unidades de conflicto se limitaban a ser pequeños grupos de individuos con valor que hacían uso de las ventajas tecnológicas de las que su grupo disponía. Estos cuasi-ejércitos no necesitaban de una organización centralizada –Estado- que pudiera comandarlos durante la batalla; más bien, debido a su reducido tamaño, encajaban perfectamente en los conflictos de baja intensidad propios de aquellos conjuntos de bajo nivel de organización social[5].

Está por demás señalar que el objetivo de estas antiguas batallas se concentraba, básicamente, en situaciones inherentes a la naturaleza de la raza humana: el instinto de supervivencia, la defensa de la propiedad o, en un sentido metafísico, del honor. No había en aquel entonces causas hegemónicas que motivaran el inicio de las hostilidades entre dos o más conjuntos sociales.

Ahora bien, estos conflictos adquirieron una mayor dimensión con el paso del tiempo, sobre todo con el estallido de las pugnas religiosas, en específico, con el inicio de la Guerra de los 30 años[6], pináculo de los enfrentamientos de este tipo durante la última fase de esta etapa: “La intensidad de los conflictos durante este periodo derivaron en lo que se ha dado en llamar ‘la revolución de los asuntos militares’, en la cual el tamaño de las armadas, el costo de la guerra, la potencia del fuego puro junto con la tecnología militar dieron un paso más allá.”[7] Este nuevo escenario, producto de batallas extremadamente violentas y desorganizadas,

[4] *Vid* Bruce D. Porter, *War and the rise of the State: The military foundations of modern politics*, Estados Unidos, The Free Press, 1994, p. 6.
[5] *Idem.*
[6] Nota: la Guerra de los 30 años fue un conflicto librado entre 1618 y 1648 en Europa central. Con un pretexto religioso por delante (Estados apologéticos y escépticos de la reforma del Sacro Imperio Romano Germánico), pronto se convirtió en una guerra que tenía por objetivo el reacomodo del equilibrio político en el continente.
[7] Bruce D. Porter, *Op. Cit. p. 6*

posibilitó el nacimiento del Estado moderno, aquel que ha durado –con distintas dificultades- hasta nuestros días:

> "Durante esta era de transición, la labor de los reinos feudales, de los ducados, de los pueblos independientes, de los pequeños principados y de las comunidades religiosas […] fue insertada en el crisol de un conflicto militar que consignó a las partes más pequeñas al olvido político. El rigor de la supervivencia militar durante la época favorecía la creación de unidades más grandes y más centralizadas políticamente que fueran capaces de controlar grandes extensiones de territorio, de manejar tecnologías militares complejas y de movilizar una inmensa cantidad de recursos tanto materiales como humanos para la batalla."[8]

Con el surgimiento del Estado moderno, nacido tras la Guerra de los 30 años y consolidado con la Paz de Westfalia de 1648, se inauguraría la primera etapa de la guerra como un fenómeno plenamente desarrollado: la de la guerra clásica.

1.2 Guerra clásica.

El primer gran periodo histórico de la guerra como fenómeno plenamente consolidado inició poco después del año 1648 -Paz de Westfalia- y culminó con el advenimiento de la Primera Guerra Mundial (1914). Durante este lapso de tiempo estallaron diferentes conflictos en diversas partes del mundo, mismos que compartían características similares que permitieron unificar su estudio bajo una única categoría: la de la guerra clásica. El principal expositor de esta etapa es Carl Phillipp Gotlieb von Clausewitz (1780-1831), un militar prusiano que se formó bajo diversas batallas libradas en su época, entre ellas las campañas del Rin, la invasión prusiana a Francia durante la Revolución y las Guerras Napoleónicas.

La principal aportación de Clausewitz fue su libro *vom Kriege* (De la guerra), el cual, además de constituir un perfecto manual de cómo librar una batalla, teoriza sobre los conflictos que el militar prusiano conoció hasta el momento de su muerte. La trascendencia de este libro escrito entre 1816 y 1830 es tal que diversos

[8] *Idem.* Traducción propia.

personajes históricos de renombre lo adularon, entre ellos Engels, Lenin y Hitler; más aún, en la actualidad sigue siendo un libro de cabecera en diversas academias militares alrededor del mundo.

Para Clausewitz, la guerra no es otra cosa más que "[…] un acto de fuerza para imponer nuestra voluntad al adversario."[9] Este acto, bajo su visión, es una actividad social representada en un duelo a gran escala, mismo que está moldeado por el tipo de sociedad que lo conduce y por el gobierno que dicha sociedad adopta.[10] Ahora bien, este duelo contiene tres elementos vitales que, en resumen, son también las principales características de la guerra clásica, a saber: el Estado, el ejército y la esfera civil.

En primer lugar, desde la óptica clausewitziana el Estado es el único ente capaz de llevar a cabo una guerra: "[…] la violencia organizada sólo debe llamarse 'guerra' si es librada por el Estado, para el Estado, y contra el Estado."[11] Esta situación responde a que sólo el gobierno, representado por el hombre de Estado, es quien puede tomar decisiones respecto a la supervivencia y fortalecimiento del ente estatal; de hecho, de este postulado nace la famosa frase que ha inmortalizado a Clausewitz a través de los años: "[…] la guerra es una continuación de la actividad política, una realización de la misma por otros medios."[12]

El segundo elemento que caracteriza a la guerra clásica es el ejército pues al ser el Estado el único capaz de librar un conflicto, éste debe poseer una herramienta que se encargue exclusivamente de tal asignación. El ejército "[…] se define como una organización que sirve al gobierno, sea monárquico, republicano o imperial. [Los ejércitos] están conformados por soldados; mismos que son preparados para el propósito de la organización de la batalla al inicio de su empleo

[9] Carl von Clausewitz, *De la guerra*, México, Colofón, 2006, p. 29.
[10] *Vid* Martin van Creveld, *The transformation of war*, Estados Unidos, The Free press, 1991, p. 35.
[11] *Ibidem*, p. 36. Traducción propia.
[12] Carl von Clausewitz, *op. cit.*, p. 46.

y formalmente separados de su cargo cuando terminan."[13] Así pues, el ejército, al servir como mecanismo de ataque y defensa bajo las órdenes del Estado, debe estar en todo momento separado del tercer elemento vital de este modelo, esto es, los civiles: de ahí que, durante el periodo que abarca esta etapa del fenómeno de la guerra, las organizaciones militares tuvieran una serie de mecanismos e instituciones diferentes a las que regulaban a la sociedad en general, entre ellas las leyes propias de la milicia o la reclusión en los cuarteles.

Finalmente, el tercer elemento de la guerra clásica, como ya se mencionó, es la esfera civil. Aunque los civiles no juegan un papel importante en la batalla, pues sólo pagan impuestos y producen para sostenerla, éstos deben de estar separados de la misma a como de lugar: "[…] desde que la guerra era una cuestión de Estado, las personas deberían estar excluidas de ella hasta donde sea posible."[14] Así pues, de este principio nace la separación formal entre lo civil y lo militar, la cual tendría que estar en todo momento garantizada por el soberano.

En resumen, el modelo clásico de la guerra está conformado por un Estado capaz de monopolizar la fuerza; un ejército organizado y centralizado con posibilidad de ejecutarla; y un pueblo que permanece al margen de los conflictos. No obstante, adicionalmente a estos tres elementos que Clausewitz desarrolla en *vom Kriege* existen otras dos características esenciales que se encuentran a lo largo de este periodo: éstas son las armas cuerpo a cuerpo y el campo de batalla definido. Durante las batallas desarrolladas en esta etapa se utilizaban, en su mayoría, armas cuerpo a cuerpo, situación que concedía un carácter caballeresco a los enfrentamientos. Sin embargo, la debacle de tal escenario inició con el perfeccionamiento de la artillería durante las Guerras Napoleónicas así como con la introducción de nuevos instrumentos letales en los combates, entre ellos el uso de caballería, por ejemplo. Por otro lado, es necesario mencionar que el campo de batalla en los conflictos estaba geográficamente definido, esto es, los oponentes,

[13] Martin van Creveld, *op. cit.*, p. 37. Traducción propia.
[14] *Ibidem*, p. 38. Traducción propia.

en este caso dos o más Estados, libraban los enfrentamientos en lugares específicamente acordados para tal designio.

Es tan grande la importancia del modelo de guerra elaborado por Clausewitz que éste se convirtió en el referente por excelencia para regular el fenómeno a nivel internacional mediante la implementación de diversos instrumentos jurídicos, pues a partir de su teoría…

> "Una serie de Tratados internacionales, muchos de los cuales datan del periodo entre 1859 (Batalla de Solferino) y 1907 (Segunda Conferencia de Paz de la Haya) codificaron estas ideas y las convirtieron en ley positiva. Para distinguir a la guerra de un mero crimen aquélla fue definida como algo librado por los Estados soberanos y sólo por ellos solos. Los soldados fueron definidos como personal licenciado para participar en la violencia armada a favor del Estado; y como parte de éste, las antiguas prácticas de expedición de patentes de corso y el corso mismo fueron prohibidas. Para obtener y mantener su licencia, los soldados tenían que ser cuidadosamente registrados, marcados y controlados para excluir las prácticas del corso. Ellos [los soldados] sólo podían luchar mientras estaban en uniforme, cargando sus armas de forma 'abierta', y obedeciendo a su comandante quien debía hacerse responsable de sus acciones. Se supone que no debían recurrir a métodos 'ruines' como ruptura de treguas, tomar las armas después de herir o tomar un prisionero, y afines. La población civil no debía ser incluida en el conflicto, mientras las 'necesidades militares' lo permitieran. Como contraparte, ésta [la población civil] debía dejar a los soldados luchar entre ellos. Los civiles que rompieran las reglas, es decir, que no hayan obtenido una licencia antes de recurrir a la violencia, se pondrían bajo su propio riesgo de tener represalias cuando fueran capturados."[15]

De igual manera, esta primera etapa de la guerra insidió de manera directa en la forma del Estado. Las grandes batallas libradas durante esta época, con la consiguiente gran acumulación de poder en los vencedores, incentivaron el nacimiento de nacionalismos, los cuales, a su vez, impulsaron el origen del Estado-nación: las Guerras Napoleónicas junto con la Revolución Francesa son grandes ejemplos de este tipo de mutación. Esta nueva forma de ente estatal se

[15] *Ibidem*, p. 40. Traducción propia.

caracterizaba por "[…] la estrecha relación entre la nación cultural y la política del Estado, del cual la legitimidad política estaba ligada con la soberanía popular."[16]

Esta novedosa forma de organización logró expandirse rápidamente por Europa -y posteriormente por el mundo- debido, entre otras cosas, a la voluntad de los distintos pueblos –surgida del nacionalismo- para derrocar a los imperios que los gobernaban así como a la novedosa política de reclutamiento que se emplazaría durante esta etapa: el alistamiento masivo de hombres merecía como contraparte la concesión de mayores derechos políticos. Fue así, pues, la forma en que se consolidó esta nueva forma de Estado.

Aun con toda su trascendencia, el modelo clausewitziano de la guerra comenzaría a perder importancia con el advenimiento de la Primera Guerra Mundial en el año 1914, pues ésta dio pie al surgimiento de un nuevo paradigma en los conflictos que prácticamente se extendió hasta el final de la Segunda Gran Guerra, la guerra total.

1.3 Guerra total.

El periodo de la guerra total inició, como anteriormente se mencionó, con el estallido de la Primera Guerra Mundial. Los principales exponentes de este periodo son Colmar von der Goltz (1843-1916) y Erich Ludendorff (1865-1937), ambos alemanes. Como participantes dentro de la Primera Gran Guerra, los dos germanos fueron capaces de teorizar sobre los cambios que había sufrido el fenómeno de la guerra con la introducción de nuevos elementos en la batalla y en la vida del mundo de aquellos años, situación que, de alguna forma, contradecía a los principios que Clausewitz había formulado durante su época.

[16] Bruce D. Porter, *Op. Cit.,* p. 8. Traducción propia.

La principal aportación de von der Goltz a la teoría militar fue su libro *Das Volk in Waffen* (La nación en armas), el cual difería de los postulados erigidos por el Varón prusiano respecto al fenómeno de la guerra, especialmente en lo que refiere a dos principios: el de las guerras hechas exclusivamente por Estados y el de la relación soberano-milicia-civil.

En lo que respecta al primer punto, para von der Goltz las guerras no son libradas por los Estados contra los Estados sino de ejército a ejército; sin embargo, su visión de ejército no es la formulada en tiempos antiguos, pues ahora éste comprende a toda la nación, es decir, no existe en la guerra total una separación entre lo civil y lo militar:

> "La demostración de la habilidad de la tecnología moderna para integrar los recursos de una nación entera, escribió von der Goltz, señala hacia la conclusión de que las futuras guerras no serán peleadas por los ejércitos como tradicionalmente se conocen […] al llamado de la bandera, la nación entera podrá ponerse un uniforme, tomar las armas y lanzarse a sí misma contra el enemigo."[17]

Desde su perspectiva, esta situación era posible debido a la introducción de nuevas invenciones militares, tecnológicas, estratégicas y logísticas al arte de la guerra, entre ellas el ferrocarril y el telégrafo, instrumentos que jugaron un papel crucial durante el desarrollo de los dos grandes conflictos del siglo XX.

Aunado a dicho postulado se erigía el otro con el que von der Goltz completaba su teoría: según él, la salvaguarda de la distinción militar-civil a cargo del soberano ya no era posible debido a la gran importancia que comenzaban a revestir los conflictos; por ello, él proponía la figura de un comandante en jefe que se encargaría de todos los asuntos relativos a la milicia.

[17] Martin van Creveld, *Op. Cit.*, p. 42. Traducción propia.

Así pues, pareciera ser que, en este modelo, el Estado ya no utilizaría a la guerra como un medio para hacer política (como Clausewitz proponía), sino que la guerra misma comenzaba a devorar al Estado, teniendo que hacer éste todo lo necesario para sobrevivir aun cuando tuviera que acabar con la distinción de la sociedad con el ejército, hecho que incluso se viviría durante la Primera Guerra Mundial:

> "Las batallas iniciales [durante la Primera Guerra Mundial] fallaron en producir una decisión, en vez de eso produjeron montañas de bajas. Los ejércitos tuvieron que ser respaldados por la movilización masiva del poder militar de hombres de todas las edades. Después vino la movilización de civiles de los dos sexos para apoyar a las fábricas que producían los medios para el esfuerzo de la guerra –los tremendos suministros que las fuerzas armadas requerían para operar y existir. Esto fue complementado con la agricultura, materias primas, transporte, finanzas, talento técnico-científico y cualquier otro tipo de recurso. La doctrina económica del siglo diecinueve de *laissez faire*, que había tomado algunos impulsos antes de la guerra, murió de repente y bajo una muerte no natural. No paso mucho tiempo antes de que los gobiernos empezaran a tomar una mano de todo lo que consideraran incluso remotamente relevante para el esfuerzo de la guerra. Esto incluía la salud del pueblo, sus condiciones de vida, su ingesta de calorías, su salario, sus cualificaciones profesionales, su libertad de movimiento, y así sucesivamente hasta el infinito."[18]

Bajo este mismo contexto, Ludendorff presentaba por los mismos años su teoría sobre el fenómeno de la guerra, la cual estaba contenida en su libro *Der Totale Krieg* (Guerra total). Al igual que von der Goltz, este militar alemán pensaba que la guerra no era "la política por otros medios" sino una verdadera lucha del Estado por sobrevivir.

En este sentido, Ludendorff menciona que los gobiernos deberían formalizar la abolición de la separación entro lo civil y lo militar con el fin de que el propio Estado pudiera librar una "guerra auténtica": "Ludendoff demandaba que las distinciones usuales entre el gobierno, el ejército y los civiles fueran destruidas […]

[18] *Ibidem*, p. 44. Traducción propia.

[así] el país entero se convertiría en el equivalente a un ejército gigante con todos los hombres, mujeres y niños sirviendo a su cargo."[19] Sin embargo, para que esta situación fuera posible debería existir un *der Feldherr*, es decir, un dictador de origen castrense que pusiera en marcha toda la maquinaria bélica sin ninguna limitación moral o jurídica.

Así pues, el paradigma de la guerra total introdujo dos postulados que en los tiempos de Clausewitz eran inconcebibles: en primer lugar, impulsó el desvanecimiento de la línea que dividía a lo militar de lo civil y, en consecuencia, promovió la movilización de países enteros (incluyendo el sector social, productivo y científico) al esfuerzo de la guerra; en segundo lugar, generó la tendencia de dividir las facultades de los gobernantes en dos personas, por un lado el jefe de Estado encargado de todos los asuntos civiles (sin descuidar lo relativo a la defensa del ente estatal) y un militar de alto rango encargado de asegurar la estrategia defensiva y ofensiva de la nación.

También, este periodo vio nacer cambios fundamentales en las batallas en lo concerniente a las armas y al campo de combate. Primeramente, y a diferencia del periodo clásico, en esta etapa la artillería mecanizada (producto de los avances tecnológicos de la época) jugó un papel importante en el desarrollo de los conflictos. Asimismo, la introducción de los gases tóxicos a las trincheras dio cuenta del potencial daño que podía provocar el ambiente al Ser Humano, hecho que formalizó el nacimiento de las guerras atmosféricas.[20] Por lo que respecta al campo de batalla, éste experimentó su primera ampliación hacia al aire (con la introducción del combate aéreo a cargo de aviones diseñados específicamente para ello) y su profundización en las aguas de los grandes océanos (con la puesta en marcha de los submarinos, portaviones y destructores).

[19] *Ibidem*, p. 45. Traducción propia.
[20] *Vid* Peter Sloterdijk, *Temblores de aire: en las fuentes del terror*, España, Pre-textos, 2003, 142 pp.

Con todos estos cambios, era de esperarse una nueva mutación en el ente estatal: durante este periodo, que duró poco más de 30 años, nació el Estado colectivista…

> "Esta última encarnación del Estado moderno estaba caracterizada por tres atributos distintivos: una penetrante intervención del gobierno en la economía, la participación masiva de la población en la política y la responsabilidad estatal directa del bienestar del ciudadano."[21]

Todos y cada una de estos elementos tiene su origen en el desarrollo de las dos grandes guerras. La intervención del Estado en la economía revestía de vital importancia debido a la dimensión de las batallas durante este periodo pues, como se mencionó anteriormente, el gobierno necesitaba encaminar todos los recursos –tanto materiales como humanos- al esfuerzo de la guerra. Por otro lado, la participación masiva de la sociedad en la política estaba directamente ligada con la rápida expansión de los medios y la concientización de la sociedad ante la catástrofe de los conflictos: por primera vez, los ciudadanos de los países beligerantes podían protestar y sugerir sobre la estrategia gubernamental –hecho que, de alguna u otra forma, se reforzaba con la naciente opinión internacional. Finalmente, el aumento en el nivel de bienestar de la población que otorgaron los Estados beligerantes en aquella época formó parte de lo que se ha dado en llamar la Paradoja de la Moral: al mismo tiempo que el Estado ejercía acciones viles contra sus contrincantes implementaba también reformas políticas que beneficiaban directamente a su población, esto con el fin de ganar adeptos para su esfuerzo bélico y disminuir el número de inconformidades relacionadas con la misma causa.

A la par de esta revolución –tanto bélica como estatal-, sucedieron cambios también en lo que a la regulación de la guerra se refiere, pues la no distinción entre lo militar y lo civil -que se reflejó en las múltiples atrocidades ocurridas durante las dos grandes guerras de este periodo- daba pie a nuevos métodos de castigo:

[21] Bruce D. Porter, *Op. Cit.*, p. 8. Traducción propia.

> "El primordial propósito de los Juicios de Criminales de Guerra llevados a cabo en Nuremberg y Tokio fue ayudar a tapar el daño hecho a la sociedad internacional definiendo las cosas que estaban y que no estaban permitidas [en la guerra]. Para ello, los factores políticos, económicos, sociales y militares que habían sido responsables de la ruptura de las distinciones [entre lo militar y lo civil] del modelo tradicional trinitario [de guerra] fueron ignorados. En cambio, la ruptura fue puesta en la puerta de un particular grupo de personas, a saber, los perdedores. Sus principales líderes fueron puestos en juicio, condenados, y la mayor parte ejecutados. Las fuerzas armadas del lado derrotado fueron desarmadas, sus principales organizaciones económicas (tal como los *Zaibatsu* japoneses) fueron dispersadas, y sus recursos expropiados como reparaciones para los victoriosos que decidieron hacer eso. Los tribunales por sí mismos ayudaron a cristalizar una serie de nuevos conceptos jurídicos [para regular al fenómeno de la guerra], tales como 'conspiración para quebrantar la paz', 'emprendimiento de guerra agresiva', y algo conocido como 'crímenes de guerra'."[22]

Estas nuevas regulaciones que poco a poco surgían en el ámbito internacional no evitaron que las catástrofes de la guerra se concretaran, tal como sucedió con el uso de las bombas nucleares en Hiroshima y Nagasaki aun cuando las negociaciones de paz de 1945 ya habían comenzado. De hecho, fueron estos aparatos de destrucción en masa los que clausuraron la etapa de la guerra total y que, de alguna forma, impulsaron el nacimiento del tercer periodo de este fenómeno: el de las nuevas guerras.

1.4 Nuevas guerras.

La etapa de las nuevas guerras inició, como ya se mencionó, con la introducción de los artefactos atómicos en el año de 1945 y se reforzó y consolidó aún más durante la Segunda Guerra del Golfo (1990-1991): ambos hechos históricos introdujeron elementos que modificaron de forma radical a los paradigmas anteriormente concebidos sobre los fenómenos bélicos.

[22] Martin van Creveld, *op. cit.*, p. 48. Traducción propia.

Ahora bien, no existe un expositor ampliamente reconocido sobre el tema pues éste es aún un tópico en discusión entre la comunidad académica; no obstante, destacan varios autores que han teorizado sobre las nuevas guerras, entre ellos es posible mencionar a Martin van Creveld, Mary Kaldor, Eric Hobsbawm, Qiao Liang y Wang Xiangsui. A continuación se realiza una breve exposición de sus postulados principales para intentar construir al final de la presente sección un modelo preciso de esta etapa de la guerra.

En primer lugar, Martin van Creveld, teórico israelí del fenómeno de la guerra, sostiene que las nuevas guerras no tienen nada de "novedoso", pues este modelo se asemeja más bien a los conflictos premodernos que sucedieron antes de la firma de los Tratados de Paz de Osnabrück y Münster (Paz de Westfalia), periodo en que los Estados no estaban aún consolidados[23]. Según van Creveld, las batallas libradas por aquellas épocas son parecidas a los "conflictos de baja intensidad" que se viven hoy en día: de ahí que el argumento central de su libro *The transformation of war* (La transformación de la guerra) sea que el modelo clausewitziano ya no es capaz de explicar a las guerras actuales, pues éste es sólo una de las etapas que ha vivido la guerra a lo largo del tiempo –la cual, señala, ya terminó. Los conflictos de baja intensidad, según van Creveld, se caracterizan por los siguientes postulados:

> "Primero, tienden a desarrollarse en las partes del mundo 'menos desarrolladas'; los conflictos armados de baja escala que toman lugar en los países 'desarrollados' son usualmente conocidos bajo una variedad de nombres, tales como 'terrorismo', 'trabajo policial', o […] 'problemas'. Segundo, raramente involucran ejércitos regulares en ambos lados, aunque a menudo existen de un lado guerrillas, terroristas, e incluso civiles, incluyendo mujeres y niños, y otros. Tercero, la mayoría de los conflictos de baja intensidad no residen primariamente en las armas colectivas de alta tecnología que son el orgullo y la alegría de cualquier fuerza armada moderna. Excluidos de ellas los aviones y los tanques, los misiles y la artillería pesada, así como otros dispositivos difíciles de conocer por sus acrónimos."[24]

[23] *Vid* sección Los conflictos premodernos y la génesis del Estado: los orígenes de la guerra.
[24] Martin van Creveld, *Op. Cit.*, p. 19. Traducción propia.

Así pues, menciona van Creveld, los conflictos de baja intensidad no se diferencian en nada de las batallas desarrolladas antes de la Paz de Westfalia sino todo lo contrario, éstos son un regreso a ese estado originario donde no existía un Estado que librara los conflictos y, por ende, no había un ejército que ejecutara la fuerza estatal: de hecho, los conflictos armados de aquellos años eran iniciados por monarcas, asociaciones religiosas y mercenarios que eran parte de la sociedad y, además, éstos no comenzaban los enfrentamientos por motivos relacionados con el interés del gobierno sino más bien tenían justificaciones personales o grupales.

Tal escenario, señala el teórico israelí, resurgió debido a la llegada del artefacto atómico al campo de batalla, el cual constituye la máxima defensa de los Estados actuales pero también genera una limitación al fenómeno de la guerra: no se pueden librar ya guerras convencionales porque éstas terminarían desembocando inevitablemente en una batalla nuclear, misma que significaría, evidentemente, un suicidio colectivo. Ante tal situación, los conflictos de baja intensidad surgen como una posibilidad de arreglar diferendos sin llegar al extremo de iniciar una batalla atómica; empero, los gobiernos no han decidido prepararse para librar enfrentamientos de este tipo pues el modelo clausewitziano ha marcado tanto a la concepción del fenómeno de la guerra que los Estados no desean deshacerse de los medios tradicionales de defensa y, también, porque hay que mantener a un complejo industrial militar extremadamente poderoso "feliz", puntualiza el teórico.

Por otro lado, Eric Hobsbawm, reconocido historiador británico, analiza la transformación que ha sufrido el fenómeno de la guerra desde del siglo XX a la fecha, y aun cuando no emplea directamente el término nuevas guerras, claramente señala cambios fundamentales que, según él, marcarán a los conflictos durante todo el siglo en curso. Para Hobsbawm,

> "[…] a principios del siglo XXI estamos en un mundo donde las operaciones armadas ya no están fundamentalmente en manos de los gobiernos y de sus agentes

> autorizados, y donde las partes en conflicto no comparten características, ni estatus, ni objetivos, excepción hecha del deseo de recurrir a la violencia."[25]

Por lo que respecta a la distinción militar-civil, el británico señala que ésta ha ido desapareciendo desde el siglo XX: "a lo largo del siglo […] el peso de la guerra ha ido recayendo más y más sobre los hombros de los civiles, que no sólo eran las víctimas del conflicto sino también el objetivo de las operaciones militares y político militares."[26]

Además, agrega que, en el siglo XXI, la frontera entre guerra y paz ha dejado de ser clara debido a la ausencia de tratados que regulen de manera puntual al fenómeno de la guerra pues, según Hobsbawm, los que existen son muy ambiguos y desatienden abiertamente a los conflictos intra-Estado, mismos que están tomando cada vez más relevancia en la escena internacional. En este sentido, Hobsbawm menciona que, en lo que va de la presente centuria,

> "[…] el Estado territorial ha perdido, por diferentes motivos, el monopolio tradicional del ejército, buena parte de la fuerza y la estabilidad que lo caracterizaron y, con una frecuencia cada vez mayor, el sentido fundamental de legitimidad o cuando menos de aceptación que les permitía obligar a ciudadanos obedientes a pagar impuestos o a someterse al servicio militar. Los instrumentos materiales para la guerra están hoy al alcance de grupos privados, como también los canales para financiar una contienda en la que no participen los Estados. Y todo esto ha provocado un cambio en el equilibrio entre las organizaciones estatales y las no estatales."[27]

Hobsbawm finaliza indicando que tal escenario es producto de la globalización y de los grandes y acelerados cambios que ha vivido el mundo en los últimos años.

En otro orden de ideas, Mary Kaldor, afamada académica británica de la *London School of Economics and Political Science*, hace referencia explícita a las

[25] Eric Hobsbawm, *Guerra y paz en el siglo XXI*, España, Crítica, 2007, p. 3.
[26] *Ibidem*, p. 4.
[27] *Ibidem*, pp. 11-12.

nuevas guerras señalando que éstas se comenzaron a desarrollarse entre los años 80 y 90. Según Kaldor, las batallas desarrolladas en este nuevo periodo

> "[…] implican un desdibujamiento de las distinciones entre guerra, crimen organizado y violación a gran escala de los derechos humanos, asimismo frente a lo que hemos [MK] definido como guerras viejas [refiriéndose a los conflictos enmarcados bajo el modelo clausewitziano]. Las nuevas guerras son diferenciables principalmente en cuanto a: 1. Objetivos de la guerra 2. Métodos de lucha y 3. Métodos de financiación."[28]

Luego entonces, según Kaldor, los objetivos de la guerra han dejado de ser preeminentemente políticos para privilegiar ahora cuestiones relativas a la identidad, el nacionalismo y la cultura (de ahí que la mayoría de estos conflictos sean luchas por la autodeterminación o guerras de exterminio racial). Asimismo, apunta que los métodos de lucha son atípicos debido a la ausencia de ejércitos regulares y de tácticas convencionales, hecho que ha dado pie a la formación de estrategias dispersas pero en algún momento organizadas bajo un solo ideal –como las guerrillas y los grupos terroristas. Finalmente, los métodos de financiación de estos nuevos conflictos son paralelos a la economía globalizada, es decir, los recursos necesarios para llevar a cabo un enfrentamiento de este tipo surgen de la economía sumergible representada en los grandes mercados negros –los cuales han crecido de manera alarmante en los últimos años debido a la interconectividad y facilidad de transporte a la que ha dado pie la globalización.

En resumen, las nuevas guerras son para Mary Kaldor un producto de la globalización, la cual ha impulsado la erosión de la autonomía del Estado y ha generado también la pérdida de la legitimidad de éste. Debido a su naturaleza, estos nuevos conflictos tienden a librarse dentro de los Estados, pues distintos grupos buscan establecer su propia definición de identidad cultural e identidad nacional. Finalmente, concluye que estos conflictos están lejos de extinguirse pues

[28] Mary Kaldor, *Las nuevas guerras: violencia organizada en la era global*, España, Tusquets, 2001, pp. 49-79.

las condiciones que ha originado el proceso globalizador proporcionan el fácil acceso a las armas y, por ende, del recurso a la violencia; hecho que desemboca en que los conflictos se vuelvan un factor altamente privatizado, dando pie al surgimiento de grupos paramilitares y organizaciones criminales cada vez más poderosas e interconectadas.

Por último, Qiao Liang y Wang Xiangsui, ambos coroneles de origen chino, desarrollan su teoría sobre las nuevas guerras o, como ellos le llaman, guerras irrestrictas. Según estos oficiales, estas nuevas formas de conflicto son producto de dos situaciones trascendentes en el mundo: en primer lugar, del desarrollo tecnológico en general y el de las armas en particular, pues, desde su visión, la innovación en las herramientas de destrucción desarrollada a partir de la Segunda Guerra del Golfo ha dado pie al surgimiento de una nueva revolución en los asuntos militares que se materializa en la constitución de guerras sin límites materiales o morales y; por otro lado, las guerras irrestrictas responden al hecho de que la sociedad internacional actual propugna por no resolver las diferencias por la vía militar, de ahí que algunos países –sobre todo los hegemónicos- creen nuevas formas de conflicto capaces de persuadir, intimidar e incluso eliminar a un enemigo sin quebrantar las convenciones aceptadas a nivel mundial.

Así pues, en esa búsqueda por encontrar una nueva forma de hacer frente a los conflictos actuales se han roto todas las fronteras y límites en las diversas áreas conocidas por el ser humano para dar origen a las guerras irrestrictas, en las cuales

> "[…] todos los medios estarán a disposición [de los enfrentamientos], la información será omnipresente, y el campo de batalla estará en todas partes. Esto significa que todas las armas y la tecnología disponible se superpondrá a la voluntad [de los contrincantes], que todos los límites que se encuentran entre los dos mundos de la guerra y la no guerra, de los militares y no militares, serán totalmente destruidos, y

también que muchos de los principios actuales de los combates serán modificados, e incluso que puede ser necesario volver a escribir las reglas de la guerra."[29]

Así pues, en estos conflictos irrestrictos los objetivos de la acción bélica son prácticamente imposibles de identificar debido a la aparición de múltiples agendas de los diversos actores que ahora participan en los enfrentamientos: ejércitos regulares bajo las órdenes de los Estados, hackers, científicos, comunicadores, en resumen, todas las personas pertenecientes a una sociedad. Asimismo, el campo de batalla ahora no está delimitado a un espacio geográfico determinado; por el contrario, debido a la impregnación de la guerra en todos los aspectos de la vida, éste está ahora en todos lados, incluyendo los espacios naturales y artificiales hasta hoy conocidos por el Hombre. Este último hecho, aunado al de la diversidad de participantes en los conflictos, dará pie a una multitud de métodos de ataque que pueden comprender las más variadas áreas, entre ellas: *hackear* sitios informáticos, ataques contra instituciones financieras, generación de crisis económicas, el uso del terrorismo, la expansión ideológica mediante los medios de comunicación, entre otros.

El modelo de guerras irrestrictas es, pues, un modelo de guerra omnipresente en todos los aspectos de la vida el cual puede ser utilizado por los países menos desarrollados para sacar ventaja del modelo tradicional adoptado por las potencias hegemónicas, concluyen los chinos.

Ahora bien, retomando a todos los autores apuntados anteriormente, es posible mencionar que las nuevas guerras se caracterizan por lo siguiente: en primer lugar, puede o no participar el Estado, no obstante, de un lado siempre existirá un grupo atípico en las batalles, sean estos terroristas, mercenarios, grupos paramilitares o incluso civiles.

[29] Qiao Liang, Wang Xiangsui, *Unrestricted Warfare: China's master plan to destroy America*, Panama, Pan American, 2002, p. 5. Traducción propia.

En segundo lugar, pueden o no participar los ejércitos regulares, sin embargo, aún con la intervención de éstos, no existe una distinción militar-civil debido a las características que revisten los nuevos guerreros en este tipo de enfrentamientos.

Por otro lado, los objetivos de la guerra dejan de ser preeminentemente políticos para darle cabida a lo cultural y a la identidad, sin menospreciar también aspectos ideológicos, económicos o incluso personales; las armas no recaen exactamente en los instrumentos letales tradicionales que se conocen pues las condiciones de la globalización han dado la oportunidad de utilizar cualquier medio disponible como arma en una batalla; el campo de batalla se ha ampliado a lugares naturales y artificiales, es decir, todas las partes del globo se han convertido en un auténtico campo de batalla debido a las múltiples armas utilizables en este tipo de guerra y a la variada cantidad de actores involucrados.

Antes de terminar es necesario hacer hincapié en el debate que se presenta durante esta etapa en lo que respecta al ente estatal. Si se presta atención, es posible identificar que muchos de los autores anteriormente citados dibujan al Estado como un ente que está siendo relegado hacia un perfil extremadamente discreto: de ahí la famosa corriente que pregona la “desaparición del Estado”. Si bien no es objeto de este trabajo profundizar sobre este tema, es menester destacar que, por cuanto a los asuntos de la guerra se refiere, el Estado ha perdido el monopolio de este fenómeno debido a los múltiples actores que han surgido después del fin de la Guerra Fría, esto es, como resultado de la redistribución de poder y del nuevo entorno tecnológico generado por la globalización: las guerrillas de liberación nacional, los grupos ultranacionalistas o las asociaciones de hackers representan tal aseveración.

Con todo, es precisamente dentro de este contexto de guerras omnipresentes y caóticas (nuevas guerras) donde se insertan las actuales batallas a través del ciberespacio –ciberguerras-, las cuales se explicarán a profundidad en la siguiente sección acatando el marco conceptual desarrollado en el presente capítulo.

Capítulo 2. De batallas virtuales: concepto y características esenciales de las ciberguerras.

> *"En el siglo XXI, los bits y bytes pueden ser tan peligrosos como las balas y las bombas."*
> William Lynn, Subsecretario de Defensa de Estados Unidos.[30]

2.1 El concepto ciberguerra.

No existe un concepto único de ciberguerra, de hecho, cada definición elaborada por los diversos especialistas alrededor del mundo corresponde a la descripción de un hecho aislado o bien centra su atención respecto a un asunto en particular que le es de interés a su autor. Esta situación ha dado pie a un intenso debate entre académicos, instituciones de investigación, organismos de seguridad e incluso empresas transnacionales que cuestionan la existencia del fenómeno aun cuando hay hechos que demuestran su presencia en el mundo de hoy. Por estas razones, el presente capítulo enlista las explicaciones más completas de este tipo de fenómenos bélicos, indaga en sus características más importantes, muestra los mecanismos de agresión que se emplean durante su desarrollo, revisa las consecuencias que traen consigo así como los objetivos que persiguen, además de señalar los conflictos informáticos más representativos que se han dado hasta el momento; todo ello sin perder de vista el marco analítico en el que se insertan: el de las nuevas guerras.

Para Richard A. Clarke, ex encargado de la Oficina Antiterrorista de Estados Unidos y pionero en el tema de los ciberconflictos, una ciberguerra, en sentido general, "se refiere a las acciones que un Estado emprende para penetrar en los ordenadores o redes de otra nación con el fin de causar mal funcionamiento o daño."[31] A pesar de que su descripción parece simplista, ésta misma sirve de

---

[30] Citado en William Márquez, *Ciberespacio: el nuevo ámbito de guerra para el Pentágono*, [en línea], BBC, 27 de julio de 2001, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml, [consulta: 20 de enero de 2013].

[31] Richard A. Clarke, *Cyber War: The next threat to national security and what to do about* it, Estados Unidos, HarperCollins, 2010, p. 6. Traducción propia.

introducción para entender un concepto más profundo de su autoría, el cual dicta que:

> "Una ciberguerra es la penetración no autorizada de, en nombre de, o en soporte de un gobierno en las computadoras o redes de otra nación, u otra actividad que afecte sistemas computarizados con el propósito de adherir, alterar y falsificar datos o causar la disrupción o el daño a una computadora, a un dispositivo de red, o al objeto que una computadora controla."[32]

Resulta especial el hecho de que, para este autor, sólo los Estados pueden hacer ciberguerras, contrariando de manera tácita las afirmaciones del capítulo anterior sobre las características de las nuevas guerras –específicamente, donde se describe que no sólo participa el ente estatal en las batallas. Esta situación obedece a que la obra de Clarke se centra en los ciberejércitos estatales, dejando la puerta cerrada a todas aquellas personas sin sujeción castrense a un Estado con capacidades de realizar un ciberataque a grande o pequeña escala: tal es el caso de los hackers, crackers o incluso de civiles con equipo de cómputo y conocimientos básicos en informática. Estos últimos parámetros sí son retomados por Adam Liff, académico de la Universidad de Princetone, quien define a una ciberguerra como un

> "[…] estado de conflicto entre dos o más actores caracterizado por la hostilidad deliberada y el costo que induce el uso de ciberataques contra infraestructuras civiles o militares críticas de un adversario con intensión coercitiva para extraer concesiones políticas, como medida de fuerza bruta contra redes militares o civiles con el fin de reducir la capacidad del adversario para defenderse o tomar represalias en especie o con fuerza convencional, o contra objetivos civiles y/o militares con el fin de enmarcar a otro actor para fines estratégicos."[33]

---

[32] *Ibidem*, p. 228.

[33] Adam P. Liff, *Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare and interstate war,* [en línea], Journal of Strategic Studies, 2012, Dirección URL: http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.663252, [consulta: 3 de enero de 2013]. Traducción propia.

Por su parte y en el mismo sentido, María Cristina Rosas, académica de la Universidad Nacional Autónoma de México, menciona que la palabra ciberguerra se refiere

> "[…] a acciones desarrolladas por individuos operando en el interior de los Estados, que efectúan acciones ofensivas y/o defensivas en el ciberespacio, empleando computadoras para atacar a otras computadoras o redes a través de medios electrónicos. El objetivo de estas acciones es buscar ventajas sobre el adversario, al comprometer la integridad, confidencialidad y disponibilidad de la información, en particular la de carácter estratégico. Así, al privar al rival de la información estratégica que requiere para tomar decisiones, se busca debilitarlo y, eventualmente, lograr la victoria sobre él."[34]

Como se aprecia, dichas definiciones son aún más completas que la enunciada por Clarke, pues estás abarcan un espectro más grande de participantes en los ciberconflictos así como de las amenazas que estos mismos representan. En este sentido, se ahondará aún más en estos dos últimos ámbitos (participantes y amenazas) pues es evidente que pueden delinear características relevantes sobre el tipo de conflictos que se desarrollarán a lo largo del siglo corriente.

2.2 Actores de las ciberguerras.

Por lo que respecta a los actores en las ciberguerras es menester mencionar, como anteriormente se remarcó, que existen diversos tipos de participantes de los más diversos ámbitos; entre ellos, figuran los Estados a través de los ciberjércitos, los hackers, los crackers, e incluso los civiles con nociones básicas de computación.

Los ciberejércitos son todos aquellos grupos dependientes de una organización militar formal encargados de la defensa cibernética e informática de su Estado y del ataque por la misma vía a otros cuando la nación así como la situación

[34] María Cristina Rosas, *De la ciberguerra a la ciberpaz*, [en línea], revisa Etcétera, 2011, dirección URL: http://www.etcetera.com.mx/articulo.php?articulo=9759, [consulta: 13 de febrero de 2013].

lo requieran. Estos conglomerados están formados por cibersoldados, mismos que se caracterizan por tener una estricta formación en informática y computación que les permite poseer una alta capacidad para realizar operaciones de ofensa en contra de las redes y equipos informáticos de los enemigos de su país, así como para resguardar los propios de ataques foráneos. Estas unidades no deben confundirse con los llamados soldados electrónicos, aquellos que

> "[…] en su mochila guardan un ordenador portátil, por su transmisor y antena está constantemente conectado a un WLAN que cubre todo el campo de batalla, cuyas armas pueden ser constantemente actualizadas con un gran número de dispositivos ópticos como cámaras de video y prismáticos infrarrojos, y cuya armadura está complementada con tecnología GPS."[35]

Si bien estos individuos tienen un gran conocimiento en equipos computarizados, no realizan operaciones agresivas a través de la red, pues su función principal se adscribe a brindar soporte en el campo de batalla a través de todos los dispositivos tecnológicos que tienen a su alcance.

Ahora bien, es necesario mencionar que todo ciberejército actúa necesariamente bajo una ciberestrategia dictada por el Estado al que éste se sujeta. El término ciberestrategía, según Daniel T. Kuehl, se refiere al

> "[…] desarrollo y empleo de capacidades estratégicas para operar en el ciberespacio, integrando y coordinando a otros ámbitos operativos, para alcanzar o apoyar el logro de objetivos a través de los elementos del poder nacional para consolidar una estrategia nacional de seguridad."[36]

---

[35] S/a, *Electronic Soldier*, [en línea], Diccionary of War, Dirección URL: http://dictionaryofwar.org/node/638, [consulta: 15 de enero de 2013]. Traducción propia.

[36] Daniel T. Kuehl, "From Cyberspace to Cyberpower: defining the problem", en Fraklin D. Kramer, Staurt H. Starr y Larry K. Wentz (editores), *Cyberpower and National Security*, Washington D. C., Center for Technology and National Security Policy/National Defense University, p. 40. Traducción propia.

Dicha ciberestrategia está cimentada en los tres componentes esenciales que definen al ciberespacio: por un lado, la tecnología con la que se cuenta para poder ingresar a la red; en segunda instancia, la interconectividad que permite la comunicación entre dicha tecnología y; finalmente, el componente humano, refiriéndose a la capacidad de operar y manipular dichos sistemas.

En este orden de ideas, hay que remarcar que los supuestos delineados en la ciberestrategia de cada Estado establecen las pautas bajo las cuales los ejércitos informáticos se organizan y, del mismo modo, dirigen la forma sobre la que se ejecutan sus "operaciones de información", entendidas éstas últimas como el

> "[…] uso integrado de capacidades núcleo de Guerra Electrónica, Operaciones de la Red de Ordenadores, Operaciones Psicológicas [PSYOP], Engaño Militar, y Seguridad Operacional en concierto con apoyo específico y capacidades relacionadas, para influir, interrumpir, corromper o usurpar adversarios humanos y la toma de decisiones automatizadas mientras se protegen las propias."[37]

Estos puntos se detallarán más adelante, al hablar sobre los ataques empleados durante la ciberguerra. Con todo, es necesario mencionar que algunos países ya han puesto en operación ciberejércitos, entre ellos Estados Unidos, con el U.S. Cyber Command[38]; Corea del Norte, con la Unidad 121[39] e Irán, con el autonombrado Ciberejército Iraní[40]. A este respecto, es menester mencionar que dicha tendencia parece consolidarse cada vez más con el paso del tiempo, pues según el Informe sobre Criminología Virtual 2009 de la compañía de software

---

[37] Departamento de la Defensa, *Information Operations Roadmap*, [en línea], Departamento de la Defensa de Estados Unidos de América, 30 de octubre de 2003, Dirección URL: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf, [consulta: 12 de marzo de 2014]. Traducción propia.

[38] *Vid* U.S. Army-Cyber Command, *USCYBERCOM*, [en línea], U.S. Cyber Command, Dirección URL: http://www.arcyber.army.mil/org-uscc.html, [consulta: 24 de marzo de 2014].

[39] *Vid* Ward Carroll, *Inside DPRK's Unit 121*, [en línea], Defenstech, 24 de diciembre de 2007, Dirección URL: http://defensetech.org/2007/12/24/inside-dprks-unit-121/, [consulta: 24 de marzo de 2014].

[40] *Vid* Alex Lukich, *The Iranian Cyber Army*, [en línea], Center for Strategic & International Studies, 12 de Julio de 2011, Dirección URL: https://csis.org/blog/iranian-cyber-army, [consulta: 24 de marzo de 2014].

antimalicioso McAfee, diversos países han comenzado a desarrollar capacidades informáticas avanzadas, hecho que ha derivado en una especie de confrontación que comienza a minarse en las relaciones internacionales del mundo actual:

> "Si bien se puede decir que el mundo no ha asistido aún a una 'ciberguerra caliente', muchos expertos están convencidos de que los países están ya envueltos en una suerte de carrera armamentística silenciosa para dotarse de un arsenal cibernético. Dicho esto, la situación no es comparable con la carrera armamentística nuclear entre la Unión Soviética y EE. UU. tras la Segunda Guerra Mundial. Si aquello era similar a un duelo, la carrera por el armamento cibernético más bien parece una reyerta abierta a todos."[41]

Así pues, debido a la relevancia que el fenómeno comienza a tomar, los gobiernos alrededor del mundo se han visto en la necesidad de empezar a reclutar personal capacitado en nuevas tecnologías con el fin de no perder ventaja en lo que se avecina como un nuevo campo de conflicto: de ahí que, por ejemplo, muchas agencias de seguridad asistan a eventos civiles masivos con el fin de encontrar individuos con capacidades tecnológicos avanzadas, en específico, *hackers* y *crackers*.

Un *hacker* es cualquier persona que puede alterar o modificar el funcionamiento de cualquier sistema electrónico debido a sus altos conocimientos técnicos en informática, computación y procesos. De hecho, Richard A. Clarke los define como

> "[…] un usuario experto de software o hardware capaz de adaptar sistemas para hacer cosas para las que no estaban contemplados u originalmente diseñados. En el discurso cotidiano, sin embargo, el término ha sido utilizado para denostar a alguien que utiliza sus habilidades para ganar acceso a computadoras o redes sin autorización. Como verbo, "hackear" significa forzar la entrada a un sistema."[42]

---

[41] McAfee, *Informe sobre criminología virtual 2009: La era de la ciberguerra, casi una realidad*, [en línea], McAfee, Dirección URL: http://www.mcafee.com/mx/resources/reports/rp-virtual-criminology-report-2009.pdf, [consulta: 12 de febrero de 2013]
[42] Richard A. Clarke, *Op. Cit.*, p. 285.

El origen de los *hackers* se remonta a los llamados *phreakers,* quienes eran personas capaces de alterar las redes telefónicas con el fin de explorar los alcances que tenían los sistemas electrónicos de los años 80: John T. Draper, mejor conocido como Capitán Cruch*,* es una figura representativa de esta corriente. Más tarde, con el auge de la informática, muchos *phreakers* comenzaron a aplicar sus hazañas en los recién nacidos computadores, especialmente en los programas que permitían que éstos funcionasen, dando origen al movimiento *hacker* –que se ha preservado hasta el día de hoy con varias mutaciones. Básicamente, existen dos variaciones en los grupos *hackers*: sean éstos de sombrero blanco o, por el contrario, de sombrero negro.

Los *hackers* de sombrero blanco son todos aquellos individuos que son capaces

> "[…] de apreciar el valor del hackeo, el cual estriba en desmenuzar el funcionamiento de los programas, encontrando vulnerabilidades en ellos. Otras acepciones incluyen a quien es capaz de programar de manera rápida y expedita; o bien, al experto en un programa en particular o que trabaja frecuentemente usando cierto programa; como también el que está entusiasmado con cualquier tema; o bien, el que disfruta del reto intelectual de superar o rodear las limitaciones de forma creativa. En la práctica se le reconoce a los hackers [de sombrero blanco] la contribución que realizan para mejorar los sistemas de seguridad de la información en el ciberespacio, lo que sugería al menos en un primer momento, que lejos de tener intenciones malignas, sus motivaciones son casi científicas, incluyendo fuertes dosis de prestigio personal e intelectual."[43]

Contrariamente al papel desarrollado por este tipo de personas hábiles en la computación se encuentra el rol de los *crackers*, o *hackers* de sombrero negro, quienes

[43] María Cristina Rosas, *Op. Cit*.

> "[…] en realidad persiguen la destrucción o el colapso de la seguridad de un sistema. Se les considera como hackers sin ética, o bien hackers de sombrero negro, dado que sus motivaciones son, sobre todo, de tipo económico o político. Entre las variantes de los crackers figuran quienes hacen un uso ilegal de la información personal confidencial; los falsificadores que buscan obtener información de números de tarjetas de crédito, contraseñas, directorios o recibos; el phreaking o uso ilegal de las redes telefónicas; y los piratas, quienes se dedican a copiar software legal, música o vídeos."[44]

Son precisamente estos últimos quienes adquieren un papel de alta relevancia en los ciberconflictos pues, hasta el día de hoy, los piratas informáticos de sombrero negro han sido quienes han creado la mayor cantidad de software y herramientas maliciosas con el fin de causar disrupciones en los sistemas informáticos de quienes consideran son sus enemigos. Finalmente, cabe aclarar que, debido a que la principal motivación de los *crackers* es monetaria, éstos pueden actuar solos, con un grupo clandestino o incluso bajo el cobijo de un gobierno mediante todas las formas virtuales posibles.

Por su parte, los civiles merecen una mención especial en el tema de las ciberguerras ya que ellos participan indirecta e involuntariamente en éstas pues sus computadoras, al verse infectadas por un software malicioso, pueden ser contraladas remotamente por una persona que encause los esfuerzos de la maquina hacia un ataque virtual masivo con consecuencias devastadoras, Todo esto sin que el usuario o controlador de la máquina mismo se percate de la situación:

> "El usuario puede notar que su laptop está funcionando un poco lento o que el acceso a las páginas de Internet está tomando un poco más de tiempo que el normal, pero eso solo es un indicador [de que el ataque está en marcha]. La actividad maliciosa está tomando lugar en el fondo sin aparecer en la pantalla del usuario. Su computadora, ahora mismo, está siendo parte de un botnet."[45]

[44] *Idem.*
[45] Richard A. Clarke, *Op. Cit.*, p. 14.

A esta lista podrían sumarse también empresas transnacionales, corporaciones privadas de seguridad, grupos activistas, organizaciones criminales, grupos terroristas y Organizaciones no Gubernamentales; reafirmando, de nueva cuenta, la premisa de las nuevas guerras enunciada en el capítulo anterior: la de la participación de múltiples actores en los fenómenos bélicos de nueva generación en los más distintos entornos y con las más variadas actividades. De igual forma, este nuevo escenario de conflictos demuestra el desvanecimiento del control del Estado en ciertas áreas que anteriormente eran de su jurisdicción y, por el contrario, muestra el empoderamiento que ha adquirido el individuo y los grupos de particulares debido a las nuevas circunstancias que predominan en el escenario internacional actual.

2.3 Instrumentos de ataque y casos representativos.

Con la parte de los actores involucrados en los conflictos cibernéticos aclarada, toca el turno de profundizar sobre los ataques que cada uno de estos grupos pueden ejercer dentro de un escenario de ciberguerra. Al respecto, existe un esquema totalizador creado por el Centro de Génova para el Control Democrático de las Fuerzas Armadas (DCAF, por sus siglas en inglés) que muestra de manera clasificada las herramientas ofensivas más utilizadas durante una batalla virtual, a saber:

Categorías de ataques cibernéticos.		
Categoría	**Sub-categoría**	**Ejemplos**
Integridad Los ciberataques pueden utilizar técnicas para modificar, destruir o hacer otras acciones que comprometan la integridad de los datos.	Propaganda/desinformación	Modificación o manipulación de datos o introducción de datos contradictorios para influir en resultados políticos o de negocios o desestabilizar un régimen extranjero.
	Intimidación	Ataques a sitios web para ejercer coerción sobre sus dueños (públicos y privados) para remover o modificar contenido, o perseguir otros fines.
	Destrucción	Destrucción permanente de datos para afectar competidores o atacar gobiernos extranjeros. Esto puede ocurrir, por ejemplo, dentro de un conflicto más grande.

Disponibilidad Ataques de denegación de servicio ejecutados por botnets, por ejemplo, pueden ser utilizados para prevenir que usuarios acceden a datos que de otra manera no estarían disponibles.	Información externa	Denegación de servicio, etc. Ataques contra servicios del gobierno o privados disponibles para el público, por ejemplo, medios de comunicación, sitios de información gubernamentales, etc.
	Información interna	Ataques a intranets gubernamentales o privadas, por ejemplo, redes de servicios de emergencia, sitios de banca electrónica, email corporativo, sistemas de control y comando, etc.
Confidencialidad Los ciberataques pueden apuntar a varios tipos de información confidencial, regularmente para propósitos criminales.	Espionaje	Firmas buscando información sobre sus competidores; Estados envueltos en actividades espías (contra gobiernos extranjeros e individuos.)
	Robo de datos personales	Ataques de falsificadores (o similares) dirigidos a usuarios débiles para revelar datos personales, , como números de cuentas bancarias; virus que almacenan y suben datos desde una computadora de un usuario.
	Robo de identidad	Troyanos, y demás, usados para robar la información de identidad y utilizarla para cometer crímenes.
	Minería de datos	Técnicas de código abierto empleadas para descubrir, por ejemplo, información personal de información disponible públicamente.
	Fraude	Generalmente enviado vía email mediante spam, el fraude incluye el popular Nigeriano “419” o técnicas avanzadas de fraude, así como intentos de convencer al destinatarios para comprar servicios o bienes fraudulentos.

Tabla 1. Categorías de ataques cibernéticos. **Fuente:** DCAF, *Democratic Governance Challenges of Cyber Security*, [en línea], Génova, DCAF, 2009, Dirección URL: http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security.
Traducción propia.

Vale la pena resaltar y explicar algunos de los ataques más utilizado de la tabla anteriormente citada, sobre todo por la relevancia que tienen en el análisis de nuestro caso de estudio. Sin embargo, antes de continuar es necesario señalar y no dejar de remarcar que todas estas ofensivas se llevan a cabo a través del ciberespacio; una dimensión más en el mundo que viene a complementar al espacio marítimo, aéreo, terrestre y espacial. Según Daniel T. Kuehl, el ciberespacio es

> "[…] un dominio global dentro del ambiente de la información cuyo carácter único y distintivo está enmarcado en el uso de aparatos electrónicos y del espectro electromagnético para crear, guardar, modificar, intercambiar, y explotar información a través de redes interdependientes e interconectadas usando tecnologías de la información y comunicaciones."[46]

Aclarado esto, se procede a profundizar sobre las herramientas de ataque informático más utilizadas en los grandes conflictos cibernéticos que se han dado en los últimos años, éstas son: el software malicioso, la infección mediante gusanos, el uso de *trapdoors*, el empleo de ataques *DDoS* así como el ciberespionaje.

El software malicioso (conocido comúnmente como virus informático) es, según la corporación de seguridad informática Panda Security, todo aquel

> "[…] programa informático diseñado para infectar archivos. Además, algunos podrían ocasionar efectos molestos, destructivos e incluso irreparables en los sistemas sin el consentimiento y/o conocimiento del usuario.
>
> "Cuando se introduce en un sistema normalmente se alojará dentro del código de otros programas. El virus **no actúa hasta que no se ejecuta el programa infectado.** Algunos de ellos, además están preparados para activarse cuando se cumple una determinada condición (una fecha concreta, una acción que realiza el usuario, etc.).
>
> "El término virus informático se debe a **su enorme parecido con los virus biológicos.** Del mismo modo que los virus biológicos se introducen en el cuerpo humano e infectan una célula, que a su vez infectará nuevas células, los virus informáticos se introducen en los ordenadores e infectan ficheros insertando en ellos su 'código'. Cuando el programa infectado se ejecuta, el código entra en funcionamiento y el virus sigue extendiéndose.
>
> "Los virus se pueden clasificar en función de múltiples características y criterios: según su funcionalidad, las técnicas que utilizan para infectar, los tipos de ficheros que infectan, los lugares donde se alojan, el sistema operativo o la plataforma tecnológica que atacan, etc."[47]

[46] Daniel T. Kuehl, *Op. Cit.*, p. 28. Traducción propia.
[47] Panda Security, *Virus informático: una categoría con una larga trayectoria que permanece al margen de la nueva dinámica del malware*, [en línea], Panda Security, Dirección URL:

Uno de los eventos históricos más famosos que involucró el uso de virus informáticos sucedió entre 2008 y 2010 y, de hecho, varios expertos coinciden en que aquél ataque evidenció la letalidad guardada tras una ciberguerra. En ese año, Irán fue presa de un software malicioso llamado *Stuxnet*, el cual, según la corporación de seguridad informática Kaspersky Lab, era "un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial."[48]

Dicho programa malicioso era uno de los sistemas de espionaje de sistemas computarizados más avanzados del mundo y, adicionalmente, era capaz de modificar o dañar a voluntad el código informático que hace funcionar a las operaciones de programas de *Supervisory Control And Data Acquisition* (SCADA, por sus siglas en inglés), sistemas hechos para controlar y monitorear procesos industriales de extrema importancia a distancia, como un línea armadora de vehículos automotores, el funcionamiento de una planta de energía eléctrica o incluso hasta la operación de una central nuclear.

En el caso de la República Islámica de Irán, este virus infectó durante el año 2010 a los sistemas computarizados de 5 instalaciones industriales que estaban incorporadas al programa nuclear del Presidente Ahmadineyad, causando varios problemas técnicos al desarrollo del mismo[49]. Si bien la presencia del software malicioso sólo derivó en la obstrucción de algunos procesos automatizados, éste también demostró su potencial destructivo al contagiar a diversos equipos informáticos del personal de la planta de energía nuclear de Bushehr, hecho que pudo desencadenar una catástrofe mayor de no haber sido detectado pues, como

---

http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/virus/, [consulta: 25 de febrero de 2013].

[48] Kaspersky Lab, *Kaspersky Lab provides its insights on Stuxnet* worm, [en línea], Kaspersky Lab, 2010, Dirección URL: http://www.kaspersky.com/news?id=207576183, [consulta: 7 de mayo de 2013]. Traducción propia.

[49] *Vid* S/a, *Stuxnet hits Iran nuclear* plans, [en línea] , BBC, 22 de noviembre de 2010, Dirección URL: http://www.bbc.co.uk/news/technology-11809827, [consulta: 8 de mayo de 2013].

anteriormente se mencionó, *Stuxnet* pudo alterar las indicaciones de las máquinas controladoras de los procesos de la planta dándoles a éstas instrucciones que derivarían en procesos inadecuados y, por lo tanto, peligrosos, convirtiendo así a la instalación en un gigantesca bomba de tiempo.[50]

Debido al objetivo del ataque, así como a su naturaleza y complejidad, no tardaron en surgir teorías de conspiración respecto al origen del software malicioso, sobre todo aquellas que envolvían la participación de un Estado extranjero, hecho que se comprobó tras el análisis exhaustivo del virus informático a cargo de las compañías de antivirus más respetadas del mundo: resulta que se encontraron rastros ocultos entre el código informático de *Stuxnet* que evidenciaron la participación de dos Estados enemigos de la República Islámica de Irán en el desarrollo de la letal aplicación de ordenador, Estados Unidos de América e Israel.[51] Fue de tal trascendencia este hecho que incluso la propia Organización del Tratado del Atlántico Norte (OTAN, por sus siglas en ingles), a través de sus expertos en temas legales, anunció que el episodio iraní era un "Acto de Fuerza" totalmente ilegal.[52]

Aún con toda la atención de los diversos actores de la política internacional en este nuevo tipo de armas éstas no han dejado de surgir, pues posterior a la aparición de *Stuxnet* comenzaron a ser descubiertos nuevos virus de la misma índole y complejidad, como *Flame*, *Gauss* y *Duqu*; escenario que demuestra que esta tendencia seguirá presente a los largo del presente siglo.

---

[50] *Vid* S/a, *Stuxnet worm hits Iran nuclear plant staff* computers, [en línea] BBC, 26 de septiembre de 2010, Dirección URL: http://www.bbc.co.uk/news/world-middle-east-11414483, [consulta: 8 de mayo de 2013].

[51] *Vid* S/a, *US-Israeli Stuxnet Cyber-Attacks against Iran: "Act of War",* [en línea], Center for Research on Globalization, 25 de marzo de 2013, Dirección URL: http://www.globalresearch.ca/us-israeli-stuxnet-cyber-attacks-against-iran-act-of-war/5328514, [consulta: 8 de mayo de 2013].

[52] *Vid* Kim Zetter, *Legal experts: Stuxnet Attack on Iran was Illegal "Act of Force"*, [en línea], Wired, 25 de marzo de 2013, Dirección URL: http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/, [consulta: 8 de mayo de 2013].

Ahora bien, cuando un virus informático tiene la capacidad de expandirse hacia otros equipos recibe el nombre de gusano (*worm* en inglés). Un gusano aparece "cuando una computadora atomiza su infección hacia otras, y esas otras hacen lo mismo […] La infección gusano es la que va de una computadora a otra través de miles de millones de éstas. Una infección puede expandirse por el globo en cuestión de horas."[53] *Stuxnet* constituye nuevamente un ejemplo claro de este tipo de herramientas, sin embargo, para demostrar aún más su capacidad destructiva se procede a analizar otro caso relevante que involucra a este tipo de software malicioso: el gusano ILOVEYOU.

ILOVEYOU fue un gusano descubierto en mayo del año 2000 que logró expandirse a través del correo electrónico a millones de equipos de cómputo alrededor del mundo en aproximadamente 6 horas, consagrándose con este hecho como el primer *worm* causante de una infección computarizada masiva en el globo y, también, como un parteaguas en la industria de la seguridad informática.[54]

El gusano informático, distribuido a través de un fichero de correo electrónico, era capaz de crear varios agujeros de seguridad en el directorio de las computadoras infectadas haciendo que éstas colapsarán al tiempo que expandían automáticamente la infección, causando al mismo tiempo un enorme tráfico en la red debido a la masiva cantidad de e-mails enviados por todos los equipos informáticos objetivos. Fue tal la destrucción generada por ILOVEYOU que se calcula que su aparición en el mundo costó entre 5 y 9 mil millones de dólares.[55]

Cabe mencionar que entre los distintos afectados, además de grandes empresas de renombre y organizaciones internacionales, también resultaron dañadas instituciones gubernamentales críticas, entre ellas el Pentágono de

[53] Richard A. Clarke, p. 14. Traducción propia.
[54] *Vid* Robert Lemos, *Inside the ILOVEYOU worm*, [en línea], ZDNET, 5 de mayo de 2000, Dirección URL: http://www.zdnet.com/news/inside-the-iloveyou-worm/107344, [consulta: 9 de mayo de 2013].
[55] *Vid* Charles R. Hooper, *The ten worst computer viruses,* [en línea], TopTen Reviews, Dirección URL: http://anti-virus-software-review.toptenreviews.com/the-ten-worst-computer-viruses.html/?cmpid=ttr-llm, [consulta: 9 de mayo de 2013].

Estados Unidos y el Parlamento de Gran Bretaña.[56] Dicho escenario mostró la enorme vulnerabilidad de los organismos públicos ante este tipo de ataques, aún cuando el gusano no fue ideado específicamente para ese propósito.

Este tipo de software malicioso da pie para entender a un nuevo elemento de este amplio abanico de armas cibernéticas, en específico, el *trapdoor* o troyano, también conocido como *backdoor* en la jerga computacional. Un troyano "es una serie de líneas de código de cómputo que aparentan ser iguales a las del programa pero que comprometen o modifican las instrucciones para el funcionamiento de un sistema operativo o una aplicación."[57] Ahora bien, las formas en las que un equipo informático puede verse vulnerado por este tipo de herramientas son varias, por ejemplo, mediante *hackeo* externo, virus o incluso de forma intencional como sucedió en un suceso reciente que involucró a Estados Unidos y a China.

A mediados del año 2012, investigadores de la Universidad de Cambridge descubrieron que el chip Microsemi/Actel ProASIC3, manufacturado en China y empleado en Estados Unidos, contenía dentro de su código informático un *backdoor* capaz de reprogramar las instrucciones del dispositivo que, dicho sea de paso, es utilizado en la industria militar así como en infraestructura crítica de dicho país[58]. Después de que el gobierno estadounidense diera cuenta de la peligrosidad del hecho (pues el chip podía ser remotamente desactivado o podía dar instrucciones letales a la maquinaria que controlaba), éste reclamo de manera directa a la cúpula del gobierno chino. De inmediato, la República Popular negó que tuviera que ver algo en el asunto, tesis que el mismo investigador que dio aviso de la situación sospechosamente corroboró[59]; sin embargo, expertos coinciden en que existe una

---

[56] *Vid* Pedro de Alzaga yEnric Pastor, *El "virus del amor" colapsa ordenadores de todo el mundo*, [en línea], El Mundo, 5 de mayo de 2000, Dirección URL: http://www.elmundo.es/navegante/2000/05/05/ailofiu_virus.html, [consulta: 9 de mayo de 2013].
[57] Richard A. Clarke, *Op. Cit.,* p.7. Traducción propia.
[58] *Vid* Shane McGlaun, *Report: Chinese built US military chip has a backdoor,* [en línea], TG Daily, 29 de mayo de 2012, Dirección URL: http://www.tgdaily.com/security-brief/63684-report-chinese-built-us-military-chip-has-a-back-door, [consulta: 13 de mayo de 2013].
[59] *Vid* Michael Lee, *China not behind US military chip* backdoor, [en línea], ZDNet, 30 de mayo de 2012, Dirección URL: http://www.zdnet.com/china-not-behind-us-military-chip-backdoor-1339338798/, [consulta: 13 de mayo de 2013].

alta probabilidad de que el gobierno chino esté realizando estos actos de forma deliberada, sobre todo después de que un analista del Pentágono descubriera en el presente año que el 80% de las telecomunicaciones a nivel global tienen un *trapdoor* cuyo origen se remonta al país asiático, el cual ha sido distribuido, entre otros medios, a través de empresas como Huawei y ZTE.[60]

Este último hecho hizo ver el potencial de espionaje que comenzaban a tener algunos actores de la política mundial a través de medios electrónicos, práctica conocida como ciberespionaje. El ciberespionaje es

> "[…] una forma de cibercrimen en la cual hackers atacan redes de computadoras para ganar acceso a información clasificada o de otro tipo que es redituable o ventajosa para el hacker. El ciberespionaje es un proceso continuo cuyo único objetivo es la obtención de información confidencial que puede ser usada para provocar desde desastres económicos hasta terrorismo.
> "Los resultados potencialmente nocivos del ciberespionaje no sólo causan fallos de seguridad en los sistemas gubernamentales, sino también pueden conducir a la desclasificación de secretos de corporaciones comerciales."[61]

Al igual que la mayoría de las otras herramientas informáticas, el ciberespionaje puede ser llevado a cabo por una persona o por un grupo de ellas, así como por empresas, gobiernos y organizaciones. Existen muchos casos sobresalientes relativos a esta novedosa forma de espionaje, sin embargo, la operación más famosa y reciente fue la descubierta por la corporación de seguridad Kaspersky Lab en octubre del año 2012: la operación *Red October*.

---

[60] *Vid* Emil Protalinskyi, *Former Pentagon analyst: China has backdoors to 80% of telecoms,* [en línea], ZDNet, 14 de julio 2012, Dirección URL: http://www.zdnet.com/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms-7000000908/, [consulta: 13 de mayo de 2013].

[61] Cory Janssen, Cyberspyng, [en línea], Techopedia, Dirección URL: http://www.techopedia.com/definition/27101/cyberspying, [consulta: 16 de mayo de 2013]. Traducción propia.

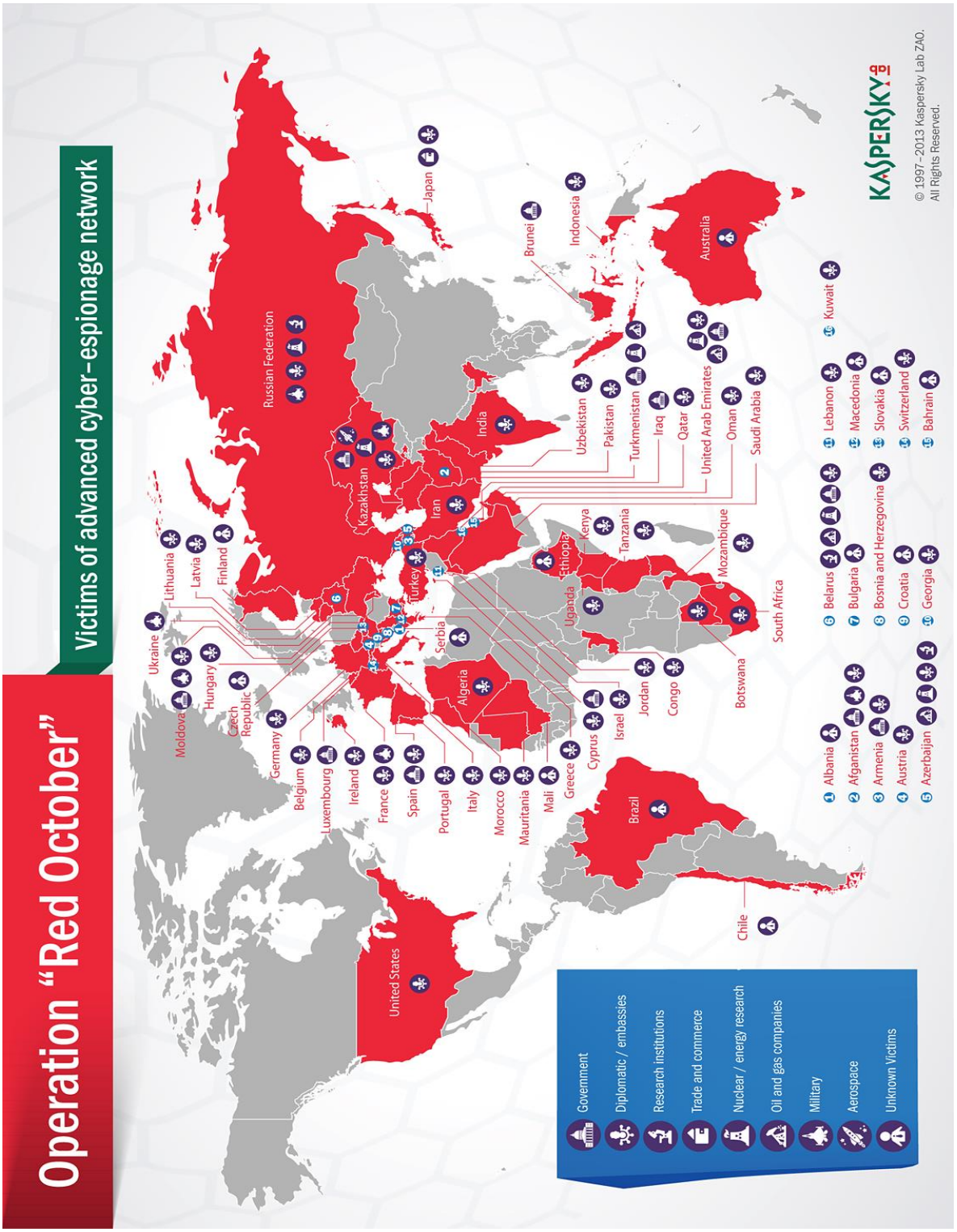

Figura 1. Mapa de las víctimas de la operación Red October. **Fuente**: Kaspersky Lab, *The "Red October" Campaign- An advance cyber espionage network targeting diplomatic and government agencies*, [en línea], Kaspersky Lab, 14 de enero de 2013, Dirección URL: http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies, [consulta: 17 de mayo de 2013].

Red October es una red de espionaje electrónico que ha obtenido información crítica de diversos gobiernos, embajadas, corporaciones, Organizaciones No Gubernamentales y otros entes (véase la figura 1) a través del uso de herramientas informáticas como virus y SPAM. Si bien se desconoce el origen de la operación, se piensa que, por su complejidad, ésta fue llevada a cabo por un grupo de *crackers* profesionales cobijados por algún ente estatal.[62]

Para cerrar esta serie de herramientas virtuales potencialmente peligrosas citaremos uno de los métodos más utilizados por los cibercombatientes de la actualidad, el *Distributed Denial of Service*, mejor conocido como ataque *DDoS*. El *DDoS,* según Richard A. Clarke, es…

> "[…] un congestionamiento preprogramado del tráfico de Internet diseñado para destruir o interferir en la red. Es 'distribuido' en el sentido de que miles, sino cientos de miles, de computadoras son ocupadas para enviar pings electrónicos a objetivos locales plenamente identificados en Internet. Las computadoras atacantes se llaman 'botnets', una red robótica de 'zombis', computadoras que están bajo control remoto. Los atacantes zombis siguen comandos que han sido cargados dentro de ellas sin que sus dueños lo sepan."[63]

La particularidad y peligrosidad de los ataques *DDoS* reside en que éstos pueden aislar las redes informáticas de un país entero congestionándolas, causando un enorme caos en todos los estratos sociales del Estado así como en su infraestructura física. Incluso, la capacidad de estos ataques es tal que pueden tener consecuencias a nivel global: baste con mirar lo ocurrido a principios del año 2013, cuando se desató el ataque *DDoS* más grande en la historia de Internet entre dos compañías informáticas, Spamhaus y Cyberbunker, cuyas consecuencias se resintieron en todo el entramado electrónico que conforma a la totalidad de Internet en el mundo, haciendo que éste se congestionara y experimentara diversos

[62] *Vid* Kaspersky Lab, *Op. Cit*.
[63] Richard A. Clarke, *Op. Cit.*, pp. 13-14. Traducción propia.

problemas técnicos en su operación[64]. Además de este ejemplo, existe uno aún más emblemático que, según los expertos, representa el nacimiento formalmente consolidado de las ciberguerras: el relativo a la guerra ruso-georgiana de 2008, misma que constituye el caso de estudio de la presente investigación y que se analizará a profundidad en el siguiente capítulo tomando en cuenta los cánones hasta ahora desarrollados.

Así pues, el presente capítulo concluye concentrando todas las características sobresalientes de las ciberbatallas de hoy, entre ellas su carácter permeado de los grandes avances tecnológicos desarrollados hasta la fecha, la facilidad con la que se pueden emprender (no necesitan de debates en los congresos nacionales o de diálogo internacional), la rápida velocidad a la que se desarrollan así como gran alcance y capacidad para crear escenarios de crisis a lo largo del planeta o; como diría Richard A. Clarke…

> "La ciberguerra ocurre a la velocidad de la luz. Cuando los fotones de los paquetes de ataque viajan a través del cable de fibra óptica, el tiempo entre el ataque y su efecto es raramente medible, creando riesgos de crisis para los tomadores de decisiones.
> "La ciberguerra es global. En cualquier conflicto, un ciberataque puede hacerse rápidamente global, cuando son adquiridas computadoras hackeadas a través del mundo y éstas se ponen en servicio, muchas naciones pueden verse implicadas.
> "La ciberguerra evade el campo de batalla. Los sistemas en que las personas confían, desde bancos hasta sistemas aéreos de defensa, son accesibles desde el ciberespacio y pueden ser rápidamente inhabilitados o tirados sin vencer primero a las fuerzas tradicionales de cualquier nación."[65]

Con esto aclarado, se procede a analizar en el siguiente apartado al ciberconflicto librado entre Georgia y Rusia en agosto de 2008, no sin antes describir el proceso que llevó al desarrollo del mismo.

---

[64] *Vid* S/a, *El ciberataque más fuerte que reduce la velocidad de Internet*, [en línea], BBC Mundo, 27 de marzo de 2013, Dirección URL: http://www.bbc.co.uk/mundo/ultimas_noticias/2013/03/130327_ultnot_ciberataque_afecta_velocidad_internet.shtml, [consulta: 22 de mayo de 2013].
[65] *Ibidem*, p.31 Traducción propia.

Capítulo 3. El otro campo de batalla: el emplazamiento de una ciberguerra a gran escala durante el conflicto ruso-georgiano de 2008.

> *"No fue una guerra entre los Estados, y sobre todo, no una guerra entre el pueblo ruso y el pueblo georgiano. Fue una operación de imposición de la paz."* Dmitri Medvédev, *en entrevista sobre el aniversario del conflicto entre Rusia y Georgia en 2008.*[66]

Para comprender a bien la ciberguerra librada entre Rusia y Georgia en agosto del año 2008 es necesario generar anticipadamente un contexto que dé cuenta de la naturaleza de las relaciones e interacciones que han tenido estos dos países a lo largo de la historia. Dicha situación nos llevará a explicar el ascenso al poder del presidente georgiano, Mijeíl Saakashvili, así como el inicio del conflicto militar acaecido en esos territorios durante su gestión, hecho que a su vez servirá como un marco para desarrollar el análisis sobre el operativo virtual que fue paralelo a esta batalla.

3.1 Georgia y Rusia, una relación difícil.

Georgia es un pequeño Estado ubicado en la región conocida como Eurasia. De acuerdo con la *Central Intelligence Agency* (CIA), este país tiene una extensión territorial de aproximadamente 69,700 km^2 y una población total de 4, 555, 911 habitantes; ambos datos cotejados al mes de julio de 2013[67]. Su historia se remonta hasta el periodo que comprende los años 550 al 164 a.C., cuando los reinos de Colchis y Kartli-Iberia se formaron en el área que comprende a su soberanía actual. Cabe mencionar que a lo largo de su formación como nación, Georgia ha sufrido múltiples invasiones así como anexiones a grandes imperios de la historia mundial,

---

[66] S/a, *Medvédev a RT: "No hubo una guerra entre Rusia y Georgia, sino imposición de la paz",* [en línea], RT, 4 de agosto de 2013, Dirección URL: http://actualidad.rt.com/actualidad/view/102052-medvedev-rt-entrevista-georgia-rusia-guerra, [consulta: 27 de agosto de 2013].

[67] *Vid* Central Intelligence Agency, *Georgia,* [en línea], CIA, Dirección URL: https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html, [consulta: 25 de junio de 2013].

hechos que han forjado los problemas a los que se enfrenta en la actualidad así como su rol dentro del entramado internacional.

Por su parte, Rusia es el segundo país más grande del mundo y por esta situación abarca prácticamente dos regiones: Europa y Asia. La CIA refiere que el Estado ruso tiene una extensión de 17, 098, 242 km^2 con una población de 142, 500, 482 habitantes[68]. Los orígenes de esta nación se remontan al siglo XII, cuando el Principado de Moscú pudo librarse de la dominación mongola iniciando así la actitud imperialista que siempre ha caracterizado a dicho país, misma que se materializó con la conformación del Imperio Ruso y, posteriormente, con la construcción de la Unión de Repúblicas Socialistas Soviéticas (URSS).

Ahora bien, los primeros contactos entre ambas naciones se dieron durante el siglo XII, siendo éstos estrictamente económicos, culturales y muy pocas veces de carácter político. Fue hasta el periodo comprendido entre los siglos XVI a XVIII cuando las relaciones entre los dos países se intensificaron debido a que ambos eran Estados cristianos ortodoxos, sin embargo, existía un escenario más que hacia que Georgia experimentará un vínculo extremadamente estrecho con el gobierno ruso: durante esa época, los territorios del pequeño país euroasiático sufrieron múltiples invasiones de imperios extranjeros, entre los que destacaron el Mongol y, posteriormente, el Persa. Ante el asedio extranjero, Georgia pedía con regularidad a Rusia ayuda militar en estos conflictos al grado de que, para el año 1782, el Rey de Kartli-Kakheti –Irakli II- solicitó formalmente a la Emperatriz Catalina su protección, dando lugar al nacimiento del Tratado de Gueorguievsk de 1783.[69]

Dicho instrumento jurídico no era más que la culminación de las estrechas relaciones de amistad que habían nacido a partir de la cooperación militar, y aunque

---

[68] *Vid* Central Intelligence Agency, *Russia*, [en línea], CIA, Dirección URL: https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html, [consulta: 25 de junio de 2013].

[69] *Vid* RIA Novosti, *Tratado de Gueorguievsk entre Rusia y Georgia (1783). Infografía*, [en línea], RIA Novosti, Dirección URL: http://sp.ria.ru/infografia/20080813/116008448.html, [consulta: 26 de junio de 2013].

el Tratado se suspendió durante la guerra entre el imperio Ruso y el Turco-Otomano por poco más de 4 años, éste demostró que existía cierta afinidad entre ambas naciones de aquella región del mundo.

Así pues, la gran afinidad cultural y religiosa así como la alianza estratégica y militar que Rusia y Georgia habían formado hasta ese momento, en adición con una coyuntura política vivida en el pequeño país euroasiático, dieron pie a un escenario que posibilitaría la anexión de este último país al gran imperio de Eurasia: primero se unió el reino de Irakli y, posteriormente, los demás territorios que ocupaban las tierras de la actual Georgia, todo ello impulsado por la cooperación bélica que se dieron mutuamente durante las guerras contra el imperio Turco-Otomano (1804-1813, 1826, 1828) y Persia (1806-1812 y 1829).[70]

Sin embargo, a partir del momento de la anexión iniciaría una relación de amor y odio entre ambos entes: por un lado, la incorporación de Georgia al gran Imperio Ruso impulsó el desarrollo y la modernización económica e industrial de aquél debido a la gran influencia y poder que comenzaban a obtener los Zares en el mundo. De igual manera, este escenario alentó la cohesión de los pueblos asentados en territorio georgiano así como la afinidad de éstos con los grandes conglomerados rusos. Sin embargo, y desde otro punto de vista, ésta fue también una época que fomentó una gran opresión de parte del imperio contra el pequeño país de Eurasia a través de su política colonial: de hecho, el saqueo de recursos y la explotación de los pueblos fue de tal magnitud que comenzaron a nacer grandes movimientos populares que protestaban contra la opresión militar y social, mismos que eran reprimidos de manera brutal por los rusos mediante el uso de pogromos –linchamientos multitudinarios-.[71]

[70] *Vid* RIA Novosti, *Historia de las relaciones entre Rusia y* Georgia, [en línea], RIA Novosti, 6 de septiembre de 2010, Dirección URL: http://sp.ria.ru/opinion_analysis/20100906/127670666.html, [consulta: 26 de junio de 2013].
[71] *Vid Idem.*

Fue tal la represión durante este periodo que, para 1917, se formó un órgano de gobierno provisional para ganarle terreno político a Rusia así como unidades militares y una guardia nacional para defenderse de la misma. Un año más tarde, el Comisariado Especial de Transcaucasia (que es como se llamaba dicha institución) proclamó la independencia de Georgia, específicamente, el 26 de mayo de 1918. Para garantizar su soberanía, este nuevo Estado independiente solicitó el apostamiento de tropas alemanas, turcas y más adelante británicas en su territorio. Sin embargo, tres años más tarde, y aún con el apoyo externo, Georgia cayó en manos de la naciente Unión de Repúblicas Socialistas Soviéticas (URSS) debido a una insurrección popular alentada y apoyada por el mismísimo Ejército Rojo. Este último hecho obligó a que este Estado adoptará una política alineada con el socialismo[72].

A partir de ese momento, Georgia entró en otro periodo de mejoras, sobre todo en el sector agrícola y, de la misma forma, el mandato soviético alentó la creación de nuevos sectores de producción, sin embargo, y como ocurrió en el pasado, el gobierno moscovita puso en marcha políticas violentas y ruines con el fin de debilitar a la cúpula georgiana de poder así como garantizar su influencia en dicho país. Dicho proceso se instauraría en esta nación por poco más de 70 años.

Fue entonces hasta el 31 de marzo de 1991 cuando Georgia, después de múltiples intentos por emanciparse de los rusos, logra recuperar su independencia en un contexto favorable para alcanzar la misma pues, para ese entonces, la URSS se estaba desintegrando y los ánimos en los pueblos subyugados estaban en su máximo esplendor. No obstante, y aún con ese desafío completado, el país emprendió nuevamente un periodo de inestabilidad política por poco más de 15 años.

[72] *Vid* s/a, *Temporary revival of Independence and reconquer of Georgia by Russia. (1918-1921)*, [en línea], Parlamento de Georgia, Dirección URL: http://www.parliament.ge/pages/archive_en/history/his11.html, [consulta: 27 de junio de 2013].

Después de las dificultades para establecer un gobierno sólido llegó al poder en 2008 Mijeíl Saakashvili, un prominente abogado de cosmovisión occidental que sería capaz de encausar la mayoría de los esfuerzos políticos de todo el país para su elección usando una estrategia política bastante efectiva: sus promesas de campaña se fundamentaban en el supuesto de que impediría como fuese la injerencia e influencia negativa rusa en su país. Este hecho, junto con el gran apoyo de Occidente hacia su candidatura, serían de vital importancia para el desarrollo del conflicto que se daría entre ambos países poco tiempo después.

3.1 El gobierno Saakashvili: influencia externa y políticas antirusas.

Misha, como es conocido Saakashvili en Georgia, llegó a la presidencia del pequeño país del Cáucaso apoyado por una gran mayoría de políticos nacionales y, además, por el soporte otorgado por varios países de Occidente, entre ellos Estados Unidos. A lo largo de sus discursos, el mandatario georgiano dejaba entrever que su gobierno iba a emprender políticas antirusas extremadamente definidas, hecho que marcaría una enorme diferencia entre él y todos sus antecesores en el cargo. En este sentido, lo que tenía más relevancia en el discurso y quehacer de Mijeíl recaía en dos elementos primordiales e inseparables: primero, el cuidado de la integridad del territorio soberano georgiano y, en segundo lugar, la protección de los recursos apostados en el mismo.

El mensaje de la integridad del territorio georgiano tocaba a su vez dos cuestiones: el estatus de Osetia del Sur y Abjasia. El primer distrito se había declarado independiente en diversas ocasiones (1989, 1990, 1992) y, con dicha acción, se habían desato cruentos conflictos oseto-georgianos que desbocaron en miles de muertos y grandes pérdidas económicas para el Estado entero. Sin embargo, estos acontecimientos disminuyeron con la firma de un acuerdo entre Rusia y Georgia a mediados del año 1992 en el cual se acordó el apostamiento de fuerzas de paz de ambas naciones en dicho territorio. Este escenario de relativa tregua impulsó nuevamente una declaración de independencia en el año 2006, hecho que no suscitó inmediata violencia pero que sin embargo generaría una

enorme tensión en Eurasia, misma que sería desfogada ahí mismo dos años después. Por su parte, en lo que respecta a Abjasia, ésta se independizó en el año de 1992 debido a los roses étnicos entre el gobierno georgiano y la cúpula de poder abjasia, situación que provocó un estallido bélico que terminó en un gran número de muertos. Aun cuando hubo un acuerdo de cese al fuego en 1994, en el año 2006 el conflicto se reavivó y, nuevamente, hubo una batalla de grandes dimensiones; sin embargo, aún con esto, Abjasia sigue considerándose como un Estado independiente ajeno a Georgia, mientras que éste último, contrariamente, le concede el estatus de República Autónoma integrada a su territorio.[73]

Respecto a la cuestión de los recursos, es conocido que la zona del Cáucaso es extremadamente estratégica debido a los energéticos que posee, entre ellos gas y petróleo. De igual manera, esta región es un punto de encuentro entre dos continentes, Europa y Asia, hecho que repunta todavía más su potencial geoestratégico. Finalmente, no hay que perder de vista que por estos territorios circulan enormes gasoductos rusos que proveen de este material al continente europeo, situación que aumenta aún más la tensión que desde principios del siglo pasado tienen ambos países[74].

Con todo esto en mente, Misha -junto con todos sus aliados extranjeros- no podía seguir tolerando el abuso que Rusia había perpetuado a su país desde hace tiempo y, en este sentido, emprendió una campaña bélica para que su gobierno fuera un parteaguas en la historia nacional: sería, pues, la administración que restauró a pleno la soberanía georgiana. Sin embargo, ante la falta de mesura política, los planes de Saakashvili para recuperar a las regiones separatistas por medio de la violencia no fueron del todo efectivos, pues no contaba con que su

[73] *Vid* United Nations News Centre, *Situation around Abkhazia and South Ossetia: Historical Overview*, [en línea], United Nations News Centre, Dirección URL: http://www.un.int/russia/new/MainRoot/docs/warfare/statement051208en.htm, [consulta: 9 de julio de 2013].
[74] *Vid* Ana Teresa Gutiérrez del Cid, *La OTAN y el conflicto Georgia-Rusia por Osetia del Sur,* [en línea], Revista de Relaciones Internacionales-UNAM, Dirección URL: http://www.journals.unam.mx/index.php/rri/article/download/16322/15528, [consulta: 11 de julio 2013].

contraparte rusa respaldaría a estos bastiones geopolíticos con una robusta maquinaria de guerra así como con el emplazamiento del nuevo tipo de conflicto que hemos venido revisando: una ciberguerra.

3.3 La guerra ruso-georgiana de 2008: desarrollo y dimensiones.

El 7 de agosto de 2008 a la media noche inició el movimiento castrense que sacudiría la débil estabilidad de la zona euroasiática: en ese momento, las fuerzas militares georgianas bajo la orden de Saakashvili emprendieron un ataque armado contra Osetia del Sur, específicamente en su capital Tsjinval. El nombre clave de la operación, según fuentes rusas, era "Campo Limpio" y, como era de esperarse, ésta tenía como primordial objetivo recuperar el territorio oseto y reintegrarlo a la soberanía georgiana mediante el uso de la fuerza.

El ataque inicial de Misha comprendió el uso de aproximadamente 12,000 tropas terrestres y de 75 unidades de acorazados, entre los que destacaban los tanques T55 y T62. Dicha operación estaba respaldada también con unidades de artillería de calibres 122 y 155 mm así como con morteros y lanzadores múltiples.[75] Por su parte, las Fuerzas de Autodefensa de Osetia del Sur esperaban hacerle frente a este movimiento con 2,500 efectivos, 15 tanques T55 y T72 así como con poco más de 50 vehículos de combate. De igual forma, la parte oseta contaba con diversos tipos de artillería, entre ellos 12 obuses remolcables D-30, 6 lanzamisiles múltiples Grad y 4 cañones antitanque Rapir de 100mm.[76]

Esta masa bélica se encargó de librar un fuerte enfrentamiento durante esa madrugada en el territorio oseta, mismo que terminó por destruir e incendiar múltiples edificios administrativos, entre ellos el Parlamento, la universidad y el hospital central así como muchas viviendas, además de provocar algunas bajas civiles. Durante las primeras horas del siguiente día -8 de agosto-, dicha situación

[75] *Vid* RIA Novosti, *Conflicto bélico en Osetia del Sur. Infografía*, [en línea], RIA Novosti, Dirección URL: http://sp.ria.ru/infografia/20080910/116667323.html, [consulta: 17 de julio de 2013].
[76] *Idem.*

se complicó pues inició la ofensiva aérea a cargo de 4 aviones SU-25 que bombardearon la ya de por sí destruida ciudad, además de que varios helicópteros Mi-24 hacían de soporte a las tropas terrestres georgianas, provocando así más muertes en su contraparte.

A pesar de esta situación, la ciudad no pudo ser capturada pues la resistencia oseta, aun cuando era inferior numéricamente ante los militares georgianos, pudo contener el ataque. Sin embargo, lo que parecía ser un conflicto de pequeña escala al interior de un país no tardó en convertirse en una guerra delicada entre dos naciones debido a un incidente que sucedió en ese día a las 00:15 horas: "Según el Comando de las Fuerzas de Pacificación Rusas, se informó que de la parte georgiana se disparaba para exterminar a las fuerzas pacificadoras en Tsjinval, y que Tbilisi trataba de confundir a la opinión mundial acerca de estos ataques."[77]

Tal como lo menciona la cita, las tropas al mando de Mijeíl Saakashvili parecían tener la orden de agredir deliberadamente a las tropas pacificadoras de Rusia que se habían apostado allí desde el fin de la guerra civil georgiana. Este escenario, según relatan diarios rusos, trató de ser ocultado e incluso se buscó culpar a las tropas de Moscú argumentando que éstas estaban participando activamente en el desarrollo del conflicto armado:

> "Fueron heridos y asesinados los pacificadores rusos, pero del Ministerio de Asuntos Exteriores de Georgia se declaró que no fueron atacadas las fuerzas rusas de pacificación. El comando georgiano anunció que no habría pláticas de paz, Georgia inició una operación bélica contra el gobierno y contra la República de Osetia del Sur."[78]

Desde la contraparte rusa no podían tolerar este escenario pues estaban sobre la mesa diversas razones externas e internas involucradas en el asunto, entre ellas destacaban las siguientes:

[77] Ana Teresa Gutiérrez del Cid, *Op. Cit.*, p. 104
[78] *Idem.*

- Rusia no podía permitir la masacre de sus tropas de paz asentadas en el territorio oseto. Adicionalmente, es por demás conocido que en esta zona habitan ciudadanos cuyos orígenes étnicos se remontan a dicha Federación.
- Por otro lado, el gobierno moscovita no podría permitir poner en riesgo sus vías de distribución energética hacia Europa, en específico sus corredores de óleo así como sus gasoductos, entre los que destaca el megaproyecto Dzaurikau- Tsjinval de 169 km de extensión.
- Adicionalmente, la cúpula de poder en Moscú debía evitar a toda costa que una de sus zonas de influencia cayera en manos de Georgia, pues este escenario debilitaría el muro de contención que Rusia había estado construyendo desde el derrumbe de la URSS.
- Finalmente, y encaminado a la razón anterior, la Federación no podía permitir que la influencia occidental (representada en Misha, el apoyo estadounidense y de la OTAN) se apostara en una zona que pondría bajo riesgo a la privilegiada geopolítica moscovita.

Con todo lo anterior, el Estado ruso no dudó en evitar que el conflicto se agravara y, por ello, inició una serie de maniobras políticas para contrarrestar el movimiento bélico: en primer lugar, el primer ministro, Vladimir Putin, voló desde el Kremlin hasta Osetia del Norte para organizar una red de ayuda que buscará proteger a todos los refugiados que salían de Osetia del Sur. Desde allí, Putin emitió una declaración que preparaba el terreno para que su país entrará de lleno al conflicto: para él, la masacre cometida en Tsjinval no era otra cosa más que genocidio.[79]

Tras estas palabras, el Kremlin decidió intervenir militarmente en la zona con la previa autorización del Consejo de Seguridad Nacional, pues era casi un hecho que, si el tiempo seguía su marcha, se correría el riesgo de que Osetia del Sur y Abjasia cayeran bajo el manto de influencia occidental cuya punta de lanza se

[79] *Vid* Ana Teresa Gutiérrez del Cid, *Op. Cit.*, p. 105

concentraba en Misha. Así pues, bajo este escenario de tensión, el presidente del Estado ruso, Dmitri Medvédev, dirigió un mensaje a toda su nación:

> "Como ustedes saben, Rusia ha mantenido y continua manteniendo una presencia en el territorio de Georgia bajo una base absolutamente jurídica, estableciendo sus fuerzas de paz en concordancia con los acuerdos concluidos. Siempre hemos considerado mantener la paz como una de nuestras tareas primordiales. Rusia ha sido históricamente un garante para la seguridad de los pueblos del Cáucaso, y esto sigue siendo vigente al día de hoy.
>
> "Durante la noche de ayer, tropas georgianas cometieron actos de agresión en contra de las fuerzas de paz rusas y de la población civil en Osetia del Sur. Lo que pasó es una violación grave a la ley internacional y a los mandatos que la comunidad internacional dio a Rusia como un socio dentro del proceso de paz.
>
> "Los actos de Georgia han causado pérdida de vidas, incluyendo entre ellas las de las fuerzas de paz rusas. La situación alcanzó el punto donde las fuerzas de paz georgianas abrieron fuego contra las tropas de paz rusas, las cuales supuestamente trabajan de manera conjunta para cumplir con la paz en esta región. Civiles, mujeres, niños y personas de la tercera edad, están muriendo hoy en Osetia del Sur, y la mayoría de ellos son ciudadanos de la Federación Rusa.
>
> "En concordancia con la Constitución y las leyes federales, y como Presidente de la Federación Rusa es mi deber el proteger las vidas y dignidad de los ciudadanos rusos donde quiera que éstos estén.
>
> "Son estas circunstancias las que dictan los pasos que tomaremos ahora. Nosotros no permitiremos que la muerte de nuestros queridos ciudadanos quede impune. Los perpetradores recibirán el castigo que ellos merecen."[80]

Como acto seguido al discurso, inició la movilización. Cerca de 10,000 efectivos pertenecientes a las fuerzas armadas rusas comenzaron el despliegue hacia Tsjinval, acompañados por aproximadamente 150 unidades acorazadas de alta potencia: los T90.

[80] Dmitri Medvédev , *Statement on the situation in South Ossetia*, [en línea], President of Russia, 8 de agosto de 2008, Dirección URL: http://archive.kremlin.ru/eng/speeches/2008/08/08/1553_type82912type82913_205032.shtml, [consulta: 23 de julio de 2013]. Traducción propia.

Tras la llegada del primer destacamento ruso a tierra osetas, inició el fuerte enfrentamiento: los tanques moscovitas así como la artillería proveniente de dicho país se asentaron en el norte del territorio en disputa, específicamente cerca del túnel Roki, desde el cual había arribado todo el apoyo del Estado ruso. Desde ahí, la masa bélica disparaba hacia las columnas de tanques y efectivos georgianos, los cuales también eran bombardeados por la vía aérea con aviones SU-24, SU-25, SU-27 así como TU-22M. Estas acciones, que también fueron apoyadas por la resistencia oseta, hicieron que la mayoría de los milicianos georgianos comenzaran su retirada de puntos estratégicos que habían sido capturados, entre ellos el puente Didi Gupta. Tras esta huida, comenzaron a llegar más refuerzos así como provisiones desde el lado ruso y, de esta forma, la ciudad empezó a ser recuperada de forma escalonada. Cabe aclarar que, aunque oficialmente se declaró la ciudad libre de invasores por la tarde del 9 de agosto[81], este escenario de conflicto se extendió por casi tres días más, periodo durante el cual hubo intentos georgianos de avanzar nuevamente hacia la capital oseta; no obstante, todos éstos fracasaron y desembocaron en repliegue.

Sin embargo, los comandos rusos de élite no tardaron en darse cuenta más tarde que los invasores georgianos habían abandonado sus posiciones debido a una estrategia muy usual dentro de cualquier campo de batalla: desde el frente de inteligencia moscovita llegaba información de que las tropas de Misha habían iniciado un reagrupamiento en la ciudad de Gori, desde la cual revalorarían posiciones y estrategias para volver a atacar a una escala mayor.

Este nuevo escenario bélico hizo que el conflicto se esparciera más allá de lo delimitado en la capital de Osetia del Sur. Así pues, iniciaron los ataques a la ciudad de Gori tan pronto se dio aviso sobre el reagrupamiento del enemigo: diversos aviones de combate rusos junto con helicópteros con capacidad ofensiva

[81] *Vid* s/a, *Georgia declara estado de guerra y Rusia dice haber liberado Osetia del Sur*, [en línea], La Nación, 9 de agosto de 2008, Dirección URL: http://www.lanacion.com.ar/1038121-georgia-declara-el-estado-de-guerra-y-rusia-dice-haber-liberado-osetia-del-sur, [consulta: 23 de julio de 2013].

iniciaron un ataque aire tierra que terminó dañando seriamente a la infraestructura del asentamiento, destruyendo parte de la universidad y la plaza central así como el hospital militar y un depósito de municiones. Adicionalmente, la cobertura mediática internacional registró el movimiento de misiles balísticos rusos SS-21 al campo de batalla[82] y de la misma forma reportaron alrededor de 15 ataques con este tipo cohetes; de hecho, hubo uno que impactó directamente en un bunker de mando cerca de la ciudad de Borjomi, al sur de Gori[83]. Todas estas acciones causaron bajas en ambos bandos pues la milicia georgiana trató de resistir el avance de la tormenta rusa con poderosa artillería tierra aire.

A pesar de la resistencia, las tropas bajo la orden de Misha tuvieron que abandonar sus posiciones en Gori debido a una orden directa del gobierno georgiano: según la cúpula de poder de aquel país, lo más factible era que las tropas se retiraran de aquella importante ciudad para reagruparse en Tbilisi, capital del país, para defenderla del avance enemigo. Tras esta salida, las tropas rusas entraron a Gori el 12 de agosto y tomaron el control de dicho asentamiento. De ahí, iniciaron su camino hacia la capital georgiana, sin embargo, decidieron montar un puesto a 55 kilómetros de la ciudad, mismo que fue el más cercano a la capital durante toda la guerra.

Tras ver la situación en la que se encontraban –con Gori ocupada, un frente de batalla en Abjasia y con los bombardeos en su capital-, los mandos georgianos no tuvieron otra opción más que llegar a un acuerdo de paz, el cual había sido impulsado desde el comienzo del conflicto por la Unión Europea y Estados Unidos. Así pues, para el 14 de agosto del año 2008 estaba firmado el "Plan de paz de 6 puntos", mismo que planteaba lo siguiente:

---

[82] *Vid* AFP, *Russia moves SS-21 missiles into Georgia: US defense oficial*, [en línea], AFP, 18 de agosto de 2008, Dirección URL: http://www.google.com/hostednews/afp/article/ALeqM5iiba8YaYXz88Y9n9OQBVKp9ofSig?hl=en, [consulta: 25 de julio de 2013].

[83] *Vid* s/a, *SS-21 "Scarab" (9K79 Tochka) SRBM*, [en línea], Harpoon Data Bases, Dirección URL: http://www.harpoondatabases.com/encyclopedia/entry2181.aspx, [consulta: 25 de julio de 2013].

1. Quedaba prohibido el recurso al uso de la violencia bajo cualquier escenario.
2. Se declaraba definitivamente el cese a las hostilidades que habían comenzado una semana antes al día de la firma del acuerdo.
3. Se garantizaba el acceso libre a la ayuda humanitaria que había sido negada en diversas ocasiones durante el conflicto por los dos países en cuestión.
4. Las Fuerzas Armadas de Georgia deben retirarse invariablemente a sus posiciones permanentes, esto es, su territorio soberano.
5. Las Fuerzas Armadas de la Federación Rusa deben retirarse invariablemente a la zona donde estaban apostadas antes del inicio del conflicto. En este mismo sentido, y de acuerdo a lo establecido en el mecanismo internacional que se había firmado tras la Guerra Civil georgiana, las tropas de paz rusas tomaran medidas adicionales de seguridad para garantizar la paz en Osetia.
6. Se llevará a cabo un debate sobre el estatus internacional de Osetia del Sur y Abjasia. De la misma forma, se analizarán los caminos más adecuados para garantizar la seguridad de ambos territorios.[84]

Así pues, con la firma de este acuerdo se cerraba un conflicto que estuvo a punto de desestabilizar el débil equilibrio de aquella zona geográfica así como provocar un conflicto internacional de dimensiones mayores que reviviría la actitud hostil experimentada entre Oriente y Occidente durante la época de la Guerra Fría. Por lo demás, quedan claras las desafortunadas consecuencias que la batalla tuvo en ambos contendientes: en Osetia del Sur hubo 162 muertos y 255 heridos además de más de 33,000 refugiados, sin contar que se destruyeron completamente 655 viviendas junto con 2,139 edificios que fueron afectados en alguna parte de su estructura; por el lado ruso se contaron 67 muertos y 283 heridos que se complementan con 3 personas desaparecidas; y, finalmente, en el lado georgiano murieron 412 personas y 1,747 resultaron heridas debido al confrontamiento, además de 24 personas desaparecidas.[85]

[84] RIA Novosti, *Medvédev firmó los seis principios de arreglo del conflicto en Georgia,* [en línea], RIA Novosti, 16 de agosto de 2008, Dirección URL: http://sp.rian.ru/international/20080816/116082935.html, [consulta: 27 de julio de 2013].
[85] *Vid* RIA Novosti, *Guerra de los cinco días entre Rusia y Georgia en agosto de 2008: crónica y balance de víctimas del conflicto. Infografía,* [en línea], RIA Novosti, Dirección URL: http://sp.ria.ru/infografia/20130808/157745603.html, [consulta: 30 de julio de 2013].

Como era de esperarse, todos estos enfrentamientos dentro del territorio oseto acapararon la atención de los medios de comunicación internacionales, mismos que hicieron una cobertura completa que derivó en una mar de información acerca de esta guerra; sin embargo, paralelo a este conflicto hubo otra batalla que pasó casi desapercibida y que pudo haber causado la misma cantidad de daños al país bajo el poder de Saakashvili: esta confrontación fue bautizada por los expertos como la ciberguerra ruso-georgiana.

3.4 La ciberguerra ruso-georgiana.

Desde el punto de vista de Richard Stiennon, la antesala de la "primera ciberguerra" de la historia comenzó a formarse desde un mes antes de los enfrentamientos bélicos entre los dos países de la zona euroasiática, Georgia y Rusia: según el destacado consultor de origen estadounidense, para el 20 de julio del año 2008 una organización independiente conocida como *ShadowServer Foundation*, cuya misión "es monitorear las redes informáticas con el fin de proveer información relevante y en tiempo a la comunidad de seguridad en línea"[86], detectó una serie de patrones en el ciberespacio que parecían ser anómalos y cuyo objetivo podría ser maligno; dichos códigos encajaron perfectamente en la categoría de una de las armas más utilizadas en los conflictos cibernéticos, los *botnets*[87].

Desde la organización bautizaron a este conjunto de códigos binarios como *Machbot* y, después de un arduo análisis informático del mismo, los expertos en seguridad de *ShadowServer* confirmaron lo que ya sospechaban: la cadena de acciones ejecutadas remotamente por el *botnet* tenía como asignación primordial iniciar un ataque *DDoS* contra uno de los principales servidores que almacenaban información así como el sistema informático de algunos sitios gubernamentales de

[86] ShadowServer Foundation, Mission, [en línea], ShadowServer Foundation, Dirección URL: https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission, [consulta: 5 de agosto de 2013]. Traducción propia.

[87] Un *botnet* es un ordenador infectado por virus informático, mismo que es controlado por un operador humano de forma remota junto a miles de computadoras en la misma condición para dirigir un ataque DDoS de manera simultánea y masiva en contra de un objetivo web específico. *Vid* página 29.

Georgia. Para ser más específica, la firma detalló que las órdenes exactas que seguía esta ciberarma eran las siguientes:

> "2008-07-20 15:15:14 62.168.168.9 president.gov.ge flood icmp www.president.gov.ge
> "2008-07-20 15:15:12 62.168.168.9 president.gov.ge flood tcp www.president.gov.ge
> "2008-07-20 15:15:08 62.168.168.9 president.gov.ge flood http www.president.gov.ge
> "2008-07-20 14:14:23 62.168.168.9 president.gov.ge flood icmp www.president.gov.ge
> "2008-07-20 14:14:20 62.168.168.9 president.gov.ge flood tcp www.president.gov.ge
> "2008-07-20 14:14:17 62.168.168.9 president.gov.ge flood http www.president.gov.ge
> "2008-07-20 13:13:33 62.168.168.9 president.gov.ge flood icmp www.president.gov.ge
> "2008-07-20 13:13:32 62.168.168.9 president.gov.ge flood tcp www.president.gov.ge"[88]

El resultado de esta operación derivó, como el lector puede deducir, en el inundamiento, saturación y caída del sitio web de la presidencia de Georgia haciendo que esta página electrónica fuera inaccesible para el público general por más de 24 horas; sin embargo, aun cuando este hecho pareció ser poco trascendente tuvo consecuencias más grandes que requirieron la atención inmediata del gobierno Saakashvili: con los ataques cuya duración fluctuó entre las 2 y 6 horas, las comunicaciones y sistemas internos de la presidencia de aquel país quedaron totalmente fuera de línea, causando desesperación y tensión entre los operarios del sitio virtual. Además de esto, Stiennon señala que este ataque planeado causó otros efectos secundarios que también fueron sobresalientes, de los cuales el que más destacó fue el de la caída de la página electrónica de la Agencia Estatal de Asistencia y Empleo (www.saesa.gov.ge), generando la molestia en miles de georgianos desempleados que se formaban a las afueras de esta oficina cuyo sistema estaba totalmente desquiciado[89].

Ahora bien, debido a la naturaleza de la agresión comenzaron a formularse diversas teorías sobre el origen del ataque así como su significación, empero, fue *ShadowServer Foundation* la que no demoró en dar cuenta atinadamente sobre las verdaderas intenciones del acto pues según sus análisis, la raíz de la corriente de bombardeos informáticos utilizados en ese día de julio se localizaba en Estados

[88] s/a, *Update: Georgian government websites under DDoS & Cyber Attack*, [en línea], The Jawa Report, Dirección URL: http://minx.cc:81/?post=193591, [consulta: 7 de agosto de 2013].
[89] *Vid* Richard Stiennon, *Surviving Cyber War*, Estados Unidos, Government Institutes, 2010, p. 97.

Unidos, no obstante, aquél *botnet* utilizado en occidente no era otra cosa más que una máquina que obedecía órdenes remotas desde un ordenador localizado en la Federación Rusa:

> "No hay una prueba conclusiva sobre el origen de los ataques. Sin embargo, muchas agencias de inteligencia han aprendido de la experiencia obtenida en años previos y están mejor equipadas para monitorear los patrones de los ataques [cibernéticos], La distribución atomizada de los ataques coordinados sugieren que diversos botnets debieron haber estado involucrados. Una línea de análisis identificó el uso de un controlador de MachBot para un ataque botnet basado en código http, una firma muy común entre hackers rusos."[90]

Con esta situación al descubierto no fue difícil discernir el significado del ataque pues, según lo demostraba la situación, todo el hecho recaía sobre ciudadanos rusos que se encontraban disgustados con las políticas antirusas y pro occidentales que el presidente de Georgia, Mijeíl Saakashvili, había puesto en marcha contra su país desde el inicio de su mandato. Empero, aun cuando la cúpula de poder georgiana dio cuenta de la situación días después, ésta decidió no llevar a cabo ninguna acción –ni diplomática ni virtual- debido a que, desde su punto de vista, el ciberataque no había tenido mayor trascendencia más allá de los problemas técnicos sufridos en sus redes por algunas horas así como la molestia de un pequeño sector de su población.

En este mismo sentido, es importante aclarar que aun cuando el evento de julio de 2008 pareció poco trascendente, éste no fue sino un prólogo al estilo ruso para iniciar una campaña bélica virtual de gran tamaño que terminó por hacer que el gobierno georgiano comenzará a reforzar su atención y medidas hacia este nuevo campo de batalla que recién se está consolidando en lo que va de este siglo.

---

[90] Chris W. Johnson, *Anti-social networking: crowdsourcing and the cyberdefense of national critical infrastructures,* [en línea], University of Glasgow, Dirección URL: http://www.dcs.gla.ac.uk/~johnson/papers/Gudela/Cyberdefence_And_Anti_Social_Networking.pdf, [consulta: 8 de agosto de 2013]. Traducción propia.

Así pues, tras el estallido del ya mencionado conflicto militar entre Rusia y Georgia del 7 de agosto de 2008 comenzó a forjarse -de manera puntual- la primera ciberguerra a gran escala en la historia. Dicha agresión virtual sirvió como otro de los frentes de ataque del gobierno ruso para mermar aún más a su enemigo y, a pesar de que la acción involucró solamente el uso de computadoras, este combate virtual de avanzada generó enormes estragos en el pequeño país del Cáucaso.

La primera agresión virtual formal por parte de los rusos se originó en la madrugada del 7 de agosto del año 2008, 15 días después del primer desfogue cibernético. Se hace hincapié en la formalidad de dicho ataque puesto que coincidió con el movimiento de las tropas militares a la orden del presidente Dmitri Medvédev y, al mismo tiempo, cumplió cabalmente con todos los criterios enlistados en el Informe sobre Criminología Virtual 2009 de la compañía de seguridad informática McAfee:

- En primer lugar, fue ejecutado por un país;
- De igual forma, tuvo un objetivo político explicito (aumentar la ventaja rusa en el conflicto armado);
- Asimismo, generó un impacto crítico y de larga duración;
- Y, finalmente, requirió de técnicas computacionales de avanzada y personalizadas.[91]

Esta sacudida bélica informática consistió en una serie de ataques *DDoS* cuya meta estratégica fue colocar una veda en las comunicaciones de los mandos georgianos: “Un velo fue bajado sobre el teatro de operaciones [georgiano] durante la invasión militar [rusa].”[92] Esta situación concedió un gran margen de ventaja a las fuerzas castrenses moscovitas pues con la disrupción de los sistemas de comunicación vitales en Georgia –entre ellos, los sitios de Internet- fueron capaces

[91] McAfee, *Op. Cit.*
[92] Richard Stiennon, *Op. Cit.*, p. 97. Traducción propia.

de organizar mejores tácticas de guerra mientras cundía la desinformación y, por tanto, la desorganización entre las tropas y mandos del enemigo.

Además del cegamiento electrónico del rival, la agresión informática también tuvo a bien en saturar y en consecuencia desestabilizar a diversos servidores de importancia localizados en territorio georgiano. Dicha acción se tradujo en la censura de los sitios de Internet de noticias que informaban sobre los enfrentamientos librados durante el conflicto así como las páginas web que el gobierno de Misha usaba para comunicar la situación de su país a sus ciudadanos: el resultado total fue, pues, el aislamiento de las comunicaciones civiles con el resto del mundo. Ahora bien, en este mismo sentido destaca una acción llevada a cabo por los agresores informáticos durante esa mañana del 7 de agosto pues, si una persona ingresaba al sitio de la presidencia de Georgia para tratar de obtener alguna información sobre esta guerra se encontraba con la siguiente imagen (figura 2):

И кончит он также...

hacked by South Ossetia Hack Crew

Figura 2. Fotograma aparecido en el sitio web presidencial de Georgia. Fuente: Asher Moses, *Georgian websites forced offline in cyber war*, [en línea], The Sidney Morning Herald, 12 de agosto de 2008, Dirección URL: http://www.smh.com.au/news/technology/georgian-websites-forced-offline-in-cyber-war/2008/08/12/1218306848654.html, [consulta: 10 de agosto de 2013].

En la misma figura, se puede apreciar como los *crackers* integraron un collage que comparaba expresamente al actual presidente de Georgia, Mijeíl Saakashvili, con el titular del poder alemán de los años 1934-1945, el Führer Adolf Hitler. En este sentido, no queda otra cosa más que recalcar que lo que esta imagen representaba no era otro hecho más que el sentimiento que tenían los ciudadanos y el gobierno de Rusia hacia Misha.

En otro orden de ideas, pero bajo los mismos objetivos delineados en el plan de batalla informático ruso, iniciaron los bombardeos con código binario contra los portales en línea de las instituciones bancarias y financieras establecidas dentro del territorio georgiano, fueran éstas de índole pública o privada. Todo esto causó el pánico entre los usuarios de estos establecimientos pues por poco más de un día las operaciones económicas del país que tenían un componente electrónico para su funcionamiento fueron prácticamente bloqueadas. Adicionalmente, todos los portales de comercio electrónico cuyo dominio fuese .ge –Georgia- sufrieron también dificultades técnicas en su operación debido a los constantes flujos de información dirigida hacia los servidores donde se almacenaban dichas páginas.

De igual forma, páginas web de embajadas (entre ellas la de Estados Unidos y Reino Unido), del Parlamento, de la Corte Suprema, del Ministerio de Relaciones Exteriores, de la Comisión Central Electoral, de estaciones de radio y televisión e incluso blogs fueron integrados en el bombardeo virtual de aquella mañana del 7 de agosto. De entre todo esto, destaca el ataque concentrado contra la página oficial de Ekaterine Tkeshelashvili, Ministra de Relaciones Exteriores, quien utilizaba este medio como una vía diplomática de comunicación y como centro de información para los nacionales; de hecho, de tal magnitud fue el vapuleo cibernético que la titular de los asuntos exteriores decidió migrar su canal comunicativo hacia una página social de un empresa privada, Blogger: desde ahí, anunció al mundo que

”una campaña de ciberguerra conducida por Rusia está desestabilizando seriamente muchos sitios web georgianos, incluyendo el del Ministerio de Asuntos Internacionales.”[93]

De forma paralela a todo esto, los *crackers* atacantes iniciaron una táctica más personalizada para generar problemas de comunicación entre los miembros de la alta cúpula de poder georgiana: mediante un sitio web, los piratas informáticos filtraron una cantidad importante de correos electrónicos institucionales y personales de los funcionarios públicos más relevantes para que fueran victimas de SPAM, hecho que derivaría en la falla generalizada de su servicio de buzón.[94]

Bajo este panorama caótico, el pequeño país euroasiático no encontró una forma adecuada para defenderse, sin embargo, desde el resto del mundo comenzaban a brotar diversas investigaciones que indagaban sobre el origen del hecho así como el patrón que comenzaba a adoptar el conflicto informático. Desde luego, fue *ShadowServer Foundation* la primera en percatarse de que las oleadas de bombardeos binarios venían desde distintos servidores instalados en todo el mundo, entre ellos, destacaban los de Estados Unidos y Turquía. Este escenario dio pie a que los expertos en seguridad de la organización digital empezarán a tener sospechas de las similitudes existentes entre estas agresiones y los atentados que había sufrido Georgia a finales de julio de ese mismo año; por lo tanto, comenzaban a perfilar a un posible culpable –mismo que el mundo ya señalaba-: Rusia.

Más tarde, la sospecha terminó por convertirse en un hecho oficial y totalmente consolidado. En una de sus investigaciones, *ShadowServer* logró mapear los patrones de diseminación virtual de los ataques y, gracias a ello, la

---

[93] Jon Swaine, *Georgia: Russia “conducting cyber war”*, [en línea], The Telegraph, 11 de agosto de 2008, Dirección URL: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html, [consulta: 12 de agosto de 2013]. Traducción propia.

[94] *Vid* Dancho Danchev, *Coordinated Russia vs Georgia cyber attack in progress*, [en línea], ZDNet, 11 de agosto de 2008, Dirección URL: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670, [consulta: 17 de agosto de 2013].

organización tuvo a bien en encontrar el punto de origen de la agresión, un sitio en línea llamado StopGeorgia.com. Desde esta página web se posteaban instrucciones precisas para instalar herramientas *DoS* complejas que ejecutarían las órdenes de ataque contra un listado de sitios web que el mismo sitio enumeraba:

www.parliament.ge	www.assitancegeorgia.org.ge
www.cec.gov.ge	www.mdf.org.ge
www.corruption.ge	www.constcourt.gov.ge
www.insurance.caucasus.net	www.mc.gov.ge
www.nsc.gov.ge	www.supremecourt.ge
www.iberiapac.ge	www.court.gov.ge
www.civil.ge	Georgia.usembassy.gov tbilisivisa@state.gov
Ukingeorgia.fco.gov.uk/en	www.all.ge
www.geres.ge	www.rustavi2.com.ge
www.opentext.org.ge	www.svobodnaya-gruzia.com
www.sanet.ge	www.messenger.com.ge
georgianmessenger.blogspot.com	www.primenewsonline.com
www.presidpress.gov.ge	www.sakinform.ge
www.sakarvelo.ru	www.internews.ge
www.internews.org.ge	www.interpressnew.ge
www.internet.ge	www.stream.ge
newsgeorgia.ge	presa.ge
www.medianews.ge	

Junto con la lista[95] se encontraba un pequeño manifiesto en la página web que expresaba el sentir del administrador o administradores del sitio:

> "Nosotros –los representantes del hackeo underground ruso no toleraremos las provocaciones de los georgianos bajo todas sus manifestaciones. Nosotros buscamos vivir en un mundo libre así como existir en un espacio libre de agresiones y Setevom [sic]. Nosotros no necesitamos ser guiados por las autoridades u otras personas, pero sí operamos en concordancia con sus pensamientos basados en el patriotismo, la conciencia y los ideales. Ustedes pueden llamarnos criminales y ciberterroristas, razvyazyvaya [sic] con la guerra y el asesinato de personas. Pero

[95] Extraída de Richard Stiennon, *Op. Cit.*, p. 98

> nosotros pelearemos y no aceptaremos agresiones contra Rusia en el espacio cibernético. Nosotros demandamos el cese de los ataques en la información y los recursos Runeta [sic] gubernamentales, y de la misma forma apelamos a que todos los medios y reporteros cubran los eventos de manera objetiva. Hasta que la situación cambie, nosotros atacaremos al gobierno georgiano y a sus recursos de información. Nosotros no hemos lanzado una guerra de la información, no nos hacemos responsables de las consecuencias. Hacemos un llamado a participar a todos aquellos que se preocupan por las mentiras de los sitios políticos georgianos, a todo aquel que es capaz de evitar la dispersión de información obscura. Existe un proyecto espejo normal –www,stopgeorgia.info. Cualquier otro recurso no tiene nada que ver con el movimiento StopGeorgia.ru [96]

Esta pequeña leyenda del sitio electrónico junto con los patrones recabados a través del monitoreo informático constante terminaron por evidenciar a los creadores de la agresiva campaña cibernética en contra de Georgia: se trataba nada más y nada menos que de la Red de Negocios Rusa (RNR). Según el propio Stiennon, la Red de Negocios Rusa

> "[…] es una organización turbulenta que ha sido acusada de crear el virus de espionaje conocido como CoolWeb Search, de emprender operaciones masivas de SPAM, de elaborar ataques en línea basados en vulnerabilidades del Iframe en Internet Explorer, de generar oleadas de ataques de phishing así como de poner en marcha campañas relacionadas con el crimen organizado ruso. Se presume que sus cuarteles generales se encuentran en San Petersburgo, Rusia, y se tiene conocimiento de que algunos de sus miembros son agentes operativos de la KGB. Muchas otras innovaciones relacionadas con la creación de malware para convertir computadoras en botnets son también atribuidas a la RNR."[97]

Cabe destacar que, como Stiennon menciona, la RNR tiene estrechos vínculos con el Comité para la Seguridad del Estado Ruso (KGB); de hecho, se ha demostrado en diversas ocasiones que el gobierno moscovita financia a este tipo de grupos para formar escuadrones bélicos de informática avanzada sin levantar

[96] Dancho Danchev, *Op. Cit.* Traducción propia.
[97] Richard Stiennon, *Op. Cit.,* p. 99. Traducción propia.

sospechas en la sociedad internacional[98]: así, cuando surgiera un escenario de batalla como el descrito en este trabajo, sería capaz de desviar su responsabilidad argumentando que las acciones emprendidas no fueron llevadas a cabo por militares rusos bajo órdenes del gobierno sino por ciudadanos con derecho a manifestarse en cualquiera de sus formas –entre ellas, la electrónica.

Así pues, bajo todas estas condiciones destaca el esquema bajo el que se ejecutó el ataque electrónico en contra de los sitios virtuales georgianos:

- En primer lugar, fue un ataque políticamente dirigido y militarmente planeado hacia un Estado; sin embargo, su puesta en marcha corrió a cargo de civiles que no tenían ninguna formación castrense aunque desde luego estaban patrocinados bajo un gobierno. En este sentido, destaca la ampliación del rango de participantes en los conflictos modernos –como ya se había hecho mención en el primer capítulo- así como el engrosamiento de las amenazas para la seguridad de un país.
- En segundo lugar, es de recalcar el escenario de anonimato proporcionado por la Tecnologías de la Información y Comunicaciones (TIC) pues al no existir un protocolo único de domicilio digital se permite que los agresores virtuales ejecuten sus acciones desde cualquier parte del mundo sin ser detectados y mucho peor, sin sufrir consecuencia alguna.
- En tercer lugar, llama la atención la facilidad con la que el conocimiento avanzado –en este caso informático- y su aplicación puede esparcirse aun cuando el objetivo de su diseminación es dañar algo. En el caso georgiano, las herramientas *DDoS* altamente complejas fueron puestas a disposición de las personas que deseaban tomar parte en el conflicto bélico, hecho que sienta un precedente para que una situación similar puede ocurrir de nuevo en el futuro.

[98] *Vid* David J. Smith, *Russian Cyber Operations*, [en línea], Potomac Institute Cyber Center, Julio de 2012, Dirección URL: http://www.potomacinstitute.org/attachments/article/1273/Russian%20Cyber%20Operations.pdf, [consulta: 20 de agosto de 2013].

- Finalmente, es de destacar la fuerte impregnación del fenómeno de la guerra en asuntos tan cotidianos como el uso de computadoras y celulares, por mencionar algunos. Dicha situación muestra como los escenarios bélicos están determinados por las circunstancias técnicas, sociales y culturales del mundo en un momento dado, situación que le confiere el carácter de cambiante a la conflictividad.

Con todo, las respuestas desde el bastión georgiano hacia este escenario de guerra virtual quedaron muy por debajo de las expectativas pues, a grandes rasgos, no hubo una estrategia planeada de contraataque sino más bien se limitaron a poner en marcha un plan de defensa bastante tibio que incluso llegó a recaer en manos de operadores civiles. Específicamente, la táctica defensiva del gobierno de Georgia giró en torno a cuatro hechos clave: en primer lugar, la puesta en marcha del sitio web de investigación en tiempo real sobre las cibercampaña, www.georgiaupdate.gov.ge; en segundo puesto, el llamado de auxilio hacia el *Computer Emergency Response Team* (CERT) estonio; en tercera posición, la respuesta técnica a los inundamientos binarios a cargo de la empresa *Tulip Systems* y el gobierno polaco y; finalmente, el contrataque ejecutado por *hackers* del pequeño país euroasiático.

La página electrónica *Georgia Update* fungía como un centro de investigación y análisis virtual centrado en el conflicto informático que vivía el país durante ese momento. En este sentido, el sitio electrónico proporcionaba reportes sobre los orígenes geográficos de los ataques así como las rutas que seguían los paquetes de datos hasta antes de llegar a su objetivo primario, los servidores nacionales. De igual forma, la página web informaba sobre el estatus de funcionamiento de las herramientas electrónicas y las comunicaciones gubernamentales y privadas, convirtiéndose así en una fuente prima y esencial de conocimiento público ante el caos que habían alcanzado los ciberbombardeos rusos. Así pues, con todo esto la web consolidaba dos metas estratégicas más: por un lado, mantenía el vínculo comunicativo entre el gobierno y sus ciudadanos así

como el del país con el resto del mundo y, finalmente, se constituía en una herramienta de inteligencia para confrontar escenarios similares en el futuro.

Por su parte, la asesoría del CERT estonio al gobierno de Georgia se constituyó como uno de los actos pioneros de cooperación internacional en materia de conflictos informáticos. Por aquellas fechas, dentro de los círculos estratégicos estonios comenzaba a correr la voz de un posible llamado de auxilio:

> "Los oficiales estonios dicen que los ataques DDoS dirigidos contra Georgia fueron muy similares a los ataques hechos contra los sitios web estonios en 2007 después de la remoción del monumento del Soldado de Bronce. De manera no oficial, Estonia y Georgia han estado discutiendo la posibilidad de enviar un equipo especial de seguridad informática a Georgia. Un representante del Centro de Desarrollo de Sistemas de Información Estatal dijo que por ahora Georgia no ha hecho formalmente la solicitud. 'Esto será decidido por el gobierno', confirmo el oficial."[99]

Dicho hecho se consumó y por primera vez en la historia, dos especialistas de la institución de seguridad virtual de Estonia, cuya creación también obedeció a un ciberconflicto que el país sufrió en condiciones más o menos similares con Rusia, salieron de su territorio para iniciar jornadas de intercambio de conocimientos con agentes y representantes de las filas castrenses y civiles del gobierno de Misha. Como era de esperarse, las reuniones buscaban dispersar todas las informaciones técnicas que habían recopilado de su experiencia así como las soluciones operativas que habían emplazado para reparar los daños causados por este tipo de batallas. Con todo, parece ser que el acto sentó un precedente vital para instaurar un protocolo similar en futuras situaciones de guerra virtual.[100]

Ahora bien, la operación técnica para contrarrestar el asalto virtual corrió a cargo de dos entes completamente ajenos a la administración georgiana: en primer

[99] Dancho Danchev, *Op. Cit.* Traducción propia.
[100] *Vid* Mike Collier, *Estonia helps Georgia in cyber war*, [en línea], The Baltic Times, 16 de agosto de 2008, Dirección URL: http://www.baltictimes.com/news/articles/21124/#.UzDaXah5NWE [consulta:24 de marzo de 2014].

lugar, a la empresa estadunidense Tulip Systems y, después, al gobierno de Polonia. Durante sus vacaciones en Georgia, el dueño de la empresa de hosting, Nino Doijashvili, ofreció al gobierno de su país natal el traslado de sus páginas electrónicas bajo ataque hacia unos servidores de su propiedad instalados en Estados Unidos. Según relata el diario británico The Telegraph, después de esta migración de datos los ataques continuaron hacia el nuevo servidor que mantenía apenas con vida a la web del presidente Misha, llegando incluso a alcanzar bombardeos binarios de magnitud 5000 a 1 aun cuando las operaciones militares en suelo georgiano habían sido oficialmente suspendidas por el presidente Dmitri Medvédev[101]; de hecho, por aquellas fechas un funcionario de la empresa, Thomas R. Burling, declaraba

> "Sólo trato de correr la voz. Debido al conflicto entre Rusia y la República de Georgia estamos recibiendo golpes [virtuales]. Emitimos, para expatriados, tres estaciones de televisión georgianas y un sitio de anuncios especiales para el presidente de Georgia, Mijeíl Saakashvili (president.gov.ge). Si usted maneja cualquier material basado en información georgiana, tenga cuidado, estamos recibiendo ataques en todo el espectro, no sólo en los sitios georgianos sino en todas nuestras IPs. Afortunadamente contamos con el equipo y los técnicos que pueden manejarlo. Pero si usted hace caso omiso y decide dejar la información relativa al conflicto es posible que desee tomar medidas precautorias para evitar un ataque. Nosotros aceptamos almacenar el sitio de la presidencia porque hackers rusos han derribado la Internet entera en Georgia. Está gente está loca. Nuestros técnicos prácticamente no duermen. Una cosa es atacar los sitios .ge. Otra cosa es tomar nuestra mesa de ARIN y tratar de llevar al suelo a toda nuestra red."[102]

Por su parte, y en una acción en el mismo sentido, el gobierno polaco accedió también a albergar parte de la información del sitio web de Saakashvili en los servidores que alojaban a la página electrónica de su máxima autoridad, el presidente Lech Kaczynski. Por esos días, el mandatario polaco realizaba la siguiente declaración electrónica: "Junto con la agresión militar, la Federación Rusa

[101] *Vid* Jon Swaine, *Op. Cit.*
[102] s/a, *Update: Georgian government websites under DDoS & Cyber Attack*, *Op. Cit.* Traducción propia.

está bloqueando los portales de Internet georgianos […] Como respuesta al presidente de Georgia, el presidente de la República de Polonia ha puesto a su disposición al sitio web del presidente de Polonia para la diseminación de la información."[103] Desde luego, ese pequeño espacio provisto por el Estado polaco inició inmediatamente operaciones bajo la forma de un blog personal de Misha, mediante el cual informaba a la sociedad internacional sobre las diversas situaciones que vivía su país, entre ellas el estatus de los combates en diferentes zonas geográficas.

Finalmente, la operación ofensiva, como ya se mencionó, corrió a cargo de *hackers* georgianos que no tenían ninguna relación con el gobierno pero que sentían la necesidad de defender su patria. Desde su bastión, estos piratas informáticos comenzaron a emplazar técnicas similares a las de su contraparte para inundar sitios de información rusos (entre ellas la agencia RIA Novosti) así como estaciones de emisión de radio y televisión locales:

> "El sitio web de la agencia de noticias RIA Novosti fue desactivado por algunas horas del domingo debido a una serie de ataques por parte de hackers, todo esto mientras el conflicto entre Rusia y Georgia sobre Osetia del Sur continua hacia su tercer día. Los sitios web en ambos países, Georgia y Rusia, han sido golpeados por ciberataques desde que Georgia lanzó una ofensiva aérea y terrestre mayor para recuperar el control de Osetia del Sur el viernes. Rusia respondió enviando tanques y cientos de tropas. 'Los servidores DNS y el sitio en sí mismo han continuado bajo severos ataques', dijo Maxim Kuznetsov, cabeza del departamento tecnológico de RIA Novosti. Los servidores de RIA Novosti ahora trabajan como normalmente'."[104]

Como se puede observar, la táctica ofensiva georgiana no tuvo el impacto deseado pues ésta se desarrolló en un enorme marco de desorganización: para

[103] Tom Espiner, *Georgia accuses Russia of coordinated* cyberattack, [en línea], Cnet, 11 de agosto de 2008, Dirección URL: http://news.cnet.com/8301-1009_3-10014150-83.html, [consulta: 23 de agosto de 2013]. Traducción propia.
[104] Dancho Danchev, *Op. Cit.* Traducción propia.

variar, desde el frente informático ruso atacaron a los foros de reunión enemigos desde los cuales se armaba el plan.[105]

Como fuese, de estos dos últimos puntos destaca la falta de reacción oportuna ante el incidente por parte de las instituciones gubernamentales de Tbilisi pues, como se puede observar, todo el proceso de defensa técnica recayó en entes ajenos a la estructura de poder del país. Bajo esta misma línea, no es difícil pensar que después de todo lo ocurrido el propio Estado del Cáucaso comenzó a generar protocolos y mecanismos que puedan enfrentar correctamente una situación similar a la acontecida en ese año.

Así pues, de esta forma concluyó la operación bélica virtual del año 2008 que le costó recursos económicos, políticos y sociales a Georgia y que le proporcionó una gran ventaja técnica, estratégica y operativa a la Federación Rusa; todo ello resultado de un acertado golpe virtual que mermó infraestructuras esenciales del ciberespacio georgiano. Sin embargo, las cenizas dejadas tras el fin del conflicto cibernético volverían a encenderse meses después, específicamente en la conmemoración anual de este evento.

En el 8 de agosto del año 2009, diversas organizaciones encargadas de monitorear la seguridad en las redes de Internet comenzaron a notar una gran corriente de información que parecía similar a los patrones virtuales que habían sido empleados durante los ataques *DDoS* de la ciberguerra anterior; horas después, la información sería confirmada: en esta ocasión, los bombardeos binarios se dirigieron contra servidores de empresas privadas que alojaban los distintos perfiles de un ciberactivista georgiano que desde hace tiempo hacia crítica contra la cúpula de poder moscovita y sus políticas neocoloniales. En esta ocasión, la ciberagresión a *Cyxymu* –nombre del bloguero- tuvo repercusiones globales importantes: según reporta el periódico The Guardian, las páginas sociales de Facebook, Twitter y LiveJorunal sufrieron estragos en su funcionamiento debido a

[105] *Vid Idem.*

los ataques que únicamente estaban dirigidos a este luchador social[106]; de hecho, fue tal la magnitud de la operación "Silence Cyxymu" que la red social de mensajes de 140 caracteres, Twitter, fue inaccesible a todos los usuarios del planeta por algunas horas[107].

En este sentido, Stiennon señala que este hecho demuestra el grado de complejidad que es inherente a este tipo de agresiones pues, como él mismo remarca, hasta las grandes empresas especializadas en la operación de Internet, aun cuando poseen grandes infraestructuras de redes y conectividad, tienen enormes dificultades para afrontar estas situaciones: luego entonces, ¿qué puede uno esperar de los Estados?

Como quiera que sea, es un hecho que las operaciones virtuales de aquel agosto de 2008 cambiaron por completo el panorama bajo el cual habían sido observados los conflictos bélicos durante los últimos años y, de igual manera, alertaron a los distintos actores de la escena internacional sobre los enormes riesgos que comenzaría a generar el hecho de no tomar en consideración estas nuevas amenazas. Bajo este mismo panorama, Stiennon señala que

> "Los ataques exitosos en las redes de Georgia, bancos, y sitios web gubernamentales clave durante el comienzo de las hostilidades físicas han cambiado el escenario para todas las naciones que confían en las computadoras y redes para conducir el comercio, la comunicación con sus ciudadanos, y la interfaz con su infraestructura crítica. Ahora tienen que asumir que cualquier conflicto armado en el futuro tendrá un vector coincidente con los ciberataques. Esto no significa una carrera armamentista sino una carrera para implementar defensas antes de que sean necesarias."[108]

---

[106] *Vid* Tom Parfitt, *Georgian blogger Cyxymu blames Russia for cyber attack*, [en línea], The Guardian, 7 de agosto de 2009, Dirección URL: http://www.theguardian.com/world/2009/aug/07/georgian-blogger-accuses-russia, [consulta: 25 de agosto de 2013].

[107] *Vid* Graham Cluley, *Was Twitter denial-of-service targeting anti-Russia blogger?,* [en línea], Naked Security, 7 de agosto de 2009, Dirección URL: http://nakedsecurity.sophos.com/2009/08/07/twitter-denialofservice-targeting-antirussian-blogger/, [consulta: 25 de agosto de 2013].

[108] Richard Stiennon, *Op. Cit.,* p. 101 Traducción propia.

Por todo esto, el siguiente capítulo se centrará en revisar cuáles han sido las consecuencias que las ciberguerras recientes han acarreado para los Estados y para el concepto de seguridad que hasta este momento habían empleado.

Capítulo 4. Ciberguerras y la reconfiguración de la noción de seguridad.

> *"En el cibercampo de batalla…*
> *remplaza francotiradores con hackers,*
> *remplaza balas con paquetes de datos*
> *remplaza la guerra química con virus informáticos,*
> *remplaza armas anti aéreas con cortafuegos,*
> *remplaza guardias con sistemas de detección de intrusiones,*
> *remplaza la inteligencia militar con el análisis de datos,*
> *remplaza los campos de batalla físicos con sus ciber equivalentes que tienen el potencial de expandir el conflicto hasta cualquier punto del planeta, y remplaza los tratados internacionales, políticas y organizaciones con NADA"*
> Sam Nitzberg, *The cyber battlefield-Is this the setting for the ultimate World War?*[109]

Tras los ataques cibernéticos del 8 de agosto de 2008 se encendieron las alarmas globales: en foros de distintos niveles, la sociedad internacional comenzaba a debatir abiertamente y con más seriedad sobre la consolidación de este nuevo campo de batalla, el virtual, y las formas de contrarrestarlo o por lo menos controlarlo, situación que ponía de relieve los agujeros críticos que la visión de seguridad tenía en ese entonces[110].

Empero, antes de continuar es preciso destacar que es incorrecto asumir que todo este escenario de alerta se montó sólo por los acontecimientos acaecidos en Georgia pues es por demás conocido que anteriormente se habían suscitado hechos similares en diversas partes del mundo; sin embargo, sí fue éste la punta de lanza que impulsó el debate pues, por primera vez en la historia, un ataque militar

[109] Sam Nitzberg, *The cyber battlefield- Is this the setting for the ultimate World War?*, [en línea], Telos Information Protection Solutios, octubre de 1998, Dirección URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.393&rep=rep1&type=pdf, [consulta: 27 de agosto de 2013]. Traducción propia.

[110] La visión prevaleciente de seguridad comprendía amenazas tradicionales tales como invasiones extranjeras, confrontaciones directas con otro Estado, desintegración del territorio, así como la proliferación de armas nucleares, químicas y biológicas, entre otras. Sólo después del esparcimiento de los conflictos en el ciberespacio se agregó a la agenda el tema de la ciberseguridad, tal y como se desarrolla en este apartado.

tradicional se desplegó junto a un nuevo tipo de conflicto, escenario que ponía en duda a todo parámetro previamente establecido en los fenómenos de conflictividad.

Con esto aclarado, se procede a analizar los cambios más destacados en el ámbito de la seguridad internacional –y en algunos casos a nivel nacional- que se dieron después del año 2008. Ahora bien, desde el punto de vista del autor de este trabajo, estas transformaciones se generaron en 4 áreas diferentes pero íntimamente conectadas, mismas que son:

1. El empoderamiento del individuo, la masificación de las amenazas y el auge del espionaje digital.
2. El fortalecimiento de las instituciones de seguridad informática, la aceleración de la conformación de unidades castrenses encargadas del ciberespacio y el aumento de la cooperación internacional en el ramo.
3. La presencia del vector informático en los conflictos futuros y la acentuación de las batallas asimétricas.
4. La búsqueda de instrumentos internacionales y nacionales que limiten las ciberbatallas y, por tanto, la libertad que ha existido en las Tecnologías de la Información y Comunicaciones, en específico, Internet.

A continuación se profundiza sobre cada uno de estos puntos y, en el mismo sentido, se establece y explica la conexión que existe entre todos y cada uno de ellos.

4.1 El empoderamiento del individuo, la masificación de las amenazas y el auge del espionaje digital.

La tecnología es un constructo social pues, lejos del enfoque instrumental, existe entre ésta y la sociedad una relación recíproca que se prolonga infinitamente: por un lado, la sociedad le confiere sentido, significado y utilidad, en la otra arista, la tecnología es ideada y planificada a partir de las necesidades de aquélla. Ambas

variables –sociedad y tecnología- se desarrollan de forma paralela y se condicionan, son dependientes, coexisten. Evidentemente, la lógica que le confiere cada ser humano a estas herramientas difiere tal como se demuestra a continuación, sin embargo, es preciso anotar que cualquiera que sea la dirección que ésta tome, es innegable que apunta hacia un solo objetivo: el empoderamiento del individuo.

Por ejemplo, es un hecho que las TIC le han conferido un gran impulso a todas las personas que tienen acceso a este tipo de recursos en la Tierra: más allá del acceso a información generada en tiempo real, estos dispositivos alentaron la creación de un ambiente de comunicación inmediata y, en este mismo sentido, dieron pie a la posibilidad de que personas de distintos lugares del mundo pudieran organizarse para luchar –virtualmente- por un objetivo común cualquiera; sin embargo, más importante es aun que dichas campañas pueden tener un alcance global. En este sentido, este escenario, que comenzó a gestarse a finales del siglo XX y que recién comienza a consolidarse en lo que va de éste, marca un hito en la historia: por primera vez en el tiempo, manifestaciones emplazadas en medios virtuales pueden terminar afectando a situaciones de distintas índoles que suceden en el mundo. Luego entonces, mediante estas nuevas herramientas digitales se ha logrado revertir la aprobación de distintas leyes, se han puesto en marcha campañas ambientales exitosas y también se han financiado completamente proyectos de distinta índole por la vía del *crowdsourcing*, por citar sólo unos ejemplos. Todo este entramado constituiría *grosso modo* un escenario de significación positiva.

Sin embargo, también es bien sabido que las TIC han traído como consecuencia de su expansión diversos daños colaterales: nacieron los delitos cibernéticos, el robo de la identidad digital y comenzaron a gestarse los hurtos a cuentas bancarias a través de traspasos electrónicos, por mencionar algunos. En este mismo sentido, este ambiente de apertura de la información dio pie a la diseminación de datos que podrían servir para poner en situaciones de riesgo a los

Estados además de que, por la naturaleza del conjunto de caracteres, esta situación se agravaría debido a que hipotéticamente cualquier persona podría acceder a los mismos y de la misma forma podría crearlos y dispersarlos por todo Internet: cómo *crackear* cuentas de correo, cómo interceptar mensajes instantáneos o incluso el cómo elaborar software maligno se han convertido en tutoriales muy fáciles de encontrar en la web y rara vez nos detenemos a pensar en su posible utilidad y alcance. Cabe aclarar que, evidentemente, este tipo de actos responden a una significación negativa de la tecnología.

Así pues, estos dos escenarios de significación, positivo y negativo, sin duda han empoderado al individuo moderno: sus acciones digitales dirigidas, individuales o colectivas, tienen un efecto que puede modificar –para bien o para mal- el curso de la historia nacional e incluso mundial.

Con este paraje puesto sobre la mesa, la ciberguerra librada entre rusos y georgianos no podía provocar otra cosa más que la exponencial atención a esta situación: la participación de ciudadanos de a pie en un conflicto militar virtual entre dos países junto con el acceso a material informático capaz de realizar daños a estructuras físicas evidenciaron que todos los seres humanos con acceso a herramientas digitales somos, desde el punto de vista clásico de la seguridad del Estado, una potencial amenaza que puede explotar en cualquier momento. Luego entonces, en un mundo donde existirán para 2014 poco más de 2, 000 millones de computadoras funcionales instaladas en distintos países[111] y donde 32,4% de la población mundial tiene acceso a Internet de banda ancha[112], ¿existe la posibilidad de que este escenario de alto riesgo se pueda repetir a una escala mayor en el planeta y de forma más continua dentro de los próximos años? Según los eventos

[111] *Vid* Gartner Inc., *Gartner says more tan 1 billion PCs in use worldwide and headed to 2 billion units by 2014*, [en línea], Gartner Inc., 23 de junio de 2008, Dirección URL: http://www.gartner.com/newsroom/id/703807, [consulta: 6 de noviembre de 2013].
[112] *Vid* Monserrat Lecaros, *Primer informe ONU: 34% de la región se conecta a banda ancha*, [en línea], América Economía, 24 de septiembre de 2012, Dirección URL: http://tecno.americaeconomia.com/noticias/primer-informe-onu-34-de-la-region-se-conecta-banda-ancha, [consulta: 6 de noviembre de 2013].

y políticas que han venido ocurriendo en distintos lugares en los últimos años, parece ser que sí.

En este sentido, no es de extrañar que diversos países comiencen a emplazar programas de espionaje digital que tengan por objetivo conocer los patrones de comportamiento así como las acciones que realizan día a día sus ciudadanos al conectarse a la web, encaminando así a todos los conglomerados sociales de distintos países hacia un escenario propio de la obra 1984 de George Orwell. Después de todo, el entramado estratégico estadunidense *PRISM*, iniciado en 2007, así como el proyecto *Tempora* puesto en marcha durante el 2011 por las autoridades británicas son ejemplos claros del escenario de tensión generados por el empoderamiento virtual individual, mismo que tomó aún más relevancia con los ciberconflictos. Finalmente, y dicho sea de paso, es curioso advertir que esta situación se ha tornado en *otro* pretexto perfecto para que los países hegemónicos –principalmente Estados Unidos- derramen sus técnicas de espionaje avanzado hacia líderes mundiales, como recién lo está dejando ver el escenario internacional actual (mismo que tomó aún más relevancia con el caso de la *National Security Agency)*.

Como sea, es un hecho que todo esta estructura que se ha forjado desde finales del siglo pasado ha dado pie al surgimiento, o en su caso fortalecimiento, de entidades militares encargadas estrictamente del ataque y defensa en la nueva dimensión virtual y, en este sentido, la cooperación internacional entre las instituciones ya establecidas comienza a adoptar un ritmo más continuo. En el siguiente apartado se profundiza sobre el tema.

4.2 El fortalecimiento de las instituciones de seguridad informática, la aceleración de la conformación de unidades castrenses encargadas del ciberespacio y el aumento de la cooperación internacional en el ramo.

Ante el escenario previamente analizado en el punto anterior, los diferentes Estados del globo comenzaron a barajar opciones que pudieran resguardar su integridad soberana y que, del mismo modo, pudiesen fortalecer su plan de seguridad en este ambiente hostil: el resultado de la revisión, según lo muestran los acontecimientos ocurridos en los últimos años, derivó en el fortalecimiento de sus grupos castrenses encargados del campo de batalla virtual o, en su caso, en la construcción de los mismos en aquellos países donde no los hay. En este mismo sentido, la cooperación internacional en torno a la defensa del ciberespacio se ha acentuado debido a este proceso de construcción de fortalezas en un área que anteriormente no era considerada prioritaria en el interés y orden estatal.

Ahora bien, el proceso de fortalecimiento de las instituciones bélicas encargadas del resguardo del espacio cibernético puede seguir distintos caminos que devengan, finalmente, en la óptima reestructuración de las mismas a través de políticas públicas o en aspectos plenamente operativos. Para ejemplificar esta situación, nos enfocaremos brevemente en la estrategia adoptada por Estados Unidos.

En el caso estadunidense, el subsecretario de defensa de dicho país, William J. Lyn, presentó al mundo a mediados del año 2011 una estrategia integral que pondría en marcha su nación para atender a los crecientes ataques virtuales dirigidos hacia este Estado. Dicho documento, intitulado *Department of Defense strategy for operating in cyberspace*, enlista una serie de preceptos para contrarrestar los efectos de este nuevo campo de batalla en este país parte del continente americano; entre ellos, resalta el punto que sugiere que diversas instancias de gobierno colaboren entre sí para generar tácticas operativas capaces de contener a las crecientes amenazas que se dibujan en el espacio virtual: así pues, este plan hizo que el Pentágono, la Agencia de Seguridad Nacional y *U.S. Cybercom* compartieran tareas de reconocimiento y, con base en ello, generaran pautas de inteligencia para explotarlo a su máxima capacidad defensiva y

ofensiva[113]. En este sentido, es de destacar el llamamiento que hace la cúpula de poder estadunidense al sector privado para que trabaje paralelamente con estas instituciones en la estrategia, reconociendo así, por primera vez, que las tareas de seguridad y las amenazas ya no recaen exclusivamente en el sector castrense del Estado.

Para complementar todo este entramado estratégico, el Departamento de Defensa había desplegado desde hace algunos años un programa de inversiones por más de 500 millones de dólares que tendría como objetivo el desarrollo de cibertecnologías de vanguardia[114]. Entre los diversos flujos de efectivo, destaca el que fue destinado para la creación de un campo de entrenamiento virtual para los nuevos reclutas encargados de vigilar el ciberespacio: el nombre de dicho proyecto es *Nacional Cyber Range.* Este simulador, supervisado por la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) y diseñado y construido por Lockheed Martin, es un modelo a escala de Internet capaz de poner en marcha simulacros de ataques de potencia extranjeras por la vía informática así como incursiones piratas desde el propio territorio estadunidense[115]. Así pues, con esta acción el plan operacional de Estados Unidos tomaría aún más relevancia que con la simple publicación del documento de gobierno.

Finalmente, y desde el bastión de las políticas públicas, el presidente de aquella nación, Barack Obama, terminó por declarar que Estados Unidos equiparía cualquier ciberataque que sufriera con un acto de índole bélico[116]. Este hecho, desde el punto de vista de quien escribe, desembocaría en dos escenario

---

[113] *Vid* Department of Defense, *Department of Defense strategy for operating in cyberspace*, [en línea], Department of Defense, Julio de 2011, Dirección URL: http://www.defense.gov/news/d20110714cyber.pdf, [consulta: 8 de noviembre de 2013].

[114] *Vid* BBC, *El nuevo campo de entrenamiento para las ciberguerras*, [en línea], BBC, 18 de junio de 2011, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2011/06/110617_eeuu_ejercito_ciberataque_ciberguerra_internet_jg.shtml, [consulta: 8 de noviembre de 2013].

[115] *Vid idem.*

[116] *Vid* Isabel Piquer, *EEUU equipara los ciberataques con actos bélicos*, [en línea], Públiclo.es, 31 de mayo de 2011, Dirección URL: http://www.publico.es/internacional/379427/eeuu-equipara-los-ciberataques-con-actos-belicos, [consulta: 8 de noviembre de 2011].

fundamentales: en primer lugar, las declaraciones de Obama terminarían por imprimirle –aún más- un sello de seriedad al entorno hostil que comenzó a gestarse en el ciberespacio desde principios de siglo y; finalmente, esta situación concedería al país otra línea argumental para justificar sus invasiones a diferentes países.

El caso estadunidense ilustra de manera clara el panorama de reestructuración y fortalecimiento de las instituciones castrenses encargadas de resguardar al espacio virtual. Sin embargo, y como anteriormente lo mencionamos, el escenario de tensión que el mundo vive desde el estallido de la ciberguerra ruso-georgiana también derivó en la creación urgente de unidades castrenses centradas en el ciberespacio en los países donde éstas no existen. El ejemplo más emblemático de este hecho puede encontrarse en el caso de Reino Unido.

A mediados del año 2013, el gobierno británico informó al mundo a través de su Ministro de Defensa, Philip Hammond, sobre sus intenciones de juntar un cuerpo de reservistas para formar un ejército cibernético que se encargaría de preparar la estrategia defensiva y ofensiva de su país ante el constante aumento de las amenazas virtuales[117]. Durante su rueda de prensa en el Parlamento, Hammond declaró específicamente lo siguiente: "En respuesta a la creciente amenaza cibernética, estamos desarrollando una cibercapacidad de espectro total, incluida la capacidad de atacar, para mejorar la gama de capacidades militares del Reino Unido."[118]

De todo este anuncio, destacó el público al que estaba dirigido la convocatoria, esto es, a ciudadanos británicos con amplia experiencia comprobable en todos los campos que rodean al mundo de los ordenadores –hackers-. De esta forma, la cúpula de poder del Reino Unido reconocía abiertamente la necesidad de

[117] *Vid* Walter Oppenheimer, *Reino Unido convoca un Ejército de 'hackers' para su defensa*, [en línea], El país, 6 de octubre de 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/10/05/actualidad/1380999276_830357.html, [consulta: 9 de noviembre de 2013].
[118] *Idem.*

incorporar a la iniciativa privada y a los ciudadanos de a pie en actos estrictamente relacionados con la guerra:

> "La Ciber Reserva será una parte esencial para asegurar que defendemos la seguridad nacional en el ciberespacio. Esta es una fantástica oportunidad para que expertos en la industria de Internet puedan poner sus conocimientos para que sean aprovechados por la nación, protegiendo servicios vitales y nuestras capacidades informáticas"[119]

Cabe aclarar que en todo momento, Hammond trató de delinear el esquema operativo y normativo bajo el que actuarían los civiles en los escenarios de conflicto: "[…] los reservistas trabajarán junto a las fuerzas regulares para proteger redes críticas de ordenadores y salvaguardar datos vitales."[120] Sin embargo, aún cuando la prioridad del Ministro de Defensa fue establecer la distinción entre lo militar y lo civil, queda claro, otra vez, que en los nuevos conflictos esta delimitación se está esfumando –tal como lo asumen en aquel país del continente europeo-.

Con todo, el caso británico muestra el camino seguido por muchas otras naciones en la actualidad, escenario que ya había sido identificado desde hace algunos años por la compañía de seguridad virtual McAfee. Ahora bien, estos dos escenarios descritos anteriormente –el del fortalecimiento y el de creación de las unidades militares para el ciberespacio- dan pie a la tercera cuestión de este apartado: la de la cooperación internacional en el ramo.

La cooperación internacional en materia de seguridad informática puede alentar el desarrollo de distintas líneas de acción para reforzar el nuevo campo de batalla virtual, empero, las más comunes son dos: la de la asesoría para construir grupos de defensa del ciberespacio nacional o, por el contrario, en tareas más específicas como reforzar inteligencia sobre el tema o compartir tácticas y soluciones técnicas sobre el mismo.

---

[119] *Idem.*
[120] *Idem.*

El primer escenario es fácil de ilustrar, pues basta mencionar la asesoría que brindó la OTAN a Estonia en 2007 sobre ciberguerras, hecho que derivó en la creación del Centro de Excelencia para la Cooperación en Ciberdefensa (CCDCOE, por sus siglas en inglés), organismo de enorme trascendencia para el tema que se analiza en este trabajo. En lo que refiere a las otras dos opciones, pueden ponerse sobre la mesa dos casos diferentes: el primero sería, por supuesto, el constante intercambio de información de inteligencia obtenida a través de espionaje entre la Agencia de Seguridad Nacional estadunidense y el *Government Communications Headquarters* de Reino Unido, interacción que fue destapada por el ex analista de la CIA Edward Snowden en el año 2013; en segundo lugar, es posible hacer alusión a la cooperación técnica que Estonia le brindó a Georgia durante su conflicto cibernético, situación a la que se hace referencia en el capítulo anterior.

Así pues, estos tres factores analizados en esta sección dan pie para entender el siguiente apartado, mismo que versa sobre la presencia del factor informático en los conflictos futuros y como éste puede aumentar la presencia y el rango de acción de los llamados conflictos asimétricos.

4.3 La presencia del vector informático en los conflictos futuros y la acentuación de las batallas asimétricas.

La dispersión en el globo del escenario anteriormente descrito de creación o reestructuramiento y fortalecimiento de instituciones encargadas de resguardar el ciberespacio nacional de cada Estado da pistas sobre lo que le espera el mundo en los próximos años en lo que a conflictos bélicos se refiere pues, tomando en consideración todo lo analizado, no es de extrañar que muchos especialistas confirmen que las guerras del futuro tendrán siempre la presencia del vector virtual durante su desarrollo, incorporándolo como un nuevo campo de batalla plenamente consolidado capaz de dañar de la misma forma que los métodos tradicionales de agresión.

En este sentido, el espectro de uso que podrán darle los diversos ejércitos informáticos alrededor del globo a las redes de comunicaciones y al ciberespacio será tan grande y variado que no es posible describirlo y analizarlo a detalle en este trabajo, empero, es importante mencionar algunas de las tácticas que podrían ser utilizadas dentro de una guerra futura para ilustrar el impacto que esta tecnología puede tener en el desarrollo de una batalla. Desde el punto de vista del autor de este trabajo, las tácticas más destacadas serán las siguientes:

- En primer lugar, la alta dependencia tecnológica propia de algunas infraestructuras críticas –como plantas eléctricas, acuíferas, petroleras y nucleares, por ejemplo- puede suponer un excelente objetivo para generar un gran daño en el enemigo: mediante un ataque informático cuidadosamente coordinado por un ciberejército, un gobierno puede desmantelar –e incluso destruir- remotamente a estas instalaciones, ahorrando una enorme suma monetaria al tiempo que causa estragos sociales, económicos, políticos e incluso estratégicos en el país objetivo.
- De igual manera, la gran penetración de los sistemas tecnológicos en los organismos encargados de la seguridad nacional de los diversos Estados así como los dispositivos y procesos de comunicación actualmente utilizados por funcionarios relacionados con el actuar del gobierno, aunado al uso de equipos electrónicos en medios de difusión de información, pueden ser un escenario llamativo de ataque para un ciberejército enemigo: al igual que en el caso georgiano, éstos pueden ser presa de un ataque que desencadenaría una falla generalizada en las formas en la que normalmente nos comunicamos, generando caos y confusión dentro de un país al tiempo que lo aísla del resto del mundo; hechos que confieren una gran ventaja operativa y táctica a la contraparte atacante sin malgastar mayores recursos.
- Otra táctica relevante sería hacer uso de las Tecnologías de la Información y Comunicaciones como una vía para el espionaje de avanzada a nivel gubernamental y militar de una forma más fácil, continua e incluso con un

rango más grande de acción. Este escenario alentaría el robo y filtración de información clasificada, situación que concedería gran ventaja estratégica al enemigo y que podría poner en riesgo al Estado afectado mediante la diseminación de los datos críticos entre sus ciudadanos.

Estos hechos no harán otra cosa más que agravar el panorama de las guerras asimétricas que se desarrollarán a futuro en el mundo pues, como es de observarse, esta novedosa forma de dañar al enemigo no encaja por completo en los métodos de guerra tradicionales que se han estado ocupando en los conflictos hasta hace poco tiempo. En este sentido, cabe recordar que un conflicto asimétrico se refiere a la lucha "[…] que se da entre dos contendientes con una desproporción de los medios a su disposición, ya sean militares, políticos, económicos, mediáticos, etc.;" [121] hecho que los obliga a emplear estrategias que se salen del marco estratégico común.

Bajo este supuesto, no sería de extrañar que un Estado considerado débil dentro del marco clásico de la guerra termine por convertirse en una gran amenaza si utiliza este tipo de recursos a su favor y en contra de una potencia enemiga: por ejemplo, qué pasaría si un país con poca dependencia tecnológica y bajo índice de conectividad a Internet utilizará la vía virtual para dar un golpe estratégico a un país como Estados Unidos, cuyos procesos productivos, económicos e incluso comunicativos se encuentran estrechamente ligados a procesos meramente electrónicos. Claramente, esta situación puede darse también de forma inversa.

Así pues, los conflictos asimétricos paradójicamente podría regresarle un poco de equilibrio estratégico a este mundo donde sólo destacan por su poderío unos pocos Estados, generando, al mismo tiempo, un clima más hostil en el planeta debido a las nuevas estrategias que podrían ser utilizadas para infligir daño a la infraestructura e incluso a la sociedad de un país.

[121] Vicente Romano, *La guerra asimétrica*, [en línea], Rebelión, Dirección URL: http://www.rebelion.org/noticia.php?id=68310, [consulta: 12 de noviembre de 2013].

Con todo, no es extrañar que, debido a esta situación, comiencen a surgir propuestas alrededor del planeta que intenten regular e incluso prohibir algunas conductas hostiles relacionadas con el uso de las nuevas tecnologías e Internet por parte de los gobiernos y sus nacionales, afectando gravemente a la libertad de las que habían gozado desde su invención hasta ahora. Sobre esto se comenta a fondo en el siguiente apartado.

4.4 La búsqueda de instrumentos internacionales y nacionales que limiten las ciberbatallas y, por tanto, la libertad que ha existido en las Tecnologías de la Información y Comunicaciones, en específico, Internet.

Tras percatarse de la hecatombe que traía consigo la consolidación de las nuevas guerras y, dentro de éstas, de las ciberbatallas, algunos países con trascendencia estratégica comenzaron a formular y promover acuerdos internacionales –y en algunos casos leyes nacionales- que pudieran contener la dispersión de estos fenómenos conflictivos. Con este acto, diversas libertades inherentes a las nuevas tecnologías podrían ser restringidas e incluso prohibidas, hecho que ha generado diversas protestas alrededor del mundo que al tiempo han desembocado en la desaprobación de estas propuestas de origen estrictamente gubernamental. Por todo esto, a continuación se hace un breve repaso de las iniciativas más relevantes en el ramo y, finalmente, se realiza una reflexión sobre las mismas.

En 2010, tan solo dos años después de la ciberguerra ruso-georgiana, Hamadoun Touré, Secretario General de la Unión Internacional de Telecomunicaciones (UIT), sugirió en Davos que el mundo necesitaba de manera apremiante un Tratado para defenderse de los ataques cibernéticos antes de que

éstos desencadenaran una ciberguerra de mayor alcance o, como el le llamaba, guerra de Internet[122].

La iniciativa de Touré, impulsada por unos ataques que recién había recibido Google en sus redes por parte del gobierno chino, proponía que, mediante un acuerdo jurídico, los Estados se comprometieran a no lanzar primero un ciberataque en contra de otra entidad estatal pues, según él, sólo de esta forma podría evitarse un acontecimiento que podría dejar "peores consecuencias que un tsunami".

Tras la declaración del Secretario General de la UIT comenzaron a surgir diversos comentarios negativos hacia la propuesta entre los asistentes al foro: por ejemplo, John Negroponte, ex director de la CIA, manifestó que todas las agencias secretas y de seguridad establecidas alrededor del mundo impondrían reservas a la idea debido a su naturaleza estratégica en el campo de batalla[123]. Dicho comentario sería posteriormente apoyado por una serie de congresistas de su país, entre ellos la senadora republicana Susan Collins.

Estas últimas declaraciones no hicieron otra cosa más que levantar sospechas contra los planes estadunidenses en cuanto a la regulación de la guerra cibernética y las actividades en Internet, escenario que se daría a conocer poco tiempo después de la propuesta de Touré. Así pues, en octubre de 2011 la Cámara de Representantes de aquél país presentaba una medida unilateral conocida como *Stop Online Piracy Act*, también llamada Ley SOPA, misma que pretendía regular las actividades de piratería en Internet[124]; sin embargo, más tarde diversos sectores, entre ellos Organizaciones No Gubernamentales, empresas privadas e incluso la

[122] *Vid* s/a, *ONU busca acuerdo para evitar 'ciberguerra'*, [en línea], El Economista, 30 de enero de 2010, Dirección URL: http://eleconomista.com.mx/tecnociencia/2010/01/30/onu-busca-acuerdo-evitar-ciberguerra, [consulta: 13 de noviembre de 2013].
[123] *Vid Idem.*
[124] *Vid* Julianne Pepitone, *SOPA explainded: what it is and why it matters*, [en línea], CNN Money, Enero 20 de 2012, Dirección URL: http://money.cnn.com/2012/01/17/technology/sopa_explained/, [consulta: 15 de noviembre de 2013].

sociedad civil dieron cuenta de las verdaderas intenciones del proyecto de este Estado: con el pretexto de terminar con la diseminación de material ilegal en la web, el gobierno estadunidense sería capaz de monitorear las actividades de todos los usuarios que fueran participes del tráfico de los servidores instalados en su territorio que, dicho sea de paso, alojan la mayor cantidad de páginas con enormes números de visitantes del mundo.

En este sentido, mediante este instrumento Estados Unidos sería capaz de censurar todo tipo de contenidos inconvenientes en la red, además de que éste le daría un marco jurídico pleno para iniciar labores avanzadas en el monitoreo de los datos que viajan a través de toda la fibra óptica que conforma a Internet, poniendo todo este escenario a su favor en caso de que un conflicto con la presencia del vector virtual explotase.

Con todo, es por todos conocido que este proyecto terminó por archivarse en los confines del Congreso debido a todas las protestas que generó a lo largo del mundo; sin embargo, no está por demás advertir que parece ser que este es el camino que pretenden seguir diversos Estados para cobijarse de la posible explosión de una ciberbatalla de gran escala: basta con mencionar el Acuerdo Comercial Anti-Falsificación (ACTA) y la iniciativa PIPA (*Preventing Real Online Threats to Economic Creativity and Theft of Intellectua Property Act*), mismas que terminaron bajo las mismas circunstancias que la Ley SOPA.

Todo este delicado escenario no hace más que generar una enorme pregunta que desde hace tiempo se plantean especialistas de diversas disciplinas que tienen que ver con el tema: ¿es posible regular mediante tratados internacionales o leyes nacionales a los conflictos cibernéticos, a las ciberguerras? Si se atiende al enorme número de factores que intervienen en la pregunta, ésta pareciera tener siempre una respuesta negativa ante los contundentes argumentos en su contra:

- En primer lugar, pocos países estarían dispuestos a perder la ventaja estratégica que conlleva el conocer y manipular al campo de batalla virtual, tal como lo expresó en su momento Negroponte. Así pues, las ciberarmas de avanzada que hasta el momento se han concebido, al igual que las que se desarrollarán en el futuro, seguirán siendo un tema tabú para los países con capacidades ofensivas avanzadas, tal y como ocurre con las bombas nucleares.
- En segundo lugar, y aun cuando comienzan a formarse ejércitos específicamente diseñados para actuar en la Internet, sería prácticamente imposible definir a los sujetos que participarían en los conflictos informáticos a regularse pues, tal y como se vio en el caso georgiano, el rango de colaboradores se extiende más allá de la esfera estatal e incluso alcanza a impregnar a ciudadanos de a pie que no tienen conocimientos profundos en informática pero que de alguna manera fueron arrastrados hacia el conflicto.
- En tercer lugar, existiría una enorme dificultad para encontrar un balance entre las cosas que podrían ser incluidas y excluidas en el instrumento jurídico desde el punto de vista de los Estados. En este sentido, la dificultad de esta situación residiría estrictamente en las necesidades que cada país convenga como urgentes con respecto al tema y, claramente, las opiniones alrededor del mundo estarán extremadamente polarizadas.
- Finalmente, ¿quién sería el encargado de hacer cumplir el instrumento internacional? Más aún, ¿no es necesario mantener un monitoreo activo y constante de todas las actividades realizadas en Internet por todos los usuarios de este mundo? ¿Qué pasaría con la libertad que rodea a este medio?

Como se puede observar, por el momento todos los supuestos parecen asegurar que no podrá existir en un tiempo cercano un Tratado capaz de regular estos fenómenos bélicos. Sin embargo, a pesar de toda esta negatividad se comienza a vislumbrar una luz al final del camino: en años recientes, Estados Unidos y Rusia iniciaron conversaciones junto con un comité de la ONU sobre el

reforzamiento de la seguridad en Internet y sobre la limitación del uso militar de este medio, hecho que marcó un precedente en el tema[125].

De igual forma, las propuestas nacionales comienzan a despegar debido al incremento de la hostilidad en el panorama ciberespacial: por ejemplo, recientemente fue aprobada parcialmente la iniciativa estadunidense CISPA (*Cyber Intelligence Sharing and Protection Act*), misma que establece el intercambio de información de inteligencia entre el gobierno y las empresas destacadas en el ramo de la tecnología con el fin de identificar y analizar las amenazas que rondan a la Internet así como garantizar la seguridad de la infraestructura electrónica contra los ataques cibernéticos[126]. Si bien el proyecto no ha sido aceptado completamente, éste establece por lo menos un hito histórico al tener por primera vez el visto bueno de los gigantes de la industria tecnológica.

No cabe duda que es prácticamente imposible determinar el resultado que tendrán éstos dos últimos hechos, sin embargo, lo que es inevitablemente un hecho es que las ciberguerras han modificado completamente al paradigma que hasta hace poco rodeaba al concepto y a la noción de la seguridad misma, tanto a nivel nacional como internacional.

[125] *Vid* s/a, *EEUU y Rusia inician conversaciones sobre ciberseguridad (informe)*, [en línea], Terra, 13 de diciembre de 2009, Dirección URL: http://noticias.terra.com/noticias/eeuu_y_rusia_inician_conversaciones_sobre_ciberseguridad_informe/act2104412, [consulta: 15 de noviembre de 2013].
[126] *Vid* s/a, *H.R. 3523*, [en línea], House of Representatives, 30 de noviembre de 2011, Dirección URL: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf, [consulta: 15 de noviembre de 2013].

Conclusiones.

Tal como lo enuncia la hipótesis del presente trabajo, las nuevas guerras en conjunto con la dispersión e impregnación de la tecnología en los distintos procesos productivos, así como en las actividades que realizamos día con día, se convirtieron en el escenario perfecto que posibilitó el surgimiento y posterior fortalecimiento de las ciberguerras como un método estandarizado de agresión entre Estados y actores no gubernamentales.

Este peculiar clima de nacimiento fue el mismo que les confirió las atípicas características que conforman a este nuevo fenómeno bélico virtual: la participación de actores ajenos al ente estatal, la utilización de armas diferentes a las tradicionales, la facilidad con la que se pueden emprender, el uso de tecnologías computacionales complejas, la velocidad con la que se desarrollan los ataques así como el anonimato en el que se generan son, por mucho, producto del intrincado ambiente que se vive en el marco del nuevo milenio.

Con base en todo lo anterior, y considerando los enormes ahorros económicos que genera al agresor, las ciberguerras se han hecho extremadamente populares para realizar ataques quirúrgicos capaces de poner en jaque por algunos momentos a Estados que contravengan a los interés estratégicos de otros países hegemónicos: el caso de Irán y Estonia así como el auge del espionaje de avanzada a nivel global ilustran de manera perfecta dicho postulado. Por su parte, el caso georgiano demuestra que el uso del vector informático como una línea adicional de fuego dentro de un conflicto tradicional puede llegar a ser tan efectivo como la movilización de tanques y aviones al terreno de batalla, pero con la ventaja de salvar recursos humanos y monetarios así como con el incentivo estratégico de pasar desapercibido ante las fuerzas enemigas, y más importante aún, ante la opinión internacional.

En este mismo sentido, vale la pena reflexionar sobre cómo estos novedosos elementos remarcan la clara diferencia que existe entre los conflictos que se dan en

la actualidad y los que ocurrieron en tiempos anteriores: la eliminación de la línea divisoria entre lo militar y lo civil, la ampliación del campo de batalla hacia terrenos que anteriormente eran desconocidos así como los métodos empleados en la arena de combate no hacen otra cosa más que remarcar el carácter cambiante de la guerra a través de los años, en específico, como ésta se moldea y acopla a los comportamientos de los seres humanos así como a las capacidades técnicas y de organización política, económica, social y cultural que estos mismos desarrollan en un lugar y tiempo determinado.

Es por este mismo carácter transformista de la guerra que los Estados deben reformular continuamente las políticas y estrategias de seguridad que garanticen su integridad y supervivencia en el escenario caótico que representan actualmente las relaciones internacionales: primero fue el desarrollo de armas convencionales para generar ventaja competitiva ante el contrincante, después el aseguramiento del espacio marítimo mediante la construcción de embarcaciones de batalla y, en seguida, el cercamiento del aire con la puesta en marcha de aviones de combate. Ahora, toca el turno de la militarización a gran escala del ciberespacio ante las constantes amenazas que éste comienza a representar. En pocas palabras, el concepto de seguridad es tan cambiante y trascendente como el de la guerra misma.

En este orden de ideas, es importante recalcar que en diversas ocasiones el reforzamiento de las políticas de seguridad sólo puede lograrse mediante la cooperación internacional: así pues, como vemos en el caso de las ciberguerras, es de tal trascendencia la amenaza que los distintos países alrededor del mundo tienen que poner en marcha programas de cooperación técnica y de inteligencia para protegerse de las posibles consecuencias de una batalla informática dirigida en su contra. En este sentido, valdría la pena revisar en un futuro los alcances que podría llegar a tener el aseguramiento grupal del espacio cibernético pero sobre todo las limitantes que pudiera llegar a imponer de manera colateral en uno de los medios que hasta ahora ha gozada de libertad absoluta: la Internet.

Sobre el tema de cooperación, también valdría la pena abundar sobre las opciones que barajan algunos de los países que no han sido integrados a este selecto circulo de ayuda: por ejemplo, qué acciones podrían tomar en el campo de las ciberbatallas aquellos Estados considerados rebeldes y qué efectos causarían sobre la arena política y estratégica del plano internacional.

En el otro extremo del argumento, qué podrían hacer los países que no cuentan con la capacidad técnica ni económica para desarrollar defensas en el ciberespacio, tal como ocurre en el caso de México y algunos países de Sudamérica. Con todo, no hay que perder de vista que las batallas a través del ciberespacio pueden reequilibrar el mapa estratégico militar que actualmente predomina en el escenario internacional, y por ello, ningún país dejará pasar eventualmente la oportunidad de desarrollar este tipo de instrumentos letales atípicos.

Ahora bien, si el lector presta atención a los últimos párrafos desarrollados en esta sección –mismos que condensan los hallazgos derivados del análisis- se dará cuenta de que todos los postulados aquí vertidos encajan de manera perfecta en una de las teorías con más relevancia en Relaciones Internacionales: el realismo. La creación y potenciación de novedosos armamentos (en este caso virtuales), así como la formación de alianzas a través de la cooperación, no hacen más que demostrar que el fin último de los Estados, tal cual proponen los números autores de la corriente realista, es la búsqueda y conservación de poder, mismo que garantizará su supervivencia en un entorno internacional anárquico, cambiante e inestable.

En este mismo sentido, y ya en el terreno de la previsión permitida por la disciplina de Relaciones Internacionales, no sería difícil suponer que podrían surgir nuevos entes hegemónicos en términos de la teoría realista: el afán de acumular poder siempre ha formado parte de los objetivos e intereses nacionales de los

distintos países que existen, y el surgimiento de las ciberguerras y su explotación por éstos parece ser el vehículo ideal para alcanzar tal cometido. Desde luego que dicho escenario no se desenvolverá en los términos más pacíficos, pues tal como Morgenthau planteó en *Politics among nations*, todos aquellos Estados que luchen por el poder entrarán fatalmente en conflicto con sus iguales que buscan alcanzar la misma aspiración: esto significa, en el tema que nos ocupa, un posible aumento en el número de eventos bélicos virtuales así como un incremento importante en la letalidad de los mismos.

Como sea, es un hecho que las batallas en el ciberespacio son ya una realidad de este siglo: la ciberguerra librada entre Rusia y Georgia en 2008 no hizo otra cosa más que mostrar al mundo que es un fenómeno que está presente entre nosotros y que tiene la misma capacidad que un conflicto convencional para dañar infraestructuras y sociedades alrededor del globo. Sin embargo, aun cuando hemos sido testigos de sus capacidades, estamos lejos de presenciar el verdadero potencial destructivo que puede alcanzar si se continúa con su desarrollo en el plano estrictamente castrense y si se sigue con la tendencia de imponer un componente electrónico e informático en todas las actividades que acontecen en la Tierra diariamente.

Finalmente, y con todo lo anteriormente expuesto, es menester mencionar también que debido a la trascendencia del fenómeno en prácticamente todas las disciplinas (debido a su carácter técnico y social), han comenzado a surgir cada vez más investigaciones y análisis a profundidad en torno al tema a lo largo del mundo, hecho que sin duda alguna enriquecerá la comprensión del mismo y que, desde luego, impactará en la formulación de las políticas de los Estados y en las posturas de otros organismos no estatales así como en la visión que todos los seres humanos de a pie tienen sobre una herramienta tan cotidiana como lo es la Internet.

Fuentes.

Fuentes bibliográficas

- A. Clarke, Richard *Cyber War: The next threat to national security and what to do about* it, Estados Unidos, HarperCollins, 2010, 320 pp.
- Archer, Christon I.; John R. Ferris, Holger H. Herwig, Timothy H. E. Travers, World History of Warfare, Estados Unidos, University of Nebraska Press, 2002, 626 pp.
- Bobbitt, Philip, *Terror and consent: the wars for the twenty-first century*, Estados Unidos, Anchor, 2009, 688 pp.
- Bobbitt, Philip, *The shield of Achilles: war, peace, and the course of history*, Estados Unidos, Anchor, 2011, 962 pp.
- C. Libicki, Martin, *Cyberdeterrence and cyberwar*, Estados Unidos, RAND Corporation, 2009, 238 pp.
- Carr, Jeffrey, *Inside Cyber Warfare: mapping the Cyber underwold*, Estados Unidos, O'Reilly, 2010, 318 pp.
- Clausewitz, Carl von, *De la guerra*, México, Colofón, 2006, 612 pp.
- D. Kramer, Fraklin, H. Starr, Staurt y K. Wentz, Larry (editores), *Cyberpower and National Security*, Washington D. C., Center for Technology and National Security Policy/National Defense University, 664 pp.
- Duarte Carvalho, Fernando; Mateus da Silva, Eduardo. *Cyberwar-Netwar: security in the Information Age*, Portugal, The NATO Programme for Security trough Science, 2006, 159 pp.
- Duffield, Mark, Las nuevas guerras en el mundo global. La convergencia entre desarrollo y seguridad, Madrid, Catarata, 2004, 347 pp.
- E. Mehan, Julie, *Cyberwar, cyberterror, cybercrime*, Reino Unido, IT Governance Publishing, 2008, 280 pp.
- F. Halpin, Edward, *et. al.*, *Cyberwar, netwar and the revolution in military affairs (part 1)*, Estados Unidos, Palgrave Macmillan, 2006, 304 pp.
- Friedman, Allan, Singer, P. W., *Cybersecurity and cyberwar: what everyone needs to know*, Estados Unidos, Oxford University Press, 2014, 320 pp.

- Girard, René, Clausewitz en los extremos. Política, guerra y apocalipsis, Argentina, Katz editores, 2010, 306 pp.
- Hernández-Vela, Edmundo, *Diccionario de Política* Internacional, México, Porrúa, Tomo I, 2001, 612 pp.
- Hirst, Paul, War and Power in the Twenty-First Century, Londres, Cambridge University Press, 2001, 176 pp
- Hobsbawm, Eric, *Guerra y paz en el siglo XXI*, España, Crítica, 2007, 179 pp.
- J. Betz, David, C. Stevens, Timothy, *Cyberspace and the state: towards a strategy for cyberpower*, Estados Unidos, Routledge, 2012, 158 pp.
- J. Janczewski, Lech, M. Colarik, Andrew, *Cyber warfare and cyber terrorism*, Estados Unidos, IGI Global, 2007, 532 pp.
- Kaldor, Mary, *Las nuevas guerras: violencia organizada en la era global*, España, Tusquets, 2001, pp. 248 pp.
- Keegan, John, *A history of warfare*, Reino Unido, Vintage, 1993, 432 pp.
- Keegan, John, *War and our world*, Reino Unido, Vintage, 2001, 112 pp.
- Keeley, Lawrence H., War before civilization, Estados Unidos, Oxford University Press, 1996, 245 pp.
- Liang, Qiao, Xiangsui, Wang, *Unrestricted Warfare: China's master plan to destroy America*, Panama, Pan American, 2002, 208 pp.
- Maleševi'c, Siniša, The sociology of war and violence, Londres, Cambridge University Press, 2010, 376 pp.
- Moran, Daniel, Strategic theory and the History of war, Estados Unidos, Naval Postgraduated School, 2001, 17 pp
- Münkler, Herfried, The new wars, Estados Unidos, Polity Press, 2005, 180 pp.
- Parker, Geoffrey (ed.), Historia de la guerra, España, Ediciones AKAL, 2010, 544 pp.
- Porter, Bruce D., *War and the rise of the State: The military foundations of modern politics*, Estados Unidos, The Free Press, 1994, 400 pp.

- Rosenzweig, Paul, *Cyber warfare: how conflicts in cyberspace are challenging America and changing the world,* Estados Unidos, Praeger, 2013, 290 pp.
- S. Reveron, Derek, *Cyberspace and national security: threats, opportunities, and power in a virtual world*, Estados Unidos, Georgetown University Press, 2012, 256 pp.
- Sloterdijk, Peter, *Temblores de aire: en las fuentes del terror*, España, Pre-textos, 2003, 142 pp.
- Stiennon, Richard, *Surviving Cyber War*, Estados Unidos, Government Institutes, 2010, 170 pp.
- Townshend, Charles (ed.), The Oxford history of modern war, Gran Bretaña, Oxford University Press, 2000, 407 pp.
- Van Creveld, Martin, The culture of war, Nueva York, Ballantine books, 2008, 485 pp.
- van Creveld, Martin, *The transformation of war*, Estados Unidos, The Free press, 1991, 272 pp.
- Ventre, Daniel, *Cyberwar and information warfare*, Reino Unido, Wiley-ISTE, 2011, 448 pp.

Fuentes electrónicas

- AFP, *Russia moves SS-21 missiles into Georgia: US defense oficial*, [en línea], AFP, 18 de agosto de 2008, Dirección URL: http://www.google.com/hostednews/afp/article/ALeqM5iiba8YaYXz88Y9n9OQBVKp9ofSig?hl=en
- Arguilla, John; Ronfeldt, David. *The advent of netwar (revisted)*, [en línea], Estados Unidos, rand.org, Dirección URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch1.pdf.
- BBC, *El nuevo campo de entrenamiento para las ciberguerras*, [en línea], BBC, 18 de junio de 2011, Dirección URL:

http://www.bbc.co.uk/mundo/noticias/2011/06/110617_eeuu_ejercito_ciberataque_ciberguerra_internet_jg.shtml

- Billo, Charles G. *Cyber warfare: an analysis of the means and motivations of selected nation states*, [en línea], Estados Unidos, Institute for Security Technology Studies At Darmouth College, Dirección URL: http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf.
- Central Intelligence Agency, *Georgia,* [en línea], CIA, Dirección URL: https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html,
- Central Intelligence Agency, *Russia*, [en línea], CIA, Dirección URL: https://www.cia.gov/library/publications/the-world-factbook/geos/rs.html,
- Cluley, Graham, *Was Twitter denial-of-service targeting anti-Russia blogger?,* [en línea], Naked Security, 7 de agosto de 2009, Dirección URL: http://nakedsecurity.sophos.com/2009/08/07/twitter-denialofservice-targeting-antirussian-blogger/,
- Danchev, Dancho, *Coordinated Russia vs Georgia cyber attack in progress*, [en línea], ZDNet, 11 de agosto de 2008, Dirección URL: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670
- DCAF, *Democratic Governance Challenges of Cyber Security*, [en línea], Génova, DCAF, 2009, Dirección URL: http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security
- De Alzaga, Pedro, Pastor, Enric, *El "virus del amor" colapsa ordenadores de todo el mundo*, [en línea], El Mundo, 5 de mayo de 2000, Dirección URL: http://www.elmundo.es/navegante/2000/05/05/ailofiu_virus.html
- Departament of Defense, *Information Operations Roadmap*, [en línea], Departamento de la Defensa de Estados Unidos de América, 30 de octubre de 2003, Dirección URL: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/info_ops_roadmap.pdf,

- Department of Defense, *Department of Defense strategy for operating in cyberspace*, [en línea], Department of Defense, Julio de 2011, Dirección URL: http://www.defense.gov/news/d20110714cyber.pdf
- Espiner, Tom, *Georgia accuses Russia of coordinated* cyberattack, [en línea], Cnet, 11 de agosto de 2008, Dirección URL: http://news.cnet.com/8301-1009_3-10014150-83.html
- Francis Mexidor, Deisy. *Ciberguerra: mercenarismo en la red* [en línea], Cuba, Granma.cu, 22 de marzo del 2011, Direccion URL: http://www.granma.cubaweb.cu/2011/03/22/nacional/artic05.html, [consulta: 6 de octubre de 2011].
- Gartner Inc., *Gartner says more tan 1 billion PCs in use worldwide and headed to 2 billion units by 2014*, [en línea], Gartner Inc., 23 de junio de 2008, Dirección URL: http://www.gartner.com/newsroom/id/703807,
- Gutiérrez del Cid, Ana Teresa, *La OTAN y el conflicto Georgia-Rusia por Osetia del Sur,* [en línea], Revista de Relaciones Internacionales-UNAM, Dirección URL: http://www.journals.unam.mx/index.php/rri/article/download/16322/15528,
- Janssen, Cory, Cyberspyng, [en línea], Techopedia, Dirección URL: http://www.techopedia.com/definition/27101/cyberspying
- Kaspersky Lab, *Kaspersky Lab provides its insights on Stuxnet* worm, [en línea], Kaspersky Lab, 2010, Dirección URL: http://www.kaspersky.com/news?id=207576183
- Kaspersky Lab, *The "Red October" Campaign- An advance cyber espionage network targeting diplomatic and government agencies*, [en línea], Kaspersky Lab, 14 de enero de 2013, Dirección URL: http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies
- Lecaros, Monserrat, *Primer informe ONU: 34% de la región se conecta a banda ancha*, [en línea], América Economía, 24 de septiembre de 2012,

Dirección URL: http://tecno.americaeconomia.com/noticias/primer-informe-onu-34-de-la-region-se-conecta-banda-ancha

- Lee, Michael, *China not behind US military chip* backdoor, [en línea], ZDNet, 30 de mayo de 2012, Dirección URL: http://www.zdnet.com/china-not-behind-us-military-chip-backdoor-1339338798/
- Lemos, Robert, *Inside the ILOVEYOU worm*, [en línea], ZDNET, 5 de mayo de 2000, Dirección URL: http://www.zdnet.com/news/inside-the-iloveyou-worm/107344
- Márquez, William, *Ciberespacio: el nuevo ámbito de guerra para el Pentágono*, [en línea], BBC, 27 de julio de 2001, Dirección URL: http://www.bbc.co.uk/mundo/noticias/2011/07/110722_eeuu_pentagono_ciberespacio_estrategia_wbm.shtml
- McAfee, *Informe sobre criminología virtual 2009: La era de la ciberguerra, casi una realidad*, [en línea], McAfee, Dirección URL: http://www.mcafee.com/mx/resources/reports/rp-virtual-criminology-report-2009.pdf
- McGlaun, Shane, *Report: Chinese built US military chip has a backdoor,* [en línea], TG Daily, 29 de mayo de 2012, Dirección URL: http://www.tgdaily.com/security-brief/63684-report-chinese-built-us-military-chip-has-a-back-door
- Medvédev, Dmitri, *Statement on the situation in South Ossetia*, [en línea], President of Russia, 8 de agosto de 2008, Dirección URL: http://archive.kremlin.ru/eng/speeches/2008/08/08/1553_type82912type82913_205032.shtml
- Moses, Asher, *Georgian websites forced offline in cyber war*, [en línea], The Sidney Morning Herald, 12 de agosto de 2008, Dirección URL: http://www.smh.com.au/news/technology/georgian-websites-forced-offline-in-cyber-war/2008/08/12/1218306848654.html
- Nitzberg, Sam, *The cyber battlefield- Is this the setting for the ultimate World War?*, [en línea], Telos Information Protection Solutios, octubre de 1998, Dirección URL:

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.393&rep=rep1&type=pdf

- Oppenheimer, Walter, *Reino Unido convoca un Ejército de 'hackers' para su defensa*, [en línea], El país, 6 de octubre de 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/10/05/actualidad/1380999276_830357.html
- P. Liff, Adam, *Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare and interstate war,* [en línea], Journal of Strategic Studies, 2012, Dirección URL: http://www.tandfonline.com/doi/abs/10.1080/01402390.2012.663252,
- Panda Security, *Virus informático: una categoría con una larga trayectoria que permanece al margen de la nueva dinámica del malware*, [en línea], Panda Security, Dirección URL: http://www.pandasecurity.com/spain/homeusers/security-info/classic-malware/virus/
- Parfitt, Tom, *Georgian blogger Cyxymu blames Russia for cyber attack*, [en línea], The Guardian, 7 de agosto de 2009, Dirección URL: http://www.theguardian.com/world/2009/aug/07/georgian-blogger-accuses-russia
- Pepitone, Julianne, *SOPA explainded: what it is and why it matters*, [en línea], CNN Money, Enero 20 de 2012, Dirección URL: http://money.cnn.com/2012/01/17/technology/sopa_explained/
- Piquer, Isabel, *EEUU equipara los ciberataques con actos bélicos*, [en línea], Públiclo.es, 31 de mayo de 2011, Dirección URL: http://www.publico.es/internacional/379427/eeuu-equipara-los-ciberataques-con-actos-belicos
- Protalinskyi, Emil, *Former Pentagon analyst: China has backdoors to 80% of telecoms,* [en línea], ZDNet, 14 de julio 2012, Dirección URL: http://www.zdnet.com/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms-7000000908/

- R. Hooper, Charles, *The ten worst computer viruses,* [en línea], TopTen Reviews, Dirección URL: http://anti-virus-software-review.toptenreviews.com/the-ten-worst-computer-viruses.html/?cmpid=ttr-llm
- Ramsay, Brett, *Ciberguerra: saltando la Gran Muralla 'cibernética'*, [en línea], El ojo digital, 15 de noviembre de 2013, Dirección URL: http://www.elojodigital.com/contenido/12710-ciberguerra-saltando-la-gran-muralla-cibernetica
- RIA Novosti, *Conflicto bélico en Osetia del Sur. Infografía*, [en línea], RIA Novosti, Dirección URL: http://sp.ria.ru/infografia/20080910/116667323.html
- RIA Novosti, *Guerra de los cinco días entre Rusia y Georgia en agosto de 2008: crónica y balance de víctimas del conflicto. Infografía,* [en línea], RIA Novosti, Dirección URL: http://sp.ria.ru/infografia/20130808/157745603.html
- RIA Novosti, *Historia de las relaciones entre Rusia y* Georgia, [en línea], RIA Novosti, 6 de septiembre de 2010, Dirección URL: http://sp.ria.ru/opinion_analysis/20100906/127670666.html
- RIA Novosti, *Medvédev firmó los seis principios de arreglo del conflicto en Georgia,* [en línea], RIA Novosti, 16 de agosto de 2008, Dirección URL: http://sp.rian.ru/international/20080816/116082935.html
- RIA Novosti, *Tratado de Gueorguievsk entre Rusia y Georgia (1783). Infografía*, [en línea], RIA Novosti, Dirección URL: http://sp.ria.ru/infografia/20080813/116008448.html
- Rodrigo Fernández. *Guerra abierta entre Rusia y Georgia*, [en línea], España, El País, Dirección URL: http://www.elpais.com/articulo/internacional/Guerra/abierta/Rusia/Georgia/elpepuint/20080810elpepiint_1/Tes, [consulta: 26 de noviembre de 2011].
- Romano, Vicente, *La guerra asimétrica*, [en línea], Rebelión, Dirección URL: http://www.rebelion.org/noticia.php?id=68310
- Rosas, María Cristina, *De la ciberguerra a la ciberpaz*, [en línea], revisa Etcétera, 2011, dirección URL: http://www.etcetera.com.mx/articulo.php?articulo=9759

- s/a, *EEUU y Rusia inician conversaciones sobre ciberseguridad (informe)*, [en línea], Terra, 13 de diciembre de 2009, Dirección URL: http://noticias.terra.com/noticias/eeuu_y_rusia_inician_conversaciones_sobre_ciberseguridad_informe/act2104412
- S/a, *El ciberataque más fuerte que reduce la velocidad de internet*, [en línea], BBC Mundo, 27 de marzo de 2013, Dirección URL: http://www.bbc.co.uk/mundo/ultimas_noticias/2013/03/130327_ultnot_ciberataque_afecta_velocidad_internet.shtml
- S/a, *Electronic Soldier*, [en línea], Diccionary of War, Dirección URL: http://dictionaryofwar.org/node/638
- s/a, *Georgia declara estado de guerra y Rusia dice haber liberado Osetia del Sur*, [en línea], La Nación, 9 de agosto de 2008, Dirección URL: http://www.lanacion.com.ar/1038121-georgia-declara-el-estado-de-guerra-y-rusia-dice-haber-liberado-osetia-del-sur
- s/a, *H.R. 3523*, [en línea], House of Representatives, 30 de noviembre de 2011, Dirección URL: http://www.gpo.gov/fdsys/pkg/BILLS-112hr3523ih/pdf/BILLS-112hr3523ih.pdf
- S/a, *Medvédev a RT: "No hubo una guerra entre Rusia y Georgia, sino imposición de la paz",* [en línea], RT, 4 de agosto de 2013, Dirección URL: http://actualidad.rt.com/actualidad/view/102052-medvedev-rt-entrevista-georgia-rusia-guerra
- s/a, *ONU busca acuerdo para evitar 'ciberguerra'*, [en línea], El Economista, 30 de enero de 2010, Dirección URL: http://eleconomista.com.mx/tecnociencia/2010/01/30/onu-busca-acuerdo-evitar-ciberguerra
- s/a, *SS-21 "Scarab" (9K79 Tochka) SRBM*, [en línea], Harpoon Data Bases, Dirección URL: http://www.harpoondatabases.com/encyclopedia/entry2181.aspx,
- S/a, *Stuxnet hits Iran nuclear* plans, [en línea] , BBC, 22 de noviembre de 2010, Dirección URL: http://www.bbc.co.uk/news/technology-11809827

- S/a, *Stuxnet worm hits Iran nuclear plant staff* computers, [en línea] BBC, 26 de septiembre de 2010, Dirección URL: http://www.bbc.co.uk/news/world-middle-east-11414483
- s/a, *Temporary revival of Independence and reconquer of Georgia by Russia. (1918-1921)*, [en línea], Parlamento de Georgia, Dirección URL: http://www.parliament.ge/pages/archive_en/history/his11.html
- s/a, *Update: Georgian government websites under DDoS & Cyber Attack*, [en línea], The Jawa Report, Dirección URL: http://minx.cc:81/?post=193591
- S/a, *US-Israeli Stuxnet Cyber-Attacks against Iran: "Act of War",* [en línea], Center for Research on Globalization, 25 de marzo de 2013, Dirección URL: http://www.globalresearch.ca/us-israeli-stuxnet-cyber-attacks-against-iran-act-of-war/5328514
- Shackelford, Scott J. *From Nuclear War to Net War: analogizing Cyber Attacks in International Law,* [en línea], Estados Unidos, boalt.org, Dirección URL: http://www.boalt.org/bjil/docs/BJIL27.1_Shackelford.pdf.
- ShadowServer Foundation, Mission, [en línea], ShadowServer Foundation, Dirección URL: https://www.shadowserver.org/wiki/pmwiki.php/Shadowserver/Mission
- Swaine, Jon, *Georgia: Russia "conducting cyber war"*, [en línea], The Telegraph, 11 de agosto de 2008, Dirección URL: http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html
- United Nations News Centre, *Situation around Abkhazia and South Ossetia: Historical Overview*, [en línea], United Nations News Centre, Dirección URL: http://www.un.int/russia/new/MainRoot/docs/warfare/statement051208en.htm
- W. Johnson, Chris, *Anti-social networking: crowdsourcing and the cyberdefense of national critical infrastructures,* [en línea], University of Glasgow, Dirección URL: http://www.dcs.gla.ac.uk/~johnson/papers/Gudela/Cyberdefence_And_Anti_Social_Networking.pdf

- Walters, Simon *Hammond's £500m new cyber army: as he reveals top-secret Whitehall bunker for the first time, Defence Secretary says futura wars will be fought with viruses*, [en línea], The Mail Online, 28 de septiembre de 2013, Dirección URL: http://www.dailymail.co.uk/news/article-2436946/Hammonds-500m-new-cyber-army-As-reveals-secret-Whitehall-bunker-time-Defence-Secretary-says-future-wars-fought-viruses.html
- Zetter, Kim, *Legal experts: Stuxnet Attack on Iran was Illegal "Act of Force"*, [en línea], Wired, 25 de marzo de 2013, Dirección URL: http://www.wired.com/threatlevel/2013/03/stuxnet-act-of-force/