UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

ATAQUES CIBERNÉTICOS: UNA NUEVA FORMA DE HACER LA GUERRA.

T E S I S

QUE PARA OBTENER EL TÍTULO DE LICENCIADA EN RELACIONES INTERNACIONALES

PRESENTA:

EMILY YOSELIN RIVERA SÁNCHEZ

ASESORA: MTRA. ANA CRISTINA CASTILLO PETERSEN

CIUDAD UNIVERSITARIA, 2015

Agradecimientos

A mi segunda casa, a la Máxima Casa de Estudios, a la Universidad Nacional Autónoma de México. Por abrirme las puertas incluso antes de saber que pasaría la mitad de mi vida entre sus muros. Qué orgullo decir "Soy egresada de la UNAM."

Al hombre que me dio la vida, aquel ángel que ha velado día y noche por mí y por mi familia. A ti papá, Emilio Rivera Amaya, que me inculcaste los principales valores que han regido mi vida, que me enseñaste que la educación es uno de los principales pilares para salir adelante y ser mejor, y que el trabajo duro siempre es recompensado. Así como me lo dijiste la última vez que nos vimos "Estoy muy orgulloso de ti hijita", sé que ahora, desde el lugar en el que estás, lo sigues estando. Te amo papito, y aunque cada día de mi vida me has hecho falta, sé que de una u otra forma siempre estarás a mi lado.

A mi mamá, Julia Sánchez, quien con mucho esfuerzo y coraje ha sabido ser padre y madre en los últimos años. Reconozco el enorme esfuerzo que ha representado sacarme adelante y brindarme el mejor regalo que cualquier padre puede darle a su hijo: un futuro. Eres el mejor ejemplo de vida que tengo.

A mis hermanos, Alfredo, Ale, Gaby y Meche, quienes de muchas y muy diversas maneras han sido un gran ejemplo a seguir. Por siempre demostrarme su cariño, su apoyo incondicional y por defender siempre a su hermanita ante cualquier persona.

A mi otro hermanito, Rubén. ¡Lo logramos chefsito! No tuvimos que decir nada, simplemente "les demostramos" que con nuestro esfuerzo se puede llegar muy lejos.

A esa personita especial, que estuvo a mi lado desde el primer día que pisé la Facultad hasta este momento. Por estar a mi lado muchas de las noches que no dormía, no importaba si era de forma remota, siempre estaba ahí para decirme "No te duermas, ya casi terminas." Por brindarme su alegría cuando el estrés se presentaba en su mayor esplendor cada fin de semestre, por todo eso y más. Gracias. Emmanuel Razo.

A aquella amiga que compartió conmigo un largo y arduo trayecto durante cinco años, incontables noches en vela, innumerables trabajos y exámenes, comidas horrendas, pero también inolvidables momentos de alegría y diversión, Tania de la O. Gracias nena, por todo.

A mi asesora, por estar conmigo en el largo camino que representó esta investigación, por no desanimarme cuando comenzamos en Hollywood y terminamos en los conflictos bélicos. Por manejar las medidas exactas de presión y paciencia para que este trabajo se llevará a cabo. Muchas gracias Profesora.

A mis sinodales, Mtra. Cruz García Neydi, Dr. Hernández-Vela Salgado Edmundo, Dra. Rosas González Ma. Cristina y al Mtro. Valenzuela Shelley Miguel Ángel. Gracias por tomarse el tiempo de leer este trabajo y enriquecerlo con sus valiosos comentarios y observaciones.

Colegio de Ciencias y Humanidades Plantel Sur (2007-2010)

Facultad de Ciencias Políticas y Sociales (2010-2014)

Índice

Índice de figuras

Índice de mapas

Introducción

La guerra ha sido un elemento persistente a través de la historia, y a pesar de que en cada etapa se han presentado características nuevas en los enfrentamientos, sin duda alguna, la constante es que la guerra ha sido la responsable de las grandes transformaciones económicas, políticas, sociales y tecnológicas, que se han producido desde la antigüedad.

Aunque los objetivos bélicos han sido variados, el que ha permanecido estático por un largo período es el de salvaguardar la seguridad del Estado, pero las directrices seguidas han sufrido diversas modificaciones a lo largo de los años, las reglas del juego han sido reformadas una y otra vez; no obstante, estos cambios no habían sido tan colosales como lo han sido en los últimos años.

Inicialmente, los enfrentamientos eran realizados de manera física, es decir, se atacaba de manera directa al contrincante, por lo que en la mayoría de las veces se sabía a quién o quiénes se enfrentaban y el fin que se buscaba estaba bien definido, así como las estrategias y procedimientos utilizados, el campo de batalla era conocido a profundidad (tierra, agua, aire y, más tarde, espacio); sin embargo, a partir de la Segunda Guerra Mundial y posteriormente, la Guerra Fría, empezaron a desencadenarse una serie de cambios importantes en el campo militar.

No sólo fue la mejora de armas tecnológicas, más sofisticadas, poderosas y con una capacidad desmesurada de destrucción, sino que, a finales del siglo XX, comenzaron a desarrollarse otro tipo de conflictos, con nuevas estrategias, objetivos y sobre todo, actores. La figura del Estado comenzó a debilitarse, al tiempo que otros sujetos, tanto nacionales como internacionales, adquirían fuerza e importancia.

Dentro de este escenario de las nuevas guerras surgió la llamada Ciberguerra, un enfrentamiento virtual que consiste en atacar el sistema operativo de alguna computadora por medio de un virus, causando diversas secuelas, las cuales abarcan una amplia gama de efectos, desde robo de información hasta el colapso o destrucción de alguna estructura. Esto significó que la sociedad internacional se

enfrentara a un nuevo reto, debido a la aparición no sólo de características diferentes, sino también al resquebrajamiento del monopolio del poder.

Los ataques cibernéticos cambiaron todas las reglas del juego, se trata de un fenómeno poco estudiado, cuya arma principal se encuentra a disponibilidad de millones de personas asentadas alrededor del mundo: la Internet. Nadie habría imaginado que una herramienta creada durante la Guerra Fría, utilizada para salvaguardar documentos confidenciales del bloque capitalista, se convirtiera en un instrumento tan temido en un enfrentamiento bélico.

El mundo estaba acostumbrado a mirar la red digital con otros ojos, para la gran mayoría, se trataba únicamente de un artefacto inocente, utilizado como un utensilio básico, tanto para los negocios, como para uso personal. Se ha hecho hincapié en que no toda la población creía que sus capacidades se limitaban a dichas funciones, solo la mayor parte; esto es porque algunos militares e informáticos tuvieron una noción sobre sus habilidades desde el momento de su creación, si bien, no imaginaban hasta qué punto podía llegar su poder, sí tenían una idea general sobre ello.

A finales de la década de los años 90 y los primeros años del nuevo siglo, algunos actores internacionales comenzaron a realizar varias incursiones en el terreno virtual; sin embargo, no fue sino hasta el año 2007 cuando el nuevo campo de batalla empezó a ser estudiado con mayor profundidad. Esto fue porque, en esa fecha, se llevó a cabo el primer ataque cibernético conocido a nivel mundial, las agresiones al gobierno de Estonia a manos del Estado ruso.

A partir de ese momento, noticias de altercados digitales, realizados en varias partes del mundo, encabezaron las primeras páginas de los periódicos internacionales. Ya no se trata de algo ficticio, que únicamente se podía observar en las películas de ciencia ficción, o en los libros cuyos autores poseían una vasta imaginación; se trata de algo real, los Estados están siendo atacados por otras naciones por medio de computadoras, sin necesidad de que las tropas intervengan de manera física en su territorio para ejecutar dicha tarea.

La sociedad internacional ha comenzado a ser testigo de algunas de las capacidades de la Ciberguerra, como el robo de información confidencial y secretos industriales, sabotaje electrónico, espionaje, entre muchas otras actividades; sin embargo, aún es un campo inexplorado, todavía se desconocen muchas de sus vertientes.

La incertidumbre fue creciendo a medida que las naciones se percataban de que su supremacía tecnológica no las exentaba de ser una víctima, al contrario, su poderío las convertía en actores débiles y fáciles de agredir. El ejemplo más claro de ello es Estados Unidos de América, potencia militar, pero un blanco sumamente atractivo al ser el país con más artefactos conectados a Internet, su dependencia hacia las redes hace que se convierta en la región más vulnerable hacia este tipo de contienda.

Al ser un tema relativamente nuevo, la existencia de investigaciones es escasa; dentro de la Universidad Nacional Autónoma de México (UNAM) hay muy pocas tesis sobre la materia y, la mayoría de ellas, son abordadas desde disciplinas diferentes a las Ciencias Sociales, como Ciencias de la Computación e Ingeniería; por lo que este trabajo busca ser uno de los estudios que abarque el fenómeno de la Ciberguerra desde el punto de vista inter, multi y transdisciplinario de las Relaciones Internacionales, y de esa manera, tener un panorama más extenso sobre el escenario que se está viviendo hoy en día.

La hipótesis en la cual se basa esta investigación es que, la Ciberguerra representa una nueva forma de llevar a cabo un conflicto bélico entre los Estados, aún más peligrosa, sencilla y rápida de realizar que la guerra convencional, con secuelas de mayor alcance, debido precisamente a la gran dependencia que poseen actualmente las naciones hacia las Tecnologías de la información y comunicación.

El objetivo general que se pretende alcanzar es examinar los nuevos enfrentamientos cibernéticos, conocer los elementos que los caracterizan y con base en eso, señalar las razones por las cuales representa una amenaza tan grave para la seguridad de todos los países, al igual que indicar cuáles han sido las

principales acciones que se han realizado para contrarrestar sus posibles consecuencias.

De ese objetivo principal, se desglosan tres fines específicos; el primero de ellos, busca explicar en qué consiste la guerra convencional, cuáles son sus principales características, elementos y recursos que necesita para llevarse a cabo, y de esa forma, poder visualizar de manera más clara la transición que hubo hacia las nuevas guerras; el segundo, señalar el origen de la Ciberguerra, sus particularidades y principios, partiendo del origen y evolución de la Internet a través del tiempo, examinando quiénes fueron los primeros sujetos en incursionar en este tipo de conflictos y de qué manera lo hicieron, y por último; determinar las razones por las cuales Estados Unidos es considerado el actor internacional más vulnerable hacia los ataques, así como las acciones que ha ejecutado para mejorar ese panorama tan desolador.

Estos apartados se desarrollarán a lo largo de tres capítulos. El episodio inicial, está dedicado a abordar dos temas principales, en primer lugar, el origen y la evolución de los conflictos bélicos convencionales, sus principales características y objetivos, en segundo, el nacimiento de las nuevas guerras, tomando como punto de partida el conflicto de Bosnia-Herzegovina, ya que fue el primer conflicto que se diferenció de los otros por la utilización de elementos diferentes a las conocidas. Asimismo, se remarca la manera en que el monopolio del poder dejó de estar únicamente en manos del Estado.

En el segundo capítulo, se abordará el surgimiento de la Ciberguerra, partiendo de la Guerra Fría, momento histórico que dio origen a la Internet, por lo que se realizará un breve recuento del uso que se le ha dado, desde su nacimiento hasta el día de hoy, esto con el fin de que el lector pueda visualizar de una mejor manera el papel que ha representado en la escena internacional. De igual manera, se habla de los precursores en el uso de las redes como armas de guerra, así como de los principales objetivos que buscan alcanzar.

En el tercer, y último, capítulo, se analizará el caso específico de Estados Unidos, ya que al ser el país que posee la mayor cantidad de ordenadores conectados a Internet en todo el mundo, tanto personales como industriales, posee una vulnerabilidad mayor que la de cualquier otra entidad internacional, por lo que resulta más sencillo analizar las posibles consecuencias que un ataque cibernético representa, así como algunas medidas de seguridad que se han tomado en torno al problema. De igual manera, se abordará el caso emblemático del ex agente informático, Edward Snowden, ya que a partir de sus declaraciones, no sólo aumentaron los ataques hacia la potencia americana, sino también, el mundo comenzó a visualizar el peligro que la Ciberguerra representa.

1. Una atrocidad llamada guerra

Gran parte de la historia de la humanidad ha estado caracterizada indudablemente por la cantidad desmesurada de conflictos bélicos que se han suscitado en todos los rincones del mundo, a pesar de eso, es prácticamente imposible conocer cuál fue el primer enfrentamiento que ocurrió. Lo que queda claro es que "[…] la guerra es tan vieja como las civilizaciones, éstas han recompuesto su paisaje político y social, a tal grado que han constituido muchas veces el origen o término de innumerables culturas"[1].

No se sabe con exactitud cuál es el origen de la guerra; hay autores que se han remitido desde el período Neolítico y otros parten del siglo XV en Europa. A pesar del desconocimiento de dónde, cuándo y cómo fueron a la guerra por primera vez los seres humanos, varias investigaciones apuntan a que, hasta en los estadíos más primitivos, los grupos de nuestra especie en los que prevalecía la paz eran una rara excepción. Entre las causas que existían para que se desarrollara una lucha en las primeras sociedades prevalecían el territorio y los recursos, sin embargo, se pueden señalar otras diferentes[2].

Quincy Wright, politólogo estadounidense, distingue cuatro tipos de guerras en las sociedades arcaicas: Algunas luchaban sólo para defenderse, pero no parecían contemplar objetivos de orden político o económico, simplemente querían obtener venganza por una ofensa sufrida o exterminar a los hombres que no pertenecían al grupo; en otras ocasiones, luchaban por el simple gusto de la competencia o el deporte; una tercera categoría son las sociedades que realizaban estas actividades belicosas con el fin de adquirir tierras, mujeres o esclavos; y por último, es la que sostenían las clases militares para mantener su propio régimen o el imperio que habían edificado[3].

---

[1]Barthélémy Courmont, *La guerra: una introducción,* Madrid, Historia Alianza Editorial, 2010, p. 23.
[2]*Cfr.* David García Hernán, Ignacio Catalá Martínez, *Historia de la guerra*, España, Editorial Síntesis, s.a. p. 15.
[3]*Cfr.* Raymond Aron, *Paz y guerra entre las naciones*, vol. I y II, Madrid, Alianza Editorial, 1984, p. 423.

Por su parte, el antropólogo estadounidense, Marvin Harris, propone otra teoría sobre los orígenes de la guerra en las sociedades sin Estado y tribales. Su hipótesis se compone de cuatro suposiciones: la guerra como solidaridad; como juego; como naturaleza humana y como continuación de la política.

La primera, explica el concepto de guerra al servicio del desarrollo político, social y económico de las sociedades que competían unas contra otras; la segunda, hace referencia al deporte como sustituto del enfrentamiento, se sucede al combatiente tradicional por el campeón deportivo; la tercera teoría retoma la idea de estado natural que desarrolló el filósofo inglés Thomas Hobbes, según la cual los seres humanos tienen tendencia a vivir en conflicto de todos contra todos; la cuarta teoría de Harris toma los términos definidos por Karl von Clausewitz, los cuales expresan que nadie comienza una guerra sin estar seguro de los objetivos que se persiguen[4].

Si se observa el fenómeno estudiado desde el punto de vista psicológico, en realidad no existen muchas diferencias con lo que manifiestan Quincy Wright y Marvin Harris, ya que la Psicología hace referencia a la conducta del hombre como algo que se mueve por impulso, "[…] que le hacen entrar en competencia con sus semejantes y, de manera casi inevitable, en conflicto con alguno de ellos"[5]. Esto debido a la necesidad que existe de defender lo que aparentemente le pertenece a una persona o grupo de personas y que, al mismo tiempo, resguarda otra colectividad reclamando los mismos derechos.

Sobre todo, menciona a la agresión como una parte constante y aparentemente útil en la conducta cotidiana de muchos animales y no se hace destructiva ni nociva, salvo en circunstancias excepcionales[6]. Es decir, útil porque se hace uso de ello cuando cualquier animal o individuo se siente amenazado por otro, y de esa forma llega incluso a salvaguardar su existencia.

[4] *Cfr*. Barthélémy Courmont, La guerra: una introducción, *op. cit.,* pp. 13-16.
[5] Raymond Aron, Paz y guerra entre las naciones, *op. cit.,* p. 413.
[6] *Ibídem*. p. 410.

Desde el punto de vista social, las guerras "[…] son un fenómeno social específico, surgido probablemente en un determinado momento de la historia humana: implican la organización de la acción violenta por las colectividades enfrentadas. […] se observan conflictos en todas, o en casi todas, las colectividades humanas, y estos conflictos degeneran a veces en violencia […]"[7].

Como se ha visto, "[…] la guerra tiene raíces a la vez biológicas, psicológicas y sociales. Agresivo entre los primates, […] en constante competencia con sus semejantes, es física y moralmente combativo, y se muestra inclinado al resentimiento contra aquéllos […] que le privan del amor, de la gloria, del dinero"[8]. Pero es importante tener en cuenta que las características que se han dado pueden depender de cada una de las culturas en las que se presentó este fenómeno, ya que la guerra, no tenía el mismo significado para todas, mientras algunos no le daban mucha importancia, otras culturas, como Roma, llegaban incluso a divinizar lo bélico[9].

No obstante, existen otros puntos de vista, los cuales sostienen firmemente que las primeras manifestaciones bélicas que se llevaron a cabo en la antigüedad no pueden ser consideradas guerras como tal, debido a que no movilizaban ni todos los recursos humanos ni todos los materiales de un pueblo; eran dirigidas, por así decir, de un modo privado por príncipes o reyes que en absoluto implicaba un verdadero estado de guerra entre las comunidades[10].

Además, se argumenta que la primera condición para hacer la guerra es que una comunidad, tras haber satisfecho sus necesidades inmediatas, le quede una parte de energía vital para dedicársela; lo que supone, desde el punto de vista económico, que las fuerzas productoras estén lo suficientemente desarrolladas como para poseer un excedente de recursos, susceptible de ser invertido en

[7] *Ibídem*. p. 414.
[8] *Ibídem*. p. 427.
[9] *Cfr.* David García Hernán, Ignacio Catalá Martínez, Historia de la guerra, *op. cit.*, p. 41.
[10] *Cfr.* Yvon Garlan, *La guerra en la Antigüedad*, España, Alderabán, 2003, p. 18.

actividades sociales no productivas de un modo inmediato; la primera de ellas, la guerra[11]. Lo cierto es que, sí existió un excedente en la antigüedad:

> […] la aparición del fenómeno bélico está relacionada con el mayor grado de complejidad que empiezan a tener las sociedades humanas a partir de la consecución, gracias a las técnicas de irrigación en los cultivos, de unos excedentes en la producción agrícola. Se pudieron obtener así grandes recursos para la movilización de personas para la guerra y medios para llevarla a cabo […][12].

Es claro que las sociedades antiguas no desarrollaron enfrentamientos bélicos ni con los mismos elementos ni buscaron los mismos objetivos, sin embargo, ya se presentaban rasgos violentos desde esa época. Los objetivos por los cuales luchaban eran diversos, pero la herramienta para conseguirlos era la misma que se utiliza hoy en día.

> La guerra es de todos los tiempos históricos y de todas las civilizaciones. Con hachas o cañones, con flechas o con balas, con explosivos químicos o con reacciones atómicas en cadena; de lejos o de cerca, aisladamente o en masas, al azar o de acuerdo con un método riguroso, los hombres se han matado unos a otros, utilizando los instrumentos que la costumbre y el saber de las colectividades les ofrecían[13].

Lo que es importante puntualizar, es que las guerras han sido responsables de los cambios más importantes que ha vivido la humanidad a lo largo de su historia. El rumbo de las relaciones internacionales ha sido enormemente modificado en los últimos siglos debido a los conflictos bélicos, y es muy posible que en un futuro muy cercano se presenten nuevos cambios ocasionados por las nuevas formas de guerra que se están desarrollando.

---

[11] *Ibídem.* p. 176.

[12] David García Hernán, Ignacio Catalá Martínez, Historia de la guerra, *op. cit.,* p. 15.

[13] Aron Raymond, Paz y guerra entre las naciones, *op. cit.,* p. 197.

1.1 ¿Cuál es su definición?

Como se ha señalado, el fenómeno se puede estudiar desde diversos puntos de vista, es por eso que existen diferentes definiciones que se han desarrollado por varios autores a lo largo de la historia. Uno de ellos es Sun Tzu, estratega militar, filósofo de la antigua China y autor de la obra *El arte de la guerra*, en la cual define a la guerra como "[…] un asunto de importancia vital para el Estado, es la provincia de la vida y de la muerte, el camino que lleva a la supervivencia o a la aniquilación"[14].

Por otro lado, Karl von Clausewitz, general prusiano e historiador especializado en temas bélicos, menciona que la guerra "[…] no es del dominio ni de las artes ni de las ciencias, sino que es un elemento de la contextura social. Constituye un conflicto de grandes intereses solucionado de manera sangrienta, lo que la diferencia de todos los demás conflictos"[15]. Incluso se menciona que es mejor realizar una comparación con la política y el comercio, ya que la primera se trata de actividades e intereses humanos y la segunda porque se asimila a una especie de comercio a gran escala.

De acuerdo con el profesor emérito de la Universidad Nacional Autónoma de México, el Dr. Edmundo Hernández-Vela Salgado, la guerra se define como "Lucha armada con cierto grado de organización, sistematización y continuidad, entre colectividades humanas, por medio de la cual cada bando pretende imponer su voluntad al contrario. Sin embargo, la *guerra* no se libra únicamente en el ámbito externo de los países como un 'acto de violencia por el que los Estados ejecutan su política exterior' […]"[16].

Por su parte Mary Kaldor, economista inglesa, experta en Globalización, Relaciones Internacionales e intervención humanitaria, explica que se trata de un fenómeno que tomó forma en Europa entre los siglos XV y XVIII, íntimamente

[14] Sun Tzu, *El arte de la guerra*, México, Colofón, 2012, p. 7.
[15] Karl von Clausewitz, *De la guerra*, Barcelona, Labor Punto Omega, 1984. p. 17.
[16] Edmundo Hernández-Vela Salgado, *Diccionario de Política Internacional*, México, Porrúa, Tomo I, 2002, Sexta Edición, p. 540.

ligado a la evolución del Estado moderno y el cual ha atravesado diferentes etapas a lo largo de la historia: las guerras relativamente limitadas de los siglos XVII y XVIII; las guerras de tipo más revolucionario del siglo XIX; y las guerras totales de principios del siglo XX, caracterizada cada una de ellas por una modalidad bélica diversa, con distintos tipos de fuerzas militares, estrategias, técnicas, relaciones y medios de lucha[17].

Pero a pesar de estas disparidades entre ellas, todas comparten particularidades específicas, las cuales no sufrieron cambio alguno aún con el pasar de los años. Hay autores que hablan incluso de objetivos eternos, es decir, propósitos que han causado la realización de cada uno de los conflictos bélicos suscitados a lo largo de la historia y que seguirán estando presentes en futuros enfrentamientos.

1.2. Objetivos principales

Sin duda, tener en claro el objetivo que se persigue en la guerra es de gran importancia debido a que es considerado la pieza clave que decide cómo, cuándo y dónde se llevarán a cabo cada una de las acciones que se realizarán en torno a los conflictos bélicos.

Raymond Aron, sociólogo francés, manifiesta en su obra *Paz y guerra entre las naciones* que la finalidad primordial que se busca en la guerra es la seguridad, es decir, la aspiración a sobrevivir. “Gobernantes y gobernados están interesados y deseosos de mantener la colectividad que forman todos juntos, por la gracia de los siglos, de la raza o del azar”[18].

Antes de iniciar un enfrentamiento, todos los sujetos implicados se deben de preguntar cuáles son los objetivos por los cuales van a encararse, esta es la razón principal por la cual Clausewitz menciona que la guerra se convierte en una continuación de la política por otros medios, porque es la última opción cuando las

[17] *Cfr*. Mary Kaldor, *Las nuevas guerras. Violencia organizada en la era global*, Barcelona, Kriterios, TusQuets Editores, 2001, p. 29.
[18]Raymond Aron, Paz y guerra entre las naciones, *op. cit.*, p. 108.

demás no han sido lo suficientemente eficaces para alcanzar lo que se está buscando[19].

Haciendo referencia una vez más al estratega prusiano, se menciona otro objetivo: obligar al enemigo a hacer nuestra voluntad. Es importante tener en cuenta que al mencionar "enemigo" y "nuestra" se hace referencia únicamente a la figura e intereses del Estado[20]. De igual manera, se debe subrayar que varios autores, incluido Clausewitz, consideraban que la labor de hacer la guerra era una acción que debía ser realizada exclusivamente por los países y así, salvaguardar sus intereses.

Es importante marcar que estas concepciones comprenden una visión tradicional de la guerra. Las ideas de von Clausewitz parten principalmente de la Paz de Westfalia de 1648, la cual se caracteriza por marcar la construcción del Estado moderno, territorial, centralizado y jerárquicamente ordenado[21], por lo que sostiene que las contiendas habían sido libradas en la mayoría de los casos por Estados, a pesar de que aún existían conflictos realizados por diferentes actores como tribus bárbaras, señores feudales e incluso por la Iglesia. A partir del siglo XIX, la guerra fue considerada como una acción que solamente este actor podía llevar a cabo, pues era el único que poseía el monopolio del uso de la violencia organizada.

A partir de estas concepciones, se podría llegar a la conclusión que la guerra se lleva a cabo únicamente si existe una amenaza que ponga en peligro la seguridad del Estado, o bien sea usada como último recurso después de agotar cualquier otra opción. Lo cierto es que, en el trasfondo, pueden existir otras causas, como la aspiración de ser reconocidos, imponer su voluntad y alzarse como el vencedor indiscutible, lo que acarrearía la completa sumisión del enemigo[22].

---

[19]*Cfr.* Barthélémy Courmont, La guerra: una introducción, *op. cit.,* pp. 15-16.
[20]*Ibídem.* p. 31.
[21]*Cfr.* Luc Reydams, "Á la guerre comme á la guerre: tipos de conflictos armados, respuestas del derecho humanitario y nuevos desafíos", [en línea], *International Review of the Red Cross*, núm. 864, diciembre, 2006, Dirección URL: http://www.icrc.org/spa/assets/files/other/irrc_864_reydams.pdf, [consulta: 25 de septiembre de 2013].
[22]*Cfr.* Aron Raymond, Paz y guerra entre las naciones, *op. cit.,* p. 110.

Hay que tener en cuenta que "[…] los objetivos concretos que se fijan las unidades políticas no evolucionan solamente de acuerdo con las técnicas de combate y de producción, sino que evolucionan también con las ideas históricas que presiden la organización y el gobierno de las colectividades"[23]. Es decir, el fin principal que se menciona puede ser para salvaguardar la seguridad del Estado, pero en el trasfondo, las intenciones que busca cada ente van cambiando de acuerdo con el contexto internacional, que a su vez, implica una transformación al interior de cada una de ellas.

Sin embargo, a pesar de todos los cambios que se han presentado en la escena internacional en las últimas décadas, existen objetivos eternos que, de acuerdo con Raymond Aron, estarán siempre presentes en el momento de efectuar un enfrentamiento bélico. Dos de ellos ya han sido mencionados anteriormente: la seguridad y la supervivencia, no obstante, nombra otro que es el territorio.

El sociólogo francés afirma que en la rivalidad de los pueblos, la posesión del espacio es el objetivo original, pero este elemento no puede estar separado de otros dos que son los hombres y las almas. "¿Para qué han de combatir las sociedades, si no es para ensanchar la tierra que cultivan y cuyas riquezas explotan, para someter a los hombres […] o para asegurar el triunfo de determinada idea, religiosa o social […]?"[24] De acuerdo con Raymond Aron, es muy difícil que estos tres elementos se separen en casos concretos.

Hoy en día, esto se puede ver reflejado en las confrontaciones que se están llevando a cabo alrededor del mundo, sobre todo en aquellos países que son considerados menos adelantados. Existen muchas razones por las cuales acontecen estas guerras, pero los factores de territorio y pertenencia están presentes en la mayoría de ellas. Son los recursos naturales que poseen pocos Estados la razón principal por la cual son arremetidos por actores ajenos a ellos, muchas veces por las grandes potencias.

[23] *Ibídem.* p. 119.
[24] *Ibídem.* p. 111.

La importancia que posee cada uno de los fines proclamados para llevar a cabo el enfrentamiento es que "[…] emprender una guerra no es más que el principio; lo que importa, a la hora de sostenerla, es en qué medida los que participan en ella consideran que el objetivo del conflicto es legítimo"[25]. Si no existe un fin en común, aquellos que están en medio del campo de batalla bien pueden desistir de seguir luchando y poner en peligro los intereses que hay de por medio.

Por otra parte, la finalidad de la guerra no constituye la última palabra del análisis; es probable que los pueblos no luchen por las razones que manifestaron en un inicio, sino que las intenciones auténticas se encuentren perdidas en el fondo del inconsciente colectivo y tal vez los Estados soberanos estén condenados a combatirse porque tienen miedo unos de otros[26], miedo tal vez de perder su lugar en la escena internacional por alguien más que está emergiendo a una velocidad sorprendente y que se está imponiendo tanto económica como militarmente en el mundo.

1.3. Evolución y tipología de la guerra

Clasificar cada uno de los enfrentamientos bélicos es una tarea muy ardua, debido no sólo a las características que cada uno de ellos posee, sino también al tiempo histórico en el que se llevan a cabo. Asimismo, cada autor sugiere una clasificación diversa de acuerdo con los elementos que considera más transcendentales para realizarla, hay quienes toman en cuenta el periodo de tiempo, recursos utilizados, actores involucrados, objetivos, etc.

Incluso Raymond Aron señala que "[…] se podría considerar como irrisoria una 'tipología formal' de las guerras y de las paces […]"[27]. Esto es porque no sólo los conflictos armados han presentado importantes modificaciones a través de la historia, sino también la definición de guerra ha estado caracterizada por no ser un elemento inmutable y estático.

---

[25] *Ibídem.* p. 45.
[26] *Ibídem.* pp. 125-126.
[27] *Ibídem.* p. 197.

A través del tiempo, los conflictos bélicos han ido evolucionando debido a varios factores específicos que han estado presentes en cada uno de los momentos históricos en los que se han desarrollado. Como ya se ha mencionado, Mary Kaldor manifiesta que la guerra tomó forma en Europa entre los siglos XV y XVIII, aunque desde ese entonces ha pasado por profundas transformaciones. El siguiente cuadro muestra la manera en que ella explica la evolución de las viejas guerras o guerras tradicionales.

Figura 1

Características de las viejas guerras a través del tiempo

	Siglos XVII y XVIII	**Siglo XIX**	**Principios del siglo XX**	**Finales del siglo XX**
Tipo de gobierno	Estado absolutista	Nación Estado	Coaliciones de Estados; Estados multinacionales; imperios	Bloques políticos
Objetivos de la guerra	Razones de Estado; conflicto dinástico; consolidación de fronteras; religión	Conflicto nacional	Conflicto Nacional e ideológico	Conflicto ideológico
Tipo de ejército	Mercenarios/ profesionales	Profesionales/ servicio obligatorio	Ejército de masas	Elite científico-militar/ ejército profesionales, tácticas
Técnica militar	Uso de armas de fuego, maniobras defensivas, asedios	Ferrocarril y telégrafo, movilización rápida	Potencia de fuego a gran escala; tanques y aviones	Armas nucleares
Economía de guerra	Regularización de los impuestos y préstamos	Expansión de la administración y la burocracia	Economía de movilización	Complejo militar-industrial

Fuente: Elaboración propia con datos de Mary Kaldor, *Las nuevas guerras. Violencia organizada en la era global*, Barcelona, Kriterios, TusQuets Editores, 2001, p. 29.

Como se puede observar, cada una de las fases se caracterizó por un modo de conflicto bélico diferente, con distintos objetivos, ejércitos, tácticas y economías diversas. Al igual que Mary Kaldor, Federico Aznar, politólogo y sociólogo español, realiza su propia tipología conformada por cuatro generaciones, la cual será utilizada como base para esta investigación, ya que dicha distribución parte desde la aplicación de la tecnología, la modificación de los procedimientos y un cambio generacional.

1.3.1. Primera Generación

Federico Aznar considera que el punto de partida que posee la Primera Generación de los conflictos bélicos es el Renacimiento, movimiento cultural surgido en Europa y que comprende los siglos XV y XVI. Este periodo de tiempo estuvo caracterizado no sólo por el renovado interés en el arte grecorromano clásico[28], sino también por las guerras religiosas que se llevaron a cabo, provocando el estallido de la Guerra de los Treinta Años cuyo desenlace se logró con la firma de la Paz de Westfalia en 1648.

Este hecho histórico es considerado no sólo como la fecha exacta en que comienzan las guerras de Primera Generación, sino también el momento en el que el Estado se hace con el monopolio de la guerra. Con anterioridad, todo tipo de entes tales como familias, tribus y ciudades, habían sido libres de llevar a cabo un enfrentamiento[29]; tras el tratado de Westfalia, únicamente los Estados tenían el derecho de ejercer el uso legítimo de la fuerza.

En esta primera clasificación cambiaron las dimensiones físicas de la guerra, el tamaño de los Ejércitos y la complejidad de las operaciones militares aumentaron. La relevancia se encuentra en que su principal elemento era el intento de establecer un orden, entendiéndolo desde el precepto militar como el uso

[28] *Cfr*. s/a, "El Renacimiento", [en línea], 44 pp., Dirección URL: http://www.educacion.gob.es/exterior/centros/severoochoa/es/departamentos/historia/material_julia/Arte_renacimiento_2_ESO.pdf, [consulta: 1 de noviembre de 2013].

[29] *Cfr*. William S. Lind, "Comprendiendo la Guerra de Cuarta Generación", [en línea], Dirección URL: http://usacac.leavenworth.army.mil/CAC/milreview/download/Spanish/JanFeb05/lind.pdf, [consulta: 1 de noviembre de 2013].

generalizado de uniformes, normas disciplinarias, ordenanzas, etc., con el fin de destruir o expulsar al enemigo de una zona en particular[30].

Durante esta época, la guerra era considerada como limitada debido a los objetivos que perseguía, los cuales eran principalmente económicos y dinásticos[31]. De igual manera surgieron varios reglamentos y ordenanzas, uno de ellos fue el Código de Lieber, redactado durante la Guerra Civil estadounidense, considerado como el primer intento en codificar las leyes de la guerra; a pesar de que era vinculante únicamente para las fuerzas armadas de Estados Unidos, sirvió de base al Proyecto de Convenio Internacional sobre las leyes de la guerra presentado en 1874 a la Conferencia de Bruselas, que a su vez dio lugar a los Convenios de la Haya de 1899 y 1907 sobre la guerra terrestre[32].

Es así como se produjeron avances no sólo tecnológicos, sino también progresos en la forma de conducir la guerra. Es en el período de la Ilustración, también conocido como el Siglo de las Luces, cuando comenzaron a aparecer los primeros signos de transformación en la forma de llevar a cabo la guerra, pero fue hasta mediados del siglo XIX cuando se comenzaron a presentar cambios más visibles en el campo de batalla.

1.3.2. Segunda Generación

Durante la época del Romanticismo, desarrollado en la primera mitad del siglo XIX, se empezaron a generar grandes modificaciones; el orden de la Primera Generación se vio fraccionado por la introducción de la guerra de masas, hubo un incremento importante en las tropas que pasaron de las decenas de miles de hombres a los centenares de miles de hombres en un tiempo relativamente corto.

---

[30] *Cfr*. Federico Aznar Fernández-Montesinos, *Entender la guerra en el siglo XXI*, España, Editorial Complutense, 2011, pp. 123-124.

[31] *Ibídem*. p. 125.

[32] *Cfr*. Luc Reydams, Á la guerre comme á la guerre: tipos de conflictos armados, respuestas del derecho humanitario y nuevos desafíos, [en línea], *op. cit.*, pp. 7-8.

Además, los soldados que antes eran campesinos dirigidos por nobles, pasaron a estar integrados por obreros liderados por técnicos[33].

En esta guerra de masas se presentó un gran desarrollo económico e industrial: apareció la siderurgia, el mundo de las comunicaciones estuvo caracterizado principalmente por la invención del ferrocarril y el telégrafo[34], y sobre todo, la aparición de nuevas armas de fuego, más rápidas y de mayor alcance que las de la Primera Generación. Fue precisamente el fuego uno de los elementos predominantes de esta tipología, cuya finalidad era disminuir la capacidad del enemigo.

Aparecieron en escena dos formas de llevar a cabo los conflictos bélicos: la guerra de desgaste y la guerra de maniobra. La primera de ellas se le atribuye a Ulysses S. Grant, militar y ex presidente de los Estados Unidos, quien luchó durante la Guerra Civil estadounidense[35]. Según Grant, en este tipo de enfrentamiento los recursos poseen un papel de suma importancia, la clave está en saberlos utilizar y movilizar en el momento oportuno, de esa manera se puede vencer al oponente, aniquilando su fuerza y su voluntad.

Por su parte, Barthélémy Courmont, especialista en Relaciones Internacionales, Ciencia Política y Asuntos Nucleares, define la misma maniobra como una manera muy matemática de hacer la guerra debido a que toda acción estaba calculada, desde el número de unidades, hasta el momento adecuado para efectuar un ataque sorpresa; mientras que Clausewitz, consideraba que este tipo de enfrentamiento era exclusivo de los Estados, si algún otro actor llevaba a cabo algún conflicto bélico, éste no encajaba en esa categoría[36].

En lo que respecta a la guerra de maniobras, ésta es definida por Courmont como la utilización de las fortalezas contra las debilidades del adversario para

[33]*Cfr*. Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit.* p. 132.
[34] *Ibídem.* p. 134.
[35]*Cfr*. The White House. Washington, *Ulysses S. Grant,* [en línea], Estados Unidos, Dirección URL: http://www.whitehouse.gov/about/presidents/ulyssessgrant, [consulta: 2 de noviembre de 2013].
[36]*Cfr*. Barthélémy Courmont, La guerra: una introducción, *op. cit.*, pp. 19-22.

emplearlas en el momento oportuno, por lo que el resultado se calcula de acuerdo con el número de soldados capturados; la clave es la astucia, ya que brinda la posibilidad de conseguir una ventaja considerable con respecto al oponente[37]. Asimismo, Federico Aznar hace énfasis en que en la guerra de maniobra gana el ejército más brillante. Como se puede observar, mientras en una categoría se hace hincapié en los recursos, en la otra se le da más importancia al ingenio militar.

Es importante recalcar el papel que tuvo la tecnología durante este periodo que comprende la Segunda Generación. Uno de los mayores exponentes en este tema fue Helmuth von Moltke, general prusiano, quien descubrió los efectos positivos que poseía la tecnología en la guerra, especialmente el ferrocarril y el telégrafo, ya que permitían a las tropas una movilización y comunicación mucho más rápida.

El modelo que utilizan la mayoría de los autores para ejemplificar esta categoría es la Primera Guerra Mundial, ya que durante esta contienda, los objetivos se plantearon en torno a factores económicos y territoriales[38]. Este conflicto se convirtió en guerra total, la cual, en palabras de Raymond Aron, es definida como "[…] aquella en la que la cifra total de combatientes tiende a coincidir con la cifra total de población en edad de luchar y en la que cualquier actividad social puede ser reconvertida para su uso en la guerra"[39].

Además, las economías nacionales se transformaron en economías de guerra[40], es decir, todas las actividades de los Estados se realizaban alrededor del conflicto bélico que se estaba desarrollando en esos momentos, con el objetivo de que cada sector de la sociedad contribuyera, de algún modo, a conseguir aquello que se estaba buscando; incluso la cultura se transformó en propaganda bélica. Estas

[37] *Ídem.*

[38] *Cfr*. Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit.*, p. 132.

[39] Jorge Verstrynge, *La guerra periférica y el Islam revolucionario* citado en Federico Aznar Fernández-Montesinos, *Entender la guerra en el siglo XXI,* España, Editorial Complutense, 2011, p. 140.

[40] *Cfr*. Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit.*, p. 141.

características prevalecieron hasta la Segunda Guerra Mundial, momento en el cual comenzaron a presentarse algunos retrocesos en la forma de efectuar un conflicto.

1.3.3. Tercera Generación

El lapso de tiempo que comprende la Tercera Generación es desde el final de la Segunda Guerra Mundial hasta principios de la década de los noventas, momento en el que estalló la guerra de Bosnia-Herzegovina, conflicto en el que se presentaron por primera vez aspectos que, hasta ese momento, eran desconocidos y con los cuales los actores internacionales no estaban familiarizados.

Durante estos años, la tecnología tomó un lugar sustancial en la evolución de los enfrentamientos, se fue produciendo un cambio en los modos de producción, lo que causó la aparición de una economía basada primordialmente en el conocimiento, dejando en segundo lugar a las materias primas, el esfuerzo físico y el desarrollo industrial[41]. Esto se vio reflejado no sólo en el rápido desarrollo que tuvieron varios países, sino también en el enorme avance científico que hubo durante esa época.

Esta transformación en la manera de desarrollar la guerra es denominada por algunos autores, entre ellos el escritor Alvin Toffler, como guerras de tercera ola, también llamadas guerras de ordenador[42], las cuales eran llevadas a cabo por tropas altamente especializadas en nuevos campos de batalla, más amplios y más diversificados que los de la Segunda Generación.

Hay un retroceso en cuanto a los objetivos, presentándose de nuevo una guerra limitada en fines, es decir, las intenciones que movían a los Ejércitos para actuar ya no era un desacuerdo explícito entre dos sociedades con intenciones diversas,

[41] *Ibídem.* p. 144.
[42] *Ídem.*

sino que las verdaderas intenciones que estaban detrás de aquello eran los intereses personales de cada uno de los actores inmiscuidos en el conflicto.

Además de la tecnología, otro elemento importante de la Tercera Generación es el movimiento, su finalidad es establecer contacto estrecho con el enemigo y situarse en condiciones ventajosas respecto a él, las operaciones a la hora de aplicar la fuerza deben de ser decisivas y abrumadoras[43] con el objetivo de vencerlo rápidamente y así evitar una prolongación innecesaria que traerá consigo pérdidas económicas y humanas superfluas.

Como se ha visto, estas tres Generaciones poseen características que las diferencian unas de otras, sin embargo, cada una de ellas pertenecen a las llamadas viejas guerras, es decir, a los conflictos que tenían como principales actores o agentes de la violencia a los Estados y a los ejércitos, sus métodos de guerra pasaban por la captura de territorio a través de medios militares y las batallas constituían encuentros decisivos[44], además de estar ligadas a la emergencia de consolidar el Estado, y así monopolizar el uso de la violencia organizada, logrando establecer profesionales a sus órdenes[45].

Las características de estos enfrentamientos se mantuvieron vigentes desde la firma de la Paz de Westfalia hasta el término de la Segunda Guerra Mundial e inicios de la llamada Guerra Fría, suceso que se caracteriza por haber sido el escenario del nacimiento de nuevos tipos de conflicto, disputas que poseían características que ya no pertenecían a los elementos que se habían establecido con anterioridad, actores, conductas e intereses que no encajaban en las anteriores definiciones

---

[43] *Ídem.*

[44]*Cfr.* José Manuel Pureza, Tatiana Moura, "Viejas, nuevas y novísimas guerras: la conflictividad desafía la modernidad", [en línea], 23 pp., Dirección URL: https://estudogeral.sib.uc.pt/bitstream/10316/13281/1/Viejas,%20nuevas%20y%20nov%C3%ADsimas%20guerras.pdf, [consulta: 25 de septiembre de 2013], p. 4.

[45]*Cfr.* Mary Kaldor, "Un nuevo enfoque sobre las guerras", [en línea], *Papeles*, núm. 94, 2006, Dirección URL: http://www.fcp.uncu.edu.ar/upload/nuevoenfoqueguerrasmarykaldor.pdf, [consulta: 26 de octubre de 2013].

Se habla de muchos escenarios, pero la mayoría de los autores coinciden en que la guerra de Bosnia-Herzegovina fue la conflagración que marcó la pauta para comenzar a hablar de un nuevo paradigma con el surgimiento de estas nuevas hostilidades.

1.4. Las nuevas guerras.

A partir del fin de la Guerra Fría, el debilitamiento de la figura del Estado comenzó a hacerse presente debido al surgimiento de algunos enfrentamientos que tomaban lugar en varias partes del mundo, conflictos que poseían características que no se habían vislumbrado antes y por lo tanto no se ajustaban a la concepción que se poseía en ese momento sobre la guerra. Es por eso que a estas contiendas no se les tomó en serio, se les vio como periféricas, marginales, conflictos de baja intensidad[46].

Federico Aznar habla de una desinstitucionalización de hostilidades, menciona que dentro de las sociedades donde comenzaron a aparecer este tipo de fenómenos, se enfrentaba una desestabilización debido a la presión que recibían del bloque capitalista o socialista durante los años de la Guerra Fría[47], así que una vez que dio fin este período de la historia, el Estado, acostumbrado a esa situación, vio debilitado su poder en gran medida y el monopolio de la fuerza comenzó a tambalearse.

El nacimiento de estos nuevos enfrentamientos significó que el uso de la fuerza ya no era más un elemento exclusivo del Estado, había otros sujetos ajenos que podían hacer uso de ella para conseguir sus propios intereses, éstos se caracterizaban por ser librados por actores estatales y no estatales, a menudo sin uniformes quienes, de acuerdo con Mark Duffield, Profesor de Desarrollo, Democratización y Conflicto, actuaban más allá de sus competencias otorgadas.

Estas nuevas guerras difieren en muchos aspectos con los conflictos tradicionales, en elementos tales como actores, procedimiento utilizado para

[46] *Ibídem.* p. 8.
[47] *Cfr.* Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit.*, p. 151.

llevarlas a cabo, propósitos, modo de financiación y tecnología. Aunque es importante tener siempre presente que dentro de esta misma categoría existen desavenencias en cada uno de esos elementos, principalmente en el plano de la tecnología, todo depende del autor que aborde los temas.

1.4.1. Nuevos actores

La aparición de nuevos actores siempre ha sido inminente en los grandes cambios que ha sufrido la humanidad, y la manifestación de recientes cambios en los conflictos no ha sido la excepción. La mayoría de los autores manifiestan que lo más significativo de esta modificación en las nuevas guerras es que la figura del Estado ha sido relegada por nuevos sujetos nacionales e internacionales.

Una de las características es que los principales protagonistas involucran una gran diversidad de grupos, la variedad de tipos de actores es muy grande, comprendiendo desde instituciones, grupos estatales, sectores privados, e incluso la sociedad civil dotados de habilidades coactivas,[48] todos ellos conduciéndose sin uniformes, es decir, sin ser un ente oficial que tenga el derecho de usar de manera legítima la violencia.

El enemigo es ahora transfronterizo, difuso y difuminado, se puede tratar de un grupo reunido en torno a las órdenes de un líder y encontrarse camuflado entre la población de otro Estado[49]. Sin embargo, varios autores remarcan que la figura del soldado aún está vigente dentro de estos nuevos enfrentamientos, tal vez no se encuentra tan marcado como Clausewitz señalaba al mencionar que el instrumento más eficiente que poseía el Estado para efectuar una conflagración era la figura del Ejército, pero aún sigue detentando un papel significativo.

A pesar de que la figura del soldado tal y como se ha conocido hasta ahora está aún presente en las nuevas guerras, sólo un pequeño porcentaje de estas hostilidades serán libradas por ellos y, en su mayor parte, ya no estarán

[48] *Cfr.* José Manuel Pureza, Tatiana Moura, "Viejas, nuevas y novísimas guerras: la conflictividad desafía la modernidad", [en línea], *op. cit.*, p. 12.
[49] *Cfr.* Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit.*, p. 181.

impulsados por propósitos militares[50], sino por intereses particulares de ciertos grupos o individuos, la mayoría de ellos implicados con aspectos puramente económicos. Se multiplican además las formas de conseguir esas intenciones, lo que refleja la variedad de identidades, motivaciones, intereses y niveles de actividad de los actores armados[51].

Por otro lado, Mary Kaldor enfatiza que a pesar del rezago de la figura del soldado, ésta siempre tendrá una gran importancia en las sociedades porque es precisamente la fuerza militar la que tiene la tarea de proteger a las personas y asegurar el cumplimiento de la ley, aunque también es cierto que se tienen que contemplar nuevos usos defensivos de la fuerza enfocados hacia la prevención, la protección y la estabilización, y no en la consecución de la victoria[52].

1.4.2. Tecnología. ¿Decisiva?

La tecnología aplicada en el ámbito militar ha estado presente desde los primeros enfrentamientos de la humanidad, sin embargo, fue a partir de la Primera y Segunda Guerras Mundiales cuando tuvo un mayor desarrollo y se comenzó a emplear con más ahínco con la creación de armas de destrucción masiva, es por eso que la posesión de estos elementos eran los que normalmente marcaban la diferencia entre el ganador y el perdedor; no obstante, este principio ha sufrido una importante modificación en las nuevas guerras.

Dentro de este nuevo fenómeno, la disponibilidad de más recursos materiales y un mayor desarrollo tecnológico siguen siendo factores importantes en el desarrollo de los conflictos, sin embargo, no deciden de manera automática quién obtendrá la victoria. La mayoría de los nuevos actores que están inmersos en las batallas se caracterizan por utilizar armas pequeñas y livianas, debido no sólo a

[50]*Cfr*. Herfried Münkler, "Las guerras del siglo XXI", [en línea], Madrid, *Revista Internacional de la Cruz Roja*, núm. 849, Dirección URL: http://www.yumpu.com/es/document/view/6736670/herfried-munkler-las-guerras-del-siglo-xxi-publicado-en-revista-, [consulta: 25 de septiembre de 2013].
[51]*Cfr*. Federico Aznar Fernández-Montesinos, Entender la guerra e el siglo XXI, *op. cit.,* p. 153.
[52]*Cfr*. Mary Kaldor, "Un nuevo enfoque sobre las guerras", [en línea], *op. cit*.

la facilidad de transportarlas, sino también porque pueden ser utilizadas por soldados que no recibieron una formación militar previa[53].

Incluso, varios autores mencionan que lejos de constituir una ventaja sobre el enemigo, la tecnología termina por representar todo lo contrario frente a los demás adversarios; esta vez son los países más adelantados quienes representan una mayor desventaja en comparación con las naciones que no poseen adelantos tecnológicos tan imponentes como ellos, debido precisamente a la dependencia tan marcada que poseen en todos los ámbitos de su vida.

[53]*Cfr*. Herfried Münkler, "Las guerras del siglo XXI", [en línea], *op. cit*.

Mapa 1
Las luces del mundo

Fuente: The National Aeronautics and Space Administration, *Visible Earth*, "Earth's city lights", [en línea], 2000, Dirección URL: http://visibleearth.nasa.gov/view.php?id=55167, .[consulta: 27 de noviembre de 2013].

Esta imagen tomada del sitio de la Administración Nacional de la Aeronáutica y del Espacio (NASA, *The National Aeronautics and Space Administration*), muestra al planeta entero de noche, iluminado únicamente por las redes eléctricas que cada país posee. En ella se puede observar, de manera muy clara, cuáles son las zonas geográficas que sobresalen más en el mapa, así como aquellas que permanecen en completa obscuridad.

Los países que se encuentran totalmente iluminados son los que cuentan con un mayor número de adelantos tecnológicos, con alto grado de complejidad y diversidad; en cambio, la mayoría de las naciones que se encuentran en la penumbra o que están alumbrados por apenas unas cuantas luces, son actores que al contar con un servicio eléctrico limitado, es difícil que posean la capacidad o los recursos necesarios para poseer herramientas más avanzadas que los otros. Sin embargo, es importante prestarles atención a estos últimos, ya que su aparente desventaja, les confiere la habilidad de ser inmunes a ser atacados utilizando su propia infraestructura en su contra.

En efecto, es el avanzado nivel de desarrollo socioeconómico de los países desarrollados el principal elemento que los convierte en blancos más vulnerables, y por mayor que sea su superioridad militar es un hecho difícil de cambiar; los enemigos que ahora poseen estas grandes naciones constituyen una seria amenaza por muy pequeñas y débiles que sean porque poseen algunas armas que los demás también, o bien, las están desarrollando[54].

Desde el atentado del 11 de septiembre de 2001, se tomó conciencia acerca de que un arma, aparentemente no inocente, representa un gran peligro para los demás si se utiliza bien[55]. No importa si se trata de un instrumento supuestamente indefenso que incluso se utiliza en la vida cotidiana, como la computadora o la Internet, en las manos correctas puede significar un artículo peligroso para cualquiera.

[54] *Ídem.*
[55] *Ídem.*

El desarrollo que poseen los países industrializados, así como sus adelantos tecnológicos aplicados en todos los ámbitos de su vida pueden ser utilizados en su contra. Sin embargo, no tienen más remedio que seguir innovando en sus aparatos militares si desean preservar su capacidad de respuesta militar[56]. De no ser así, se encontrarían aún más a expensas de cualquier otro actor que decida realizar algún acto en contra de ellos.

Federico Aznar manifiesta que esta vulnerabilidad de los países más adelantados ha ido en crecimiento con el pasar de los años; cuanto más ha aumentado su supremacía tecnológica, más probabilidades se le ha conferido al actor más débil. En el siguiente cuadro se expresa con mayor claridad esto; desde principios del siglo XIX, período que coincide con la Primera Revolución Industrial, comienza una reducción en la ventaja que tenían los países desarrollados, es así como a mediados y finales del siglo XX, período que constituye la era de la Guerra Fría, esta ventaja ya no está presente, las posibilidades de ambos actores ante un enfrentamiento se van nivelando.

Figura 2

Victorias del Estado fuerte y del Estado débil

Período	**1800-1849**	**1850-1899**	**1900-1949**	**1950-1999**
Victoria fuerte	88,2%	79,5%	65,1%	48,8%
Victoria débil	11,8%	20,5%	34,9%	51,2%

Fuente: Ivan Arreguin-Toft, *How the weak in wars. A theory of asimmetric conflict,* citado en Federico Aznar Fernández-Montesinos, *Entender la guerra en el siglo XXI*, España, Editorial Complutense, 2011, p. 171.

[56] *Ídem.*

1.4.3. Nuevos objetivos y zona de conflicto

Como se manifestó anteriormente, existen propósitos que se han mantenido estáticos desde el surgimiento de las primeras guerras, el principal ha sido claramente sobrevivir, sin embargo, hay otros fines que han presentado grandes modificaciones con el pasar de los años. El surgimiento de las nuevas guerras marcó un nuevo paradigma en lo que se refiere a los objetivos, porque al ser otros los actores que llevaban a cabo los enfrentamientos, evidentemente sus intereses comenzaron a ser muy diferentes de aquellos que eran buscados con anterioridad por el Estado.

En las guerras tradicionales, el conflicto se llevaba a cabo en torno a intereses sobre todo territoriales, siempre con el objetivo de seguir manteniendo la posesión del monopolio del uso de la fuerza. En las nuevas guerras esos factores ya no son parte de los intereses de los actores implicados en la contienda, ahora los enfrentamientos se basan principalmente en alcanzar fines ideológicos y políticos[57].

Ahora, la mayoría de los objetivos militares están siendo sustituidos por fines civiles, los cuales son movidos por intereses personales o de un pequeño grupo, por ejemplo líderes de milicias y jefes militares. Esa es una de las razones por las cuales los medios empleados para realizar los enfrentamientos han sufrido un cambio tan grande que cada vez poseen menos carácter genuinamente militar[58]. Es decir, los actores no responden ante ninguna clase de reglamento que regule sus actividades, no existe como tal un documento o algo similar que indique el término de las hostilidades, por lo que resulta difícil definir la línea que separa a la paz de la guerra.

---

[57]*Cfr*. Teofilo Vásquez. "Las nuevas guerras y el conflicto armado en Colombia", [en línea], Colombia, *Controversia*, núm. 190, junio 2008, Dirección URL: http://biblioteca.clacso.edu.ar/Colombia/cinep/20100926025844/lasnuevasguerras.pdf, [consultado: 26 de octubre de 2013].

[58]*Cfr*. Herfried Münkler, "Las guerras del siglo XXI", [en línea], *op. cit*.

Otro elemento importante que ha sufrido grandes modificaciones en los últimos años es el espacio donde se realizan estas acciones bélicas. En las guerras tradicionales se tenía claro el espacio en el que eran llevadas a cabo, el cual normalmente se trataba de un territorio definido dentro de un Estado, sin embargo, en estas nuevas contiendas ya no se tiene tan delimitado este factor tan importante.

Hoy en día, se tratan de conflictos que, debido a sus características, han desdibujado las líneas fronterizas, es decir, ya no se sabe con exactitud dónde comienzan las zonas de combate y las zonas de paz, las cuales siempre se habían mantenido rígidas y bien delimitadas en épocas anteriores[59].

"[A]sí como es difícil distinguir entre lo político y lo económico, lo público y lo privado, lo militar y lo civil, [es] también cada vez más difícil distinguir entre la guerra y la paz"[60]. Debido a eso, se ha comenzado a buscar espacios alternativos donde realizar las nuevas guerras, lugares en los que se pueda contar con una superioridad y que representen mayores posibilidades de éxito para algunos y por lo tanto grandes debilidades para otros[61].

Por supuesto, la búsqueda de sitios alternos no se reduce únicamente a lugares "tangibles", es decir, escenarios terrestres, aéreos, marítimos o espaciales. También se tiene que incluir áreas en las que ni siquiera se había pensado en un inicio como posible escenario, por ejemplo, el Ciberespacio, el cual se abordará con mayor detalle posteriormente.

[59]*Cfr.* José Manuel Pureza, Tatiana Moura, "Viejas, nuevas y novísimas guerras: la conflictividad desafía la modernidad", [en línea], *op. cit.,* p. 4.

[60]*Mary Kaldor* citada en José Manuel Pureza, Tatiana Moura, "Viejas, nuevas y novísimas guerras: la conflictividad desafía la modernidad", [en línea], 23 pp., Dirección URL: https://estudogeral.sib.uc.pt/bitstream/10316/13281/1/Viejas,%20nuevas%20y%20nov%C3%ADsimas%20guerras.pdf, [consulta: 25 de septiembre de 2013], p. 8.

[61]*Cfr.* Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit.,* p. 175.

1.4.4. Retroceso en la historia

Si bien se ha abordado el fenómeno de las nuevas guerras, es importante mencionar que no todos los elementos pertenecen precisamente a la época actual. Hay muchas características de estas confrontaciones que comparten factores con conflictos llevados a cabo antes de que comenzara la Primera Generación de guerras, las cuales eran precisamente efectuadas por actores no estatales.

Se mencionan tres puntos principales que diferencian las primeras confrontaciones de las nuevas guerras, estas son[62]:

1. Predominio de armas ligeras;
2. Utilización de combatientes casi sin formación alguna;
3. Financiación mediante el robo y el comercio con mercancías ilegales.

Sin embargo, Federico Aznar menciona que el verdadero factor que diferencia a una época con la otra es el fenómeno de la Globalización porque:

> […] pone en contacto directo a sociedades con ejes referenciales distintos, produciendo como resultado un modo de hacer la guerra que se diferencia sensiblemente del practicado hasta el momento en que la victoria se creía sustentada sobre la tecnología […][63]

Aparecen nuevas estrategias que no sólo se basan en la utilización de los medios tecnológicos, sino también en la explotación de otros elementos que pueden marcar una diferencia importante entre los contingentes[64]. Además, como ya se ha mencionado, la superioridad tecnológica no significa asegurar un triunfo inmediato por alguna de las partes.

---

[62] *Cfr.* Teofilo Vásquez. "Las nuevas guerras y el conflicto armado en Colombia", [en línea], *op. cit.*

[63] Federico Aznar Fernández-Montesinos, Entender la guerra en el siglo XXI, *op. cit*, p. 152.

[64] *Ídem.*

La razón por la cual se les llamó nuevas guerras es porque en el momento que comenzaron a suscitarse significaron un enfrentamiento desconocido, ya que empezaron a surgir elementos extraños, los cuales no se ajustaban a la concepción de guerra que se poseía en ese momento; un ejemplo claro de esto es la Guerra de Bosnia-Herzegovina.

Este enfrentamiento se llevó a cabo del 6 de abril de 1992 al 14 de diciembre de 1995, ocasionado principalmente por problemas étnicos entre la población ya que se trataba de "[…] la república étnicamente más diversa de la antigua ex Yugoslavia, pues allí la población era musulmana (43,7%), serbia ortodoxa (31,4%) y croatas católicos (17,3%). Estos grupos serían los enfrentados en la guerra […]"[65], buscando cada uno, un objetivo diferente.

Este conflicto es considerado por muchos autores como la primera contienda que entró en esta nueva clasificación debido a los múltiples factores nuevos que tomaron lugar durante su desarrollo, como la utilización de nuevos métodos de guerra, la forma de financiar las hostilidades y sobre todo, el debilitamiento del Estado con la usurpación del monopolio de la fuerza al surgir nuevos actores en el campo de batalla.

Sin embargo, debido a varios factores, esta definición de nuevas guerras ya no se puede aplicar a los sucesos que están aconteciendo hoy en día, si bien se trata aún de fenómenos contemporáneos, los cuales todavía poseen algunas de las características que se han mencionado con anterioridad como la aparición de otros actores, diversas estrategias e instrumentos para realizar los conflictos, hay un elemento muy importante que ya no se presenta más: el debilitamiento, o en su caso, la desaparición de la figura del Estado junto con el monopolio de la fuerza.

Al parecer el retroceso en la historia se ha detenido y no ha conseguido mermar la importancia de este actor tan polémico, ya que este sujeto es el que, una vez

[65]Emersson Forigua Rojas, "Las nuevas guerras: Un enfoque desde las estructuras organizacionales", [en línea], Dirección URL: http://www.javeriana.edu.co/politicas/publicaciones/documents/9LASNUEVAS.pdf, [consulta: 20 de noviembre de 2013].

más, está al frente de todas las nuevas contiendas que se están elaborando actualmente alrededor del mundo, con la utilización de nuevos instrumentos bélicos, nuevas estrategias y objetivos, pero al final nadie ha sido capaz de usurpar su lugar.

Muchos han sido los elementos que han influenciado el cambio de paradigma, pero se considera que la tecnología es uno de los más importantes, ya que han sido precisamente estos adelantos los que han marcado la pauta para cambiar de una etapa a otra, provocando grandes transformaciones en la historia, y uno de ellos, el que quizá ha causado cambios mucho más rápidos en la sociedad, y claro está en el modo de efectuar una conflagración, es la Internet.

2. El ciberespacio como quinto dominio de la guerra

Tomando como referencia a la Real Academia Española, se entiende por dominio el poder que alguien tiene de usar y disponer de lo suyo, así como el ámbito real o imaginario de una actividad[66], de manera que se podría definir al dominio de la guerra como la capacidad que se posee para llevar a cabo enfrentamientos bélicos en los espacios que ya han sido estudiados y utilizados previamente en alguna contienda.

De acuerdo con el Departamento de Defensa estadounidense, el ciberespacio es el "[d]ominio que se caracteriza por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas de redes e infraestructuras físicas asociadas"[67].

Anteriormente, existían únicamente cuatro dominios de la guerra, sin embargo, en los últimos años se ha presentado un nuevo escenario en donde se están llevando a cabo los enfrentamientos bélicos: el ciberespacio. "[…] [A]unque es un dominio artificial, ciberespacio es ahora un dominio tan relevante para el Departamento de Defensa como las actividades que ocurren en dominios como tierra, mar, aire y espacio"[68].

Si bien este tipo de contiendas no son nuevas porque se han manifestado desde la década de los años ochenta y noventa, es ahora cuando están tomando más importancia debido a la gran dependencia que posee la mayoría de los países hacía la tecnología, sobre todo a la red inalámbrica, visto que muchos de sus servicios vitales dependen de ella.

---

[66]*Cfr*. Real Academia Española, "Dominio", [en línea], Dirección URL:http://lema.rae.es/drae/?val=dominio, [consulta: 26 de noviembre de 2013].

[67] Department of Defense, "Joint Terminology for Cyberspace Operations", [en línea], Dirección URL: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, [consulta: 29 de noviembre de 2014]. Traducción propia.

[68]Nathalie Caplan, "Cyber War: the Challenge to National Security", [en línea], vol. 4, núm. 1, *Global Security Studies,* 2013, Dirección URL: http://globalsecuritystudies.com/Caplan%20Cyber.pdf, [consulta: 20 de enero de 2014].

Una vez más, Internet se está utilizando como una herramienta en términos militares como sucedió durante la llamada Guerra Fría, período en el que surgió debido a las carreras armamentística y tecnológica llevadas a cabo entre los bloques capitalista y socialista. Si bien, aún es utilizada en términos económicos, hoy en día está regresando a sus raíces.

2.1. Guerra Fría: nacimiento de la Internet como arma

Al término de la Segunda Guerra Mundial en 1945, se llevaron a cabo las Conferencias de Yalta y Potsdam, en las cuales se planificó el primer reparto de los territorios ocupados en tres zonas de influencia que correspondían a los tres países vencedores: Gran Bretaña, Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas (URSS).

Inglaterra se encargaría de la región este del Mediterráneo, Estados Unidos, controlaría Europa Occidental y la URSS dominaría sobre Europa central y oriental. A partir de ese momento, esta alianza que había derrotado a las Potencias del Eje conformadas por Alemania, Japón e Italia, se empezó a deteriorar, dando paso a la conformación de un nuevo orden internacional que terminó de configurarse entre 1946 y 1947, momento en el que se puso fin a la colaboración existente y aumentó la tensión entre Estados Unidos y la URSS, dando pie a la conformación de dos bloques: el capitalista y el socialista.

En el momento en que Stalin impuso la tesis de que quien ocupara un determinado territorio, impondría en ése su propio sistema social, el mundo quedó automáticamente dividido. El orden mundial se comenzó a estructurar en forma bipolar y en 1946 Winston Churchill anunció el surgimiento de la cortina de hierro: una línea que dividía a la Europa Central y Oriental de la Occidental, los primeros sometidos no sólo a la influencia soviética, sino también a su completo control[69].

Ambas potencias buscaban reducir o eliminar la influencia del contrario, sin llegar nunca al enfrentamiento directo, incluso todas las hostilidades que se llevaron a

[69] *Cfr*. María Cristina Rosas, Walter Astié-Burgos, *El mundo que nos tocó vivir. El siglo XXI, la Globalización y el Nuevo Orden* Mundial, México, Miguel Ángel Porrúa, 2005, p. 41.

cabo fueron realizadas en otras regiones, jamás se derramó una gota de sangre dentro de su territorio. Esta rivalidad era de tal magnitud que fue llevada a varios campos, como el armamentista, espacial y tecnológico.

En varias ramas, la supremacía estadounidense era más que evidente, sin embargo, esto se puso en tela de juicio en 1957, con el lanzamiento del primer satélite artificial de la Unión Soviética: *Sputnik I*; para el bloque socialista este hecho significó un gran triunfo, no obstante, para la potencia estadounidense implicaba que al tener la capacidad de poner un satélite en órbita, también poseía los medios suficientes para portar una bomba atómica[70].

Es así como el presidente de Estados Unidos, Dwight Eisenhower, a través del Departamento de Defensa (DoD, *Department of Defense*), decide fundar la Agencia de Proyectos de Investigación Avanzada (ARPA) en 1958, con el objetivo de movilizar recursos, principalmente procedentes de universidades, y así poder alcanzar la superioridad tecnológica militar de la Unión Soviética[71].

A pesar de tener su origen en el Departamento de Defensa, el discurso que se manejaba era principalmente el desarrollo de la ciencia informática en Estados Unidos. Las aplicaciones militares, por otro lado, eran únicamente secundarias, se buscaba contar con una red de comunicaciones que tuviera la capacidad de mantenerse de pie, aún después de un ataque nuclear, con el fin de poder ingresar a sus datos desde cualquier parte del mundo, muy parecido a lo que es Internet hoy en día, a esta red se le llamó ARPANET (Red de la Agencia de Proyectos de Investigación Avanzada).

En 1975, ARPANET fue transferida a la Agencia de Comunicación de la Defensa, quien comenzó a utilizar la red con intenciones exclusivamente militares. A partir de ese momento, la coexistencia entre los programadores militares y los investigadores universitarios se tensó mucho, lo que sentó las bases para que se

[70]*Cfr*. Gonzalo Abella, "A propósito de la energía nuclear", [en línea], *Visiones Alternativas*, Cuba, Dirección URL: http://www.nacionmulticultural.unam.mx/mezinal/docs/545.pdf, [consulta: 25 de noviembre de 2013].
[71]*Cfr*. Manuel Castells, *La Galaxia Internet,* Barcelona, areté, 2001, pp. 23-24.

dividiera la red en 1983 entre MILNET, con objetivos únicamente militares y ARPA-INTERNET, dedicada solamente a la investigación[72].

Después de esta separación, comenzaron a desarrollarse varios adelantos en la red, así que en 1985 Internet ya se caracterizaba por tener una cobertura amplia entre la comunidad de investigadores y desarrolladores, quienes la usaban para comunicaciones informáticas diarias. Para ese entonces, el correo electrónico se había transformado en una herramienta conocida entre ellos[73].

Una vez que se llevó a cabo esta separación, ARPANET, que ya no poseía rasgos militares, fue consignada por el Pentágono a la Fundación Nacional para la Ciencia (NSF) en febrero de 1990, quien procedió inmediatamente a la privatización de la red. Pero lo que hizo posible que se comenzara a expandir por todo el planeta fue la aparición de la telaraña mundial de redes[74] (*world wide web)*, aplicación desarrollada por Tim Berners-Lee, la cual consistía en poder sacar e introducir información desde cualquier computadora conectada a través de Internet (HTTP, HTML y URI, denominado más tarde URL)[75].

Posteriormente, al iniciarse la expansión global de Internet, la NSF comenzó a planear su privatización, se decidió que la red debía de ser global, independiente de cualquier empresa y del control directo del Gobierno de Estados Unidos. Fue así como en enero de 1992 se formó la Sociedad Internet, (*Internet Society*) organismo sin ánimo de lucro a la que se le entregó la supervisión de la red[76].

Fue entonces cuando comenzaron a surgir varios navegadores, libres y privados, por lo que se hizo más sencillo acceder a la red para las pocas personas que, en ese entonces, contaban con un ordenador.

---

[72] *Ibídem*, p. 36.

[73]*Cfr*. Barry M. Leiner, Vinton G. Cerf, David D. Clark, *et. al*., *Internet Society*, "Brief History of the Internet" [en línea], Dirección URL: http://www.internetsociety.org/brief-history-internet, [consulta: 22 de noviembre de 2013].

[74]*Cfr*. Edmundo Hernández-Vela Salgado, Diccionario de Política Internacional, *op. cit.*, p. 560.

[75]*Cfr*. Manuel Castells, La Galaxia Internet, *op. cit.*, pp. 26-29.

[76]*Ibídem*, p. 45.

> Para mediados de los noventa, Internet estaba ya privatizado y su arquitectura técnica abierta permitía la conexión en red de todas las redes informáticas de cualquier punto del planeta, la *World Wide Web* podía funcionar con el *software* adecuado y había varios navegadores de fácil uso a disposición de los usuarios[77].

A pesar de que en un inicio los fines con los que se había comenzado a desarrollar la red eran académicos y militares, dependiendo de la red a la que se haga referencia, ARPA-INTERNET o MILNET, con el paso de los años su aplicación tomó un rumbo diferente al empezar a usarse con fines exclusivamente económicos; la mayoría de las empresas lo tomaron como una herramienta innovadora y asombrosa para poder expandir sus mercados a todos los rincones del mundo.

2.2. Evolución de su uso: círculo que regresa a la guerra

La red nació con propósitos académicos, no obstante, el elemento militar inminentemente estaba adherido al proyecto por el simple hecho de haber surgido en el seno de la Guerra Fría y por haber estado bajo la supervisión del Departamento de Defensa de Estados Unidos. Sin embargo, a partir de la década de los noventas, su difusión comenzó a acelerarse de manera significativa por todo el mundo, principalmente en el campo económico.

[77] *Ibídem*, p. 31.

De acuerdo con el Dr. Edmundo Hernández-Vela Salgado, Internet se define como:

> Red mundial de redes informáticas, que funciona gracias a un lenguaje común que define la manera en que los datos y mensajes son encaminados por medio de líneas telefónicas y otros enlaces de comunicación.
> Con los recientes impresionantes avances e *innovación* de la tecnología de la *información* y las comunicaciones, junto con la *biotecnología,* ambas decisivas impulsoras de la mundialización, y particularmente la fusión de la computación y comunicación, especialmente por conducto de la *Internet*, ha roto los límites de costo, tiempo y distancia, iniciando desde los primeros años noventa del siglo pasado una explosión sin precedentes de forma de comunicarse y una era de formación de redes de *información* mundial.
> Así, la *Interred* es una interconexión de más de 50,000 redes públicas y privadas en el mundo, basada en un *protocolo* de comunicación que sirve de lenguaje común para su interconexión, y que al estar injertada en las redes de *telecomunicaciones* públicas y privadas mundiales por una multitud de líneas rentadas, se apoya en 'redes de interconexión' resultantes en su gran mayoría de enlaces controlados por operadores públicos de telecomunicaciones.
> En más de 150 países los utilizadores enlazados a *Internet* tienen acceso a un amplio abanico de servicios telemáticos: correo electrónico, microservidores que cubren miles de temas, conversaciones en tiempo real, acceso a informaciones y datos provenientes de bibliotecas o de bases de datos electrónicos.
> […] La *Internet* se hizo verdaderamente popular al ofrecer herramientas más accesibles de –navegación- y de –investigación- sobre la red y permitir relacionar informaciones almacenadas en diferentes computadoras.
> […] Es indudable que una de las principales causas del acelerado desarrollo del mercado de las telecomunicaciones es la interacción de las nuevas maneras de hacer las cosas en la economía y la demanda de servicios PI y de banda ancha, ya que el intercambio de información entre las empresas se hace cada vez más por medio del Protocolo Internet. Las

> grandes empresas y las transnacionales y multinacionales utilizan de manera creciente las intranets o intrarredes, para intercambiar, distribuir y tratar la información al interior de la organización; y las extranets o extrarredes para comunicarse con sus asociados, proveedores y subcontratistas, así como con sus clientes para suministrarles información, efectuar transacciones y asegurar el servicio posterior a la venta[78].

La red ha sido considerada como el medio indispensable y el motor de la nueva economía, lo que provocó el surgimiento de nuevas reglas y procesos de producción en los mercados[79]. Es importante mencionar que esto no sólo ha influido en términos económicos, sino que también se ha convertido en una herramienta fundamental para millones de personas en todo el mundo, quienes lo utilizan en el trabajo y en la vida cotidiana.

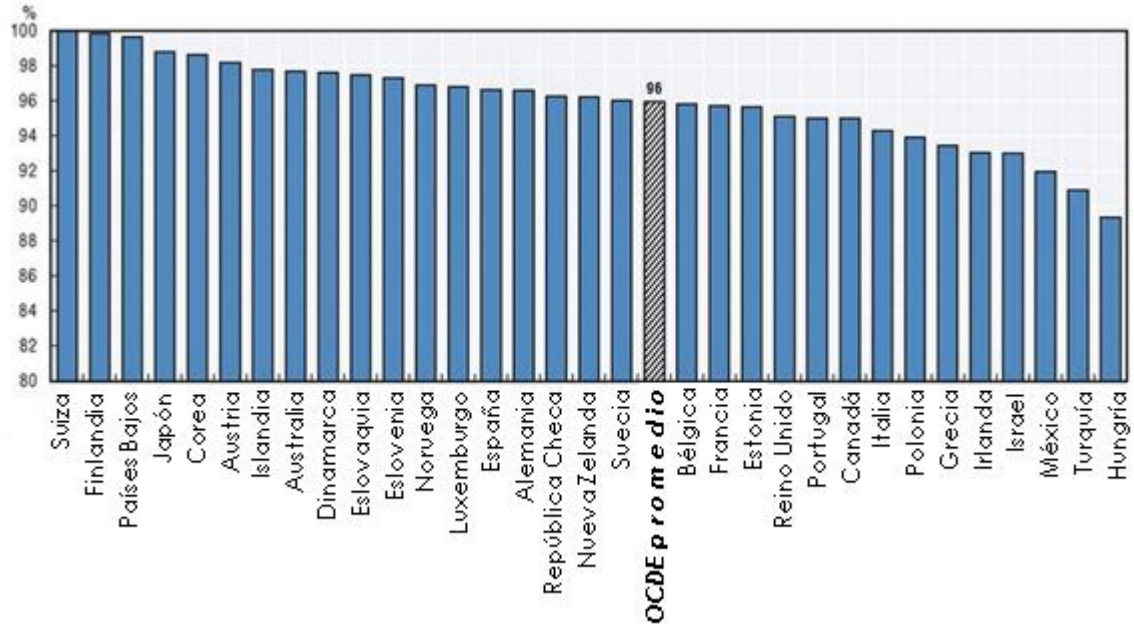
Internet ha transformado varios aspectos de la práctica empresarial, desde la relación con los proveedores y los clientes, hasta su gestión, proceso de producción y cooperación con otras empresas. El uso de esta herramienta se ha convertido en una fuente fundamental de productividad y competitividad para toda clase de empresas[80].

Desde la década de los noventas, el número de negocios que se han servido de la Internet para tener un crecimiento económico ha aumentado significativamente. En la siguiente tabla se muestra el porcentaje de comercios que utilizaba la red como herramienta principal en algunos países en el 2011.

[78] Edmundo Hernández-Vela Salgado, Diccionario de Política Internacional, *op. cit.*, pp. 594-596.
[79] *Cfr.* Manuel Castells, La Galaxia Internet, *op. cit.*, p. 71.
[80] *Ibídem.* p. 81.

Figura 3

Negocios usando internet, 2011



Fuente: Elaboración propia con datos de Organization for Economic Co-operation and Development, *OECD Internet Economy Outlook 2012*, [en línea], Dirección URL: http://www.keepeek.com/oecd/media/science-and-technology/oecd-internet-economy-outlook-2012_9789264086463-en#page1, p. 136, [consulta: 20 de noviembre de 2013].

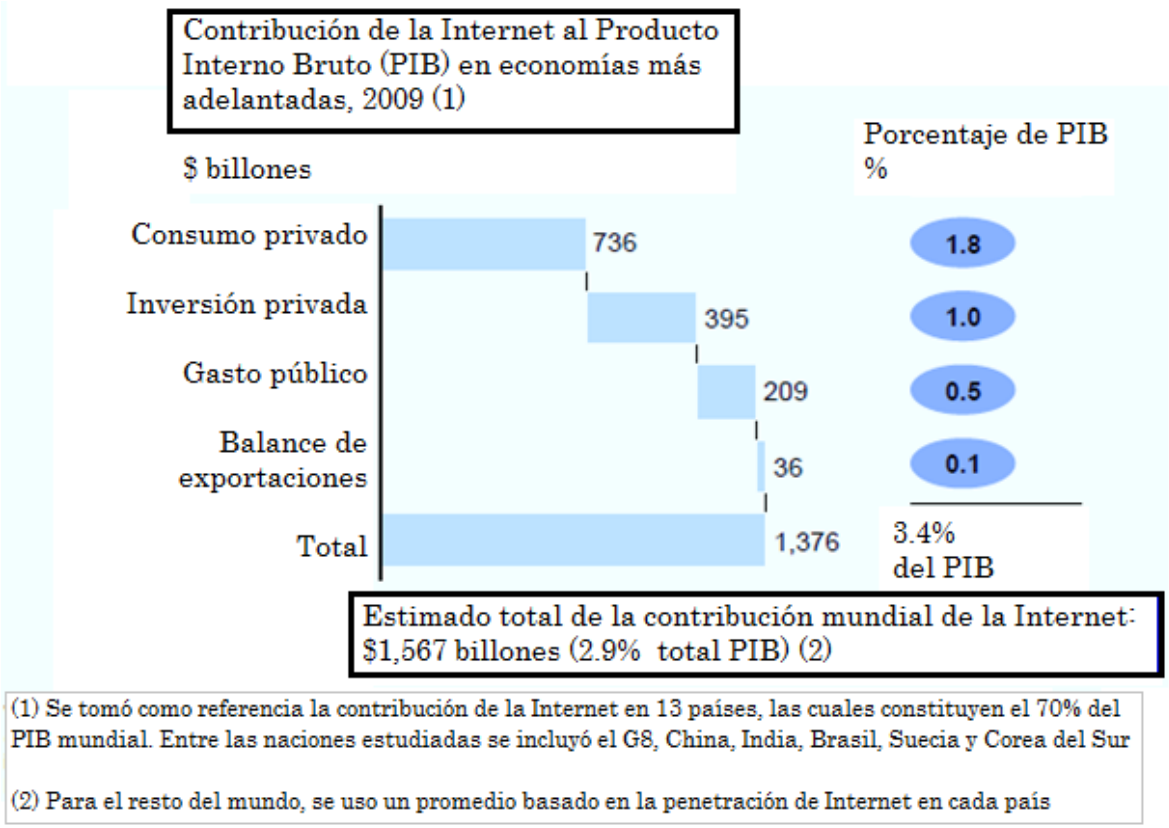
Utilizar la red en los negocios ha resultado ser una decisión que la mayoría de las industrias ha tomado para obtener grandes ganancias, situación que no sólo beneficia a las empresas, sino también a los Estados en general. Tan sólo en el año 2000, el valor de las transacciones comerciales a través de la red alcanzó en Estados Unidos la cifra de 400,000 millones de dólares[81].

La siguiente gráfica muestra de una manera más clara el papel que ha tenido Internet en la economía de las naciones, en este caso se muestra la contribución de ello en su Producto Interno Bruto (PIB).

[81] *Ídem.*

Figura 4

Internet en el PIB de las economías desarrolladas, 2009



Fuente: James Manyika, Charles Roxburgh, *McKinsey Global Institute*, "The great transformer: The impact of the Internet on economic growth and prosperity", [en línea], 2011, Dirección URL: http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer, [consulta: 15 de noviembre de 2013].

Este nuevo panorama en los negocios es definido como negocios en línea (*e-business*) por el autor Manuel Castells, quien asegura que se trata de una

> […] actividad cuyas operaciones clave de gestión, financiación, innovación, producción, distribución, ventas y relaciones entre los empleados y con los clientes tienen lugar sobre todo por Internet o en otras redes de redes informáticas, sin prejuzgar el grado de conexión entre las dimensiones virtual y física de la empresa. Al utilizar Internet como un medio fundamental de

> comunicación y procesamiento de la información, las empresas adoptan la red como su forma organizativa.[82]

Las empresas, conscientes del potencial que ofrecía Internet, no dudaron en adoptarla como parte fundamental de su estructura. Se considera que el pionero de este modelo es Cisco Systems, el mayor productor de equipos electrónicos durante los años noventa, quien fue uno de los primeros en instalar la infraestructura de la red en el momento en que comenzaba a tomar importancia y eso le aseguró un gran triunfo durante los años posteriores.

Sin embargo, nunca se dejó de lado el uso bélico de esta herramienta, si bien es cierto que durante algunos años se utilizó en mayor medida con fines económicos, los asaltos cibernéticos han formado parte de las estrategias de seguridad nacional desde varias décadas atrás. Como indica Edward Luttwak, economista, politólogo, reconocido por sus publicaciones sobre estrategia militar y política exterior, "[a] medida que la guerra y la sociedad se han vuelto más complicadas […] la estrategia tiene por necesidad la creciente consideración de factores no militares como los económicos, psicológicos, políticos, morales y tecnológicos […]"[83].

Un ejemplo de ello es cuando Estados Unidos se estaba preparando para su primera guerra contra Iraq en 1990, se deseaba utilizar algo más que armamento militar, se quería implementar el uso de la internet para eliminar la red de radares y cohetes de la defensa antiaérea iraquí antes de que los aviones estadounidenses fueran detectados.

Se planeaba llevar a algunos especialistas en el tema para que se conectaran a la red, posteriormente enviar un programa que haría que todos los ordenadores del país conectados a ella se bloquearan y fuera imposible reiniciarlos[84]. A pesar de tener lista la estrategia, el plan se consideró demasiado peligroso y en cierto

---

[82] *Ibídem.* p. 83.

[83] Edward Luttwak, "Strategy: The logic of War and Peace", [en línea], Dirección URL: http://reasonpapers.com/pdf/20/rp_20_9.pdf, [consulta: 20 de febrero de 2015].

[84] Richard A. Clarke, Robert K. Knake, *Guerra en la red. Los nuevos campos de batalla*, Barcelona, Ariel, 2011, p. 27.

sentido utópico, ya que no se creía realmente que fuera posible interferir en los sistemas de seguridad de otro país de forma remota.

Se habían hecho algunos ataques utilizando algún tipo de virus, pero nunca se había intentado algo semejante como aquello. Sin embargo, con el pasar de los años esa idea ya no resultaba ser tan extravagante, porque las noticias sobre ataques a los sistemas informáticos de los países eran cada vez más frecuentes.

Fue a partir del 2007 cuando comenzaron a escucharse los términos de ataques cibernéticos, guerra cibernética, ciber comandos, etc., con mayor vehemencia. Siria, Estonia y Georgia fueron de los primeros países en sufrir un ataque masivo realizado gracias al uso de Internet, asaltos que tuvieron varios objetivos: facilitar agresiones militares tradicionales, el colapso de páginas gubernamentales, bloquear servicios claves como los bancos, privarlos de comunicación con el exterior, etc.

Una nueva forma de hacer la guerra ha surgido y está evolucionando a un ritmo impresionante. Los países se están enfrentando a un nuevo fenómeno sin precedentes; como pasó en la Guerra de Bosnia-Herzegovina, es necesario estudiar a fondo el conflicto para entender con mayor claridad lo que está sucediendo y tomar las medidas pertinentes.

2.3. Guerra cibernética

Debido a que el tema tratado es relativamente nuevo, no existe un concepto aceptado por la mayoría de los países, aún no ha habido un acuerdo internacional sobre qué elementos específicos constituyen un acto de Ciberguerra, es por eso que varios autores han tratado de definirla basándose en los sucesos recientes, algunos de ellos poseen algunos rasgos similares, sin embargo, hay otros que no comparten ninguna característica en común.

Entre ellos se encuentra el autor Jeffrey Carr, experto en ciberataques contra gobiernos e infraestructuras efectuados por actores estatales y no estatales. Partiendo de los preceptos de Sun Tzu él menciona que la Ciberguerra es “[…] el

arte y la ciencia de pelear sin pelear, de vencer a un oponente sin derramar sangre"[85]. Una definición muy breve y poco clara, ya que otro tipo de contiendas podrían encajar con esa descripción, por ejemplo la guerra psicológica.

Por otra parte, en la revista Estudios de Seguridad Global (*Global Security Studies)* de la Universidad Wilmington en Carolina del Norte, Nathalie Caplan lo define como aquellas acciones que tienen como fin "[…] alterar, interrumpir, engañar, degradar o destruir sistemas o redes de información y/o programas residentes o en tránsito en esos sistemas o redes"[86]. De igual manera, asegura que este tipo de ataques son extremadamente baratos y fáciles de realizar, por lo que será cada vez más frecuente su presencia en la escena internacional.

Andrew Krepinevich, presidente del Centro para Evaluaciones Estratégicas y Presupuestarias otorga la siguiente definición:

> Ciberguerra puede ser definida como acciones realizadas por actores estatales o no estatales empleando ciber armas para penetrar computadoras o redes con el propósito de entrar, corromper, y/o falsificar datos […]. Pueden involucrar engaños y actos de espionaje, actividades criminales y guerra económica. También pueden incluir acciones destinadas a operaciones militares en diversos niveles, así como operaciones independientes destinadas a lograr efectos estratégicos[87].

Después de analizar cada una de las descripciones brindadas, sin duda la que explica con mayor claridad la mayoría de los elementos que conforman a la Ciberguerra es la del Dr. Krepinevich. Incluso menciona el espionaje y las actividades criminales como parte de la Ciberguerra, siendo que otros autores, como Jeffrey Carr, manejan estos elementos como sinónimos.

---

[85] Jeffrey Carr, *Inside Cyber Warfare,* Segunda edición, Estados Unidos, O'Reilly, 2012, p. 2.
[86] Nathalie Caplan, "Cyber War: the Challenge to National Security", [en línea], *op. cit*.
[87] Andrew Krepinevich, *Cyber Warfare. A 'Nuclear Option'?*, Center for Strategic and Budgetary Assessments, 2002, pp. 8-9.

Es por eso que es de gran importancia recalcar que Ciberguerra y cibercrimen no deben ser tratados como iguales, ya que el segundo se refiere a "[…] un delito económico cometido mediante el uso de tecnología, casos típicos de la delincuencia informática [como] la distribución de virus, las descargas ilegales de medios […] y el robo de información personal, como datos bancarios"[88]. Sin embargo, para enfrentar a ambos se requiere de una estrategia de Ciberseguridad y Ciberdefensa.

Si bien aún no se ha llegado a un acuerdo sobre la definición y elementos de la Ciberguerra, es claro que este nuevo fenómeno afecta tanto a la Seguridad Nacional como a la Internacional, la primera definida por el Dr. Edmundo Hernández-Vela como el

> Conjunto de políticas, estrategias, normas, instituciones y acciones que tienden a la armonización plena de los elementos constitutivos el Estado, protegiéndolos y salvaguardándolos de actos o situaciones de cualquier naturaleza, internos o externos, que perjudiquen o afecten de alguna manera su integridad o óptimo desempeño y aprovechamiento en el impulso del proceso de desarrollo y el progreso del país en todos los órdenes. En esta perspectiva global e integral la seguridad nacional de cada Estado se desenvuelve, al mismo tiempo, en diferentes esferas de su vida nacional e internacional: social, económica, jurídica, política, estratégico-militar, etcétera, destacando o sobresaliendo alguna o varias de ellas según el desarrollo de la situación[89].

Por otro lado, Seguridad Internacional está "[…] basada en la estabilidad y armonía de las interrelaciones de las seguridades nacionales de todos los Estados, lo que constituye la *seguridad internacional*, así como a la *seguridad colectiva*, cuando varios de estos sujetos de la *sociedad internacional* se agrupan

[88] PWC, "Cibercrimen: ¿Está su organización en riesgo? Encuesta Global de Delitos Económicos 2011", [en línea], Dirección URL: http://www.pwc.com/gx/en/economic-crime-survey/assets/pwc-gecs-venezuela.pdf, [consulta: 21 de febrero de 2015].

[89] Edmundo Hernández-Vela Salgado, Diccionario de Política Internacional, *op. cit.*, p. 1094.

estableciendo sistemas de protección conjunta contra riesgos y peligros del exterior de los mismos"[90].

Asimismo, hasta cierto punto la mayoría de los autores ha aceptado el ciberespacio como nuevo dominio de la guerra. Sin embargo, existen sus excepciones, otros autores como Jeffrey Carr han declarado que estos ataques no pueden ser clasificados como actos de guerra debido a que se está presentando como un área sumamente maleable y no se puede llegar a ese tipo de conclusiones sin estudiar a fondo el fenómeno.

Para este autor, "la guerra no comienza hasta que el metal está volando a través del aire", asimismo exhorta no sólo a que se maneje de manera diferente de la guerra tradicional, ya que la mayoría de los militares la conduce como una conjunción con los ataques militares físicos y eso no debería ser así, sino también a que se utilice la palabra "guerra" más cuidadosamente y no de una manera tan indiscriminada[91].

Lo que es un hecho es la cantidad de asaltos cibernéticos que se han ido desarrollando en los últimos años. Si bien hoy en día la mayoría de las personas apenas se está percatando de estos altercados que ocurren alrededor del mundo, los agravios iniciaron desde tiempo atrás, de una forma más arcaica y sosegada, pero ya se comenzaba a buscar la manera de penetrar en las redes enemigas.

La siguiente gráfica muestra la manera en que estos ataques han ido aumentando, desde principios del siglo hasta el año 2007, momento en el que se llevó a cabo el asalto a Estonia e iniciaron las agresiones de manera más consecutiva y sin tapujo alguno.

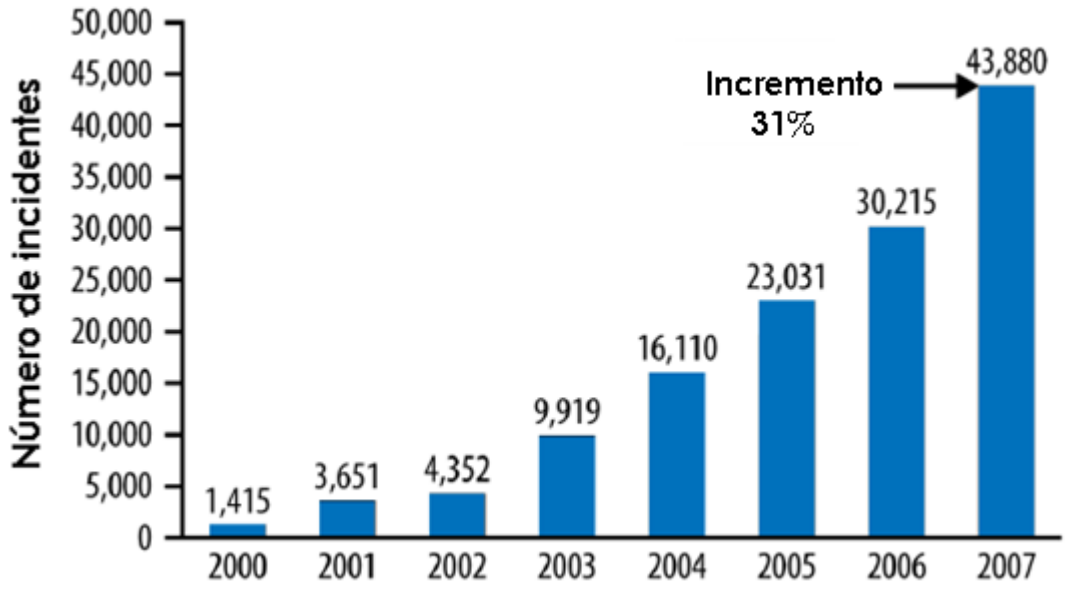
---

[90] *Ibídem*. pp. 1094-1095.

[91] *Cfr*. Andy Greenberg, "The Real Meaning of Cyberwarfare", [en línea], *Forbes,* marzo, 2010, Dirección URL: http://www.forbes.com/2010/03/03/jeffrey-carr-internet-technology-security10-cyberwar.html, [consulta: 20 de enero de 2014].

Figura 5

Incidentes de ciberataques



Fuente: Elaboración propia con datos de Jeffrey Carr, *Inside Cyber Warfare*, Segunda edición, Estados Unidos, O'Reilly, 2012, p. 6.

Es claro que a partir de ese punto, el porcentaje de las agresiones ha aumentado estrepitosamente, debido a la facilidad y al bajo costo que representa realizarlos. Es precisamente por eso que los objetivos que se buscan actualmente se han ampliado de manera significativa en comparación con los primeros ataques que se realizaron.

2.3.1. Breve historia de la Ciberguerra

Así como sucedió con la guerra tradicional, se desconoce completamente dónde, cómo y cuándo se realizó el primer ataque cibernético en la historia; algunos autores lo remiten desde la década de los ochentas, mientras que la gran mayoría lo relacionan con el auge de la Internet en los años noventa.

El autor Andrew Krepinevich argumenta que los asaltos cibernéticos se han llevado a cabo por lo menos desde hace quince o tal vez treinta años. Uno de los primeros fue realizado en 1982, durante la administración del presidente Ronald Reagan; el ataque consistió en introducir un virus de Troya en los equipos

informáticos que la Unión Soviética había adquirido en Canadá, lo que causó varias fallas en un gasoducto transiberiano, conduciéndolo a una explosión de gran escala[92].

A partir de la década de los noventas, época en que inició de manera vertiginosa la expansión de la Internet, los *hackers* comenzaron a realizar "ciber bromas" para explorar el potencial de los ataques. Después de algunos años, cuando ya se había demostrado de cierta manera su efectividad, los gobiernos empezaron a interesarse cada vez más, por lo que decidieron brindar su apoyo al desarrollo e investigación de esos asaltos.

Es en este momento cuando se recomienda que el término *hacker* sea sustituido por el de *cracker,* ya que, como lo indica la Dra. Ma. Cristina Rosas, "[…] los hackers son muy distintos de los crackers, dado que éstos, aunque muestran una conducta similar a la de aquellos, 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"[93].

Las primeras agresiones no tenían como objetivo usar virus para acceder o borrar datos importantes, colapsar computadoras, robar secretos comerciales o cualquier otra actividad que se está llevando a cabo hoy en día, sino que ellos buscaban tomar el control de los sistemas y usarlos para mandar correos electrónicos masivos (*spam*), la mayoría de ellos con la finalidad de extorsionar[94].

En general, la mayoría de los agravios potenciales que se cometieron durante las décadas de los ochenta y noventa asociados con sistemas y redes, difícilmente

[92]*Cfr.* John Markoff, "Old Trick Threatens the Newest Weapons", [en línea], *The New York Times*, 26 de octubre de 2009, Dirección URL: http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all&_r=0, [consulta: 20 de febrero de 2014].

[93] María Cristina Rosas, "De la ciberguerra a la ciberpaz", [en línea], Dirección URL: http://www.etcetera.com.mx/articulo/de_la_ciberguerra_a_la_ciberpaz/9759/pagina/2, [consulta: 20 de febrero de 2015].

[94]*Cfr.* Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.,* p. 18.

se dieron a conocer en esos años. Krepinevich menciona que fue hasta inicios del siglo XXI cuando el poder de los virus de computadoras fue revelado, debido a uno de los primeros programas que causó grandes daños alrededor del mundo: *The Love Bug*.

Este virus fue creado en Filipinas en el año 2000 e infectó de manera exitosa aproximadamente 55 millones de computadoras. El *malware*[95] fue enviado en forma de correo a miles de personas con el texto "I LOVE YOU", en el momento en que el usuario abría el correo, un gusano invadía el equipo provocando que se auto enviara el mensaje a toda la lista de contactos, causando graves percances al ordenador. El daño fue calculado en quince mil millones de dólares[96].

The Love Bug fue sucedido por otros virus como: *SoBig*, *Bagle* y *MyDoom*[97]. Los tres tuvieron gran similitud con su predecesor, lo único en lo que se diferenciaron fue que existieron muchas versiones de cada uno de ellos, más peligrosas y mejoradas. Por ejemplo, *SoBig* es considerado como el primer virus comercial, es decir, creado para poder robar datos importantes de gobiernos y/o empresas.

Todos causaron pérdidas estimadas en miles de millones de dólares, sin embargo, a pesar del daño hecho nunca pudieron encontrar al responsable de esas actividades. Aunque posteriores investigaciones arrojaron que el origen de uno de los virus se debía a La Red de Negocios Rusa (*RBN*, The Russian Business Network) jamás se pudo comprobar nada, incluso cuando en 2007 el 40%[98] de los ciberataques fue atribuido a ellos.

La RBN es el único organismo que ha sido identificado por la Organización del Tratado del Atlántico Norte (OTAN) como una de las mayores amenazas cibernéticas. Asimismo, fueron los principales sospechosos en los ataques

[95]*Software* malicioso que obliga a los ordenadores a hacer cosas de manera que sus propietarios no se enteran. Ejemplos: gusanos, bombas lógicas, etc.
[96]*Cfr.* Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.,* p. 19.
[97]*Ídem.*
[98] *Ibídem.* p. 21.

realizados contra Estonia en 2007 y contra Georgia en 2008, los cuales serán abordados más adelante.

2.3.2. Principales pioneros

Existen otras agresiones que fueron emprendidas por diferente actores internacionales como India y Paquistán (1998), Hamas (1999), Turquía y Armenia (2000), Hezbollah (2001), Indonesia y Malasia (2005)[99], sin embargo, los principales pioneros y quienes llevaron los ataques cibernéticos a otros niveles fueron, sin duda, Estados Unidos, Rusia, China y Corea del Norte.

2.3.2.1. Federación Rusa

De acuerdo con varios autores, Rusia ha sido autor de innumerables ataques dirigidos a todas partes del mundo, no obstante, existen tres agresiones que llevan su firma y que han sido de las más importantes, no sólo por la forma en que se llevaron a cabo, sino porque dieron pie a la creación del Manual de Tallin, creado a petición del Centro de Excelencia para la Defensa Cooperativa Cibernética de la Organización del Tratado del Atlántico Norte, el cual establece el Derecho Internacional que se puede aplicar a la Ciberguerra, así como la constitución de 95 normas que deberían regir este tipo de conflictos[100].

El primero de ellos se llevó a cabo en Estonia en el año 2007. Después de la implosión de la Unión de Repúblicas Socialistas Soviéticas (URSS), el Partido Comunista no quería que los estonios olvidaran los sacrificios que se habían realizado para liberarlos, así que se decidió poner una estatua de bronce con la figura de un soldado del Ejército Rojo.

En febrero de 2007 se aprobó una ley llamada "ley de estructuras prohibidas"[101], la cual ordenaba demoler todo signo de ocupación, incluido el soldado de bronce.

---

[99]*Cfr*. Nathalie Caplan, "Cyber War: the Challenge to National Security", [en línea], *op. cit*.

[100]*Cfr*. s/a, "Publicación del Manual de Tallin sobre 'Ley Internacional en la Ciberguerra' ", España, *Ministerio de Defensa*, 22 de marzo de 2013, Dirección URL: http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59, [consulta: 16 de abril de 2013].

[101]*Cfr*. Richard A. Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, p. 31.

Esta decisión causó una gran controversia entre Estonia y Rusia, porque el primero argumentaba que ese monumento, construido en 1947, simbolizaba la ocupación soviética, mientras los rusos discrepaban de ese comentario afirmando que la figura recordaba a los héroes que lucharon contra los nazis. Esta postura no hubiese tenido un gran peso en el país báltico si no hubiera sido porque la tercera parte de la población está compuesta por rusos[102].

El presidente Estonio, Toomas Hendrik Ilves, al enfrentarse a tal situación decidió vetar la ley para evitar un problema internacional de mayor magnitud. Sin embargo, la presión por aquellos que querían que la estatua fuera quitada fue tan grande que el 27 de abril estalló un enfrentamiento llamado "la noche de bronce"[103] entre ambas facciones, a causa de eso, se dictaminó moverla de lugar, causando la indignación de los medios moscovitas.

Fue a partir de ese punto que las páginas electrónicas más utilizadas alrededor de Estonia comenzaron a ser atacadas con miles de solicitudes de acceso provenientes de todas partes del mundo, causando su inminente colapso. "Los estonios no podían utilizar sus bancos en línea, leer sus periódicos en Internet o acceder a los servicios electrónicos del gobierno. […] El Hansapank, el banco más grande del país, se tambaleó. A lo largo y ancho del país, el comercio y las telecomunicaciones se vieron afectadas […]"[104], incluso la página oficial del presidente y la del Parlamento fueron bloqueadas.

El problema persistió por varias semanas, lo que provocó que Estonia acudiera al Consejo del Atlántico Norte. Después de las investigaciones pertinentes, los datos arrojaron que los ataques tenían su origen en computadoras rusas. Un oficial de Estonia concluyó que las agresiones representaban una nueva forma de relación

[102]*Cfr*. s/a, "La guerra fría cibernética", [en línea], Londres, *BBC Mundo*, sección "Internacional", 17 de mayo de 2007, Dirección URL: http://news.bbc.co.uk/hi/spanish/international/newsid_6665000/6665367.stm, [consulta: 29 de abril de 2013].
[103]*Cfr*. Richard A. Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, p. 32.
[104]*Ibídem.* pp. 33-34.

público-privado, es decir, ataques ejecutados por hackers pero dirigidos por el Kremlin[105], sin embargo, como es evidente, Rusia lo negó.

Algunos expertos creen que estos altercados proporcionaron a Rusia una manera innovadora de probar sus nuevas armas para las guerras venideras, integrando los conocimientos adquiridos en las acciones militares tradicionales que se llevaron a cabo en la operación que realizaron contra Georgia.

El segundo ataque fue realizado en el 2008 contra la República de Georgia. En 1993 Georgia perdió el control de dos de sus territorios, en donde hubo una participación muy activa por parte de Moscú: Osetia del Sur y Abjasia. A principios del 2008 Osetia del Sur atacó Georgia, la respuesta por parte del país fue natural, invadió la región. No obstante, Rusia de inmediato ayudó a los separatistas atacando a los georgianos con su ejército y con sus ciberguerreros de manera simultánea.

Su objetivo era cortar la comunicación con el exterior, bloqueando páginas electrónicas de los medios de comunicación locales, el acceso a los sitios de la CNN y la BBC. Esto causó que no se pudieran conectar a ninguna fuente exterior de noticias o información y tampoco enviar correos electrónicos fuera del país[106]. Georgia se convirtió en una nación completamente aislada, sin poder saber lo que sucedía en el exterior ni tampoco dar a conocer su condición, a pesar de que intentó hacerle frente a Rusia de la misma manera, los moscovitas neutralizaron cada uno de sus intentos.

Incluso los rusos hicieron parecer que era Georgia la que estaba efectuando esos ataques cibernéticos, no sólo contra Rusia sino contra bancos de todo el mundo, lo que causó que fueran cortadas todas sus conexiones con el sector bancario. Acceso al exterior, actividades bancarias, telefonía móvil, entre otras actividades le fueron bloqueadas.

[105]*Cfr.* Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.,* p. 24.
[106]*Cfr.* Richard A. Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.,* p. 40.

El tercer ataque efectuado fue contra Kirguistán, llevado a cabo en enero de 2008, tan sólo cinco meses después del asalto en Georgia. Este agravio consistió en lanzar un Ataque de Denegación de Servicio (DDoS*, Destributed Denial of Service*)[107], contra los dos principales servidores del Estado, lo que causó el bloqueo de sitios web y el envío de correos electrónicos alrededor del país. Todo esto se efectuó con la intención de ejercer coerción contra Kirguistán, ya que el mismo día del ataque, la administración rusa presionaba al gobierno kirguiso "[…] para finalizar el acceso de EE.UU a su base aérea en Manas, un centro logístico clave de apoyo a sus operaciones militares en Afganistán"[108].

Así que, en cuanto Kirguistán informó al gobierno estadounidense que su acceso a dicha base debería concluir, los ataques cibernéticos cesaron de manera inmediata; un claro ejemplo de cómo Rusia utiliza su poder sin reparo alguno para ejercer coerción contra terceros, con la única finalidad de responder a sus propios intereses.

De acuerdo con un informe de *Fire Eye*, compañía líder en ciber defensa, los ataques rusos poseen características específicas que se han presentado en la gran mayoría. Según ellos, el objetivo principal de Rusia es la obtención de información, un ejemplo de ello es "Octubre rojo"[109], un ataque realizado en el 2012, el cual buscaba espiar a millones de ciudadanos alrededor del mundo, principalmente a aquellos países que eran parte de la antigua Unión Soviética y, sorprendentemente, a su propia población.

---

[107] Ataque que se basa en coordinar ordenadores huéspedes o *zombis* conectados a Internet, de tal manera que concentren el asalto de forma simultánea y desde diferentes lugares sobre un único objetivo, causando una denegación del servicio, es decir, hacer que un sistema no pueda cumplir su cometido; o una saturación de la red que puede llevar a un colapso inminente.
La ventaja de este ataque, es que, al usar diferentes ordenadores, resulta muy difícil saber cuál es el verdadero origen.

[108] Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.*, p. 26. Traducción propia.

[109] *Cfr*. Kenneth Geers, Darien Kindlund, *et. al*., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, [en línea], Dirección URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf, [consulta: 29 de enero de 2014].

Entre los blancos se encontraban, embajadas, empresas de investigación, bases militares, proveedores de energía, agencias nucleares e información sobre la infraestructura clave de cada una de las naciones implicadas.

Figura 6

Características de ciberataques rusos

Exploración	Posibles fuentes de obtención de información secreta
Militarización	Documentos maliciosos/Formatos de archivo XLS
Entrega	Correo electrónico con archivos adjuntos infectados
Aprovechamiento	Vulnerabilidades de las aplicaciones, *Día Cero*
Instalación	Tecnología de acceso remoto (RAT, *Remote Access Technology)* con módulos encriptados
Mando y Control	Protocolo de transferencia de hipertexto (HTTP, *Hyper Text Transfer Protocol)* con codificación incrustada personalizada /encriptación
Objetivos	Recopilación de información (Centrada en el gobierno)
Modelos de tácticas, técnicas y procedimientos	Octubre Rojo

Fuente: Elaboración propia con datos de Kenneth Geers, Darien Kindlund, *et. al*., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, [en línea], Dirección URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf, [consulta: 29 de enero de 2014].

Otra característica importante que se debe mencionar es que, algunas medidas de seguridad que ha tomado el gobierno ruso contra este fenómeno han sido totalmente extremas, un ejemplo de ello es la adopción de máquinas de escribir para recabar toda la información importante y de esa manera, no correr el riesgo de que sea robada[110].

[110]*Cfr*. Geoffrey Ingersoll, "Russia Turns to Typewriters to Protect Against Cyber Espionage", [en línea], *Business Insider*, 11 de julio de 2013, Dirección URL: http://www.businessinsider.com/russia-turns-to-typewriters-for-secrets-2013-7, [consulta: 12 de febrero de 2014].

Rusia se encuentra dentro de los países emisores de ciberataques más complejos y avanzados que existen, desarrollados con aún más cautela que los asaltos realizados por China, ya que en cada uno de los agravios su identidad y sus objetivos han sido escondidos tras una bandera falsa, principalmente perteneciente al continente asiático.

2.3.2.2. Estados Unidos

Los ataques emitidos por Estados Unidos son considerados como los más avanzados y de más alta tecnología alrededor del mundo. La potencia estadounidense ha emitido innumerables ataques hasta en los rincones más recónditos del globo; sin embargo, uno de los más famosos ha sido el *malware Stuxnet*, visto como el primer virus realmente malicioso de la historia, capaz de realizar daños físicos.

Se desconoce con exactitud quién o quiénes fueron los creadores de dicho gusano, aún así diversas fuentes apuntan que fue diseñado conjuntamente en junio de 2010 por Estados Unidos e Israel. La característica principal de este virus es que "[…] se enfoca en el Control de Supervisión y Adquisición de Datos (SCADA, *Supervisory Control and Data Acquisition*), el cual controla sistemas tales como motores, sensores, alarmas, bombas, válvulas entre otras infraestructuras trascendentales"[111]. Lo único que se necesita es instalar el programa y de esa forma realizará automáticamente las funciones específicas que se le fueron asignadas.

El objetivo central de la creación de *Stuxnet* fue conocer los elementos clave del programa nuclear de Irán y así poder llevarlo a pique destruyendo las centrifugadoras de gas usadas para abastecerse de uranio, ocasionando un inminente caos[112]. Para conseguir este propósito, más de 50,000 computadoras fueron infectadas dentro de la planta nuclear, sin que los avanzados sistemas de

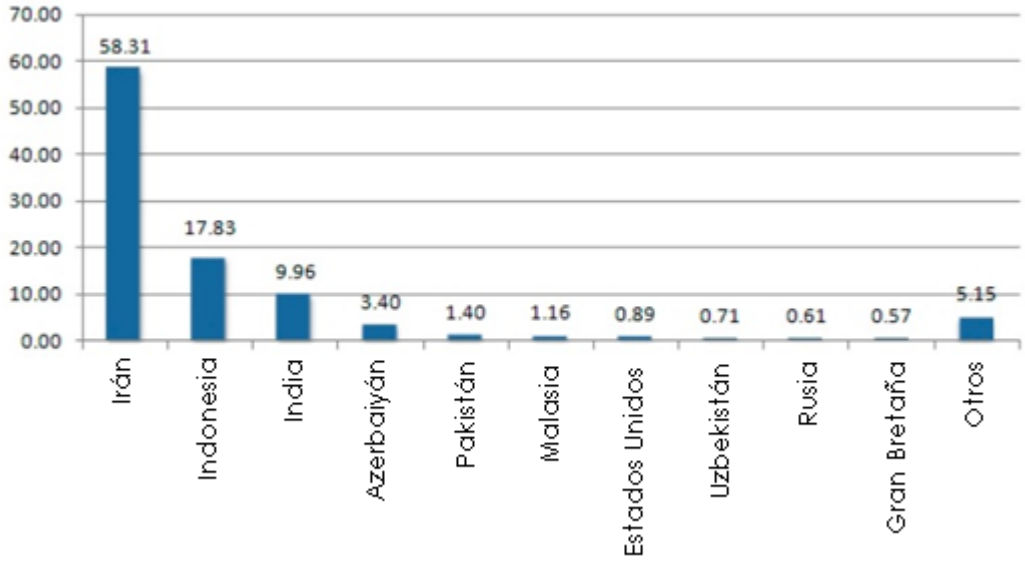
[111] Nathalie Caplan, "Cyber War: the Challenge to National Security", [en línea], *op. cit.* Traducción propia.
[112] *Cfr*. Paul Mueller, BabakYadegari, "The Stuxnet Worm", [en línea], Dirección URL: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf, [consulta: 3 de febrero de 2014].

seguridad iraníes se percataran de ello, suscitando fallas en el motor eléctrico de los abastecedores causando la destrucción de 1000 centrifugadoras aproximadamente.

Sin embargo, Irán no fue el único blanco que tenía en la mira dicho virus, aunque sí el más perjudicado; de los 100,000 equipos afectados por *Stuxnet*, 40,000 se encontraban fuera del territorio iraní, en países como Indonesia e India, entre muchos otros[113].

Figura 7

Distribución geográfica de infección por Stuxnet



Fuente: Illaro Eguskiñe Lejarza, "Ciberguerra, los escenarios de confrontación", [en línea], *Instituto Español de Estudios Estratégicos, Opinión*, núm. 18, febrero, 2014, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf, [consulta: 20 de abril de 2014].

Algunos expertos manifiestan que *Stuxnet* posee tal sofisticación que es poco probable que sólo hayan estado implicados Estados Unidos e Israel, ya que existen más actores internacionales que están en contra del programa nuclear de

[113]Illaro Eguskiñe Lejarza, "Ciberguerra, los escenarios de confrontación", [en línea], *Instituto Español de Estudios Estratégicos, Opinión*, núm. 18, febrero, 2014, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf, [consulta: 20 de abril de 2014].

Irán y ellos bien pudieron haber tenido una participación activa en la destrucción de sus abastecedores de uranio. Además, teniendo en cuenta la variedad de blancos, debieron de haber estado comprometidos más intereses, no sólo los estadounidenses o israelíes.

Más tarde, en octubre de 2011 *CrySys*, el Laboratorio de Criptografía y Seguridad de Sistema, perteneciente a la Universidad de Tecnología y Economía de Budapest, descubrió un segundo gran virus llamado *Duqu*, el cual parecía haber sido creado siguiendo el mismo código que su predecesor: *Stuxnet*, pero lo que los diferenciaba era que *Duqu* tenía otro funcionamiento por lo que su objetivo era completamente diferente.

Este nuevo gusano no contenía ningún código relacionado con sistemas de control industrial, es decir, que no fue creado para sabotear sistemas como sensores, alarmas, bombas, o centrifugadoras; su principal funcionamiento consistía en recolectar información sustancial como contraseñas y documentos de diseño[114], accediendo a ella por acceso remoto, no como *Stuxnet* en el que se necesitaba programarse para realizar de manera automática ciertas funciones.

Dicha información era guarecida en un archivo local ligeramente encriptado y comprimido, el cual debía ser extraído sin demasiada demora, ya que luego de treinta días el virus era automáticamente sustraído del sistema, aunque dejando a su paso *puertas traseras*[115] para poder acceder posteriormente al sistema con mayor facilidad. El funcionamiento de los datos recogidos era utilizarlos para poder efectuar un ataque en cualquier momento y de esa manera destruir cualquier red.

---

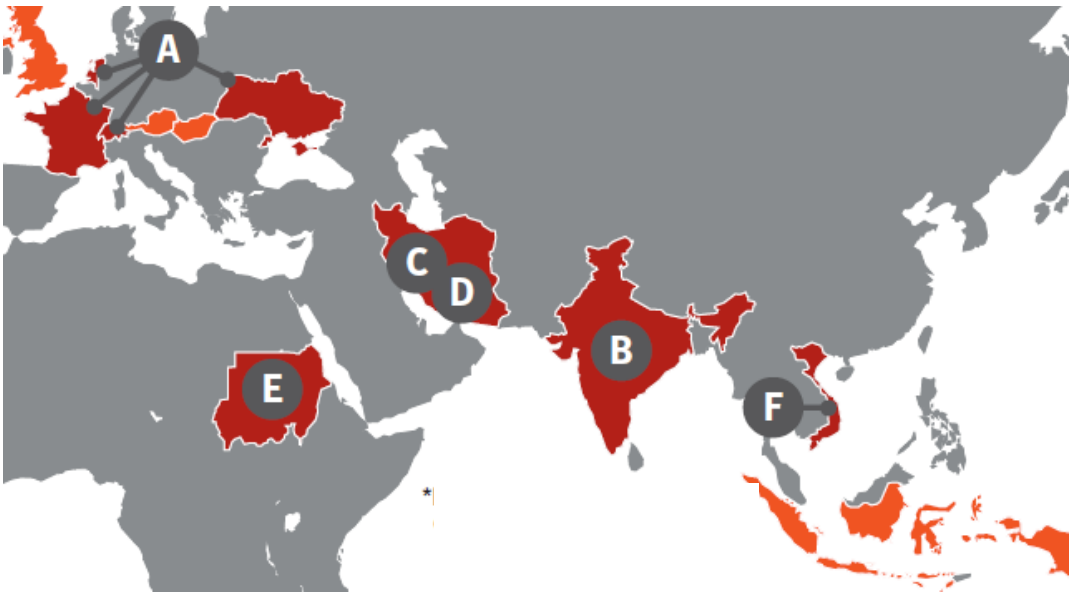
[114] *Cfr*. *Symantec. Security Response*, "W32.Duqu The precursor to the next *Stuxnet*" [en línea], Dirección URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_*Stuxnet*.pdf, [consulta: 21 de marzo de 2014].

[115] *Software* no autorizado, añadido de forma maliciosa a un programa, para permitir el ingreso sin autorización en una red o un programa de *software*. Con frecuencia, después de haber conseguido por primera vez un sistema, un ciberdelincuente o ciberguerrero deja instalada una puerta trasera que le permitirá en el futuro acceder de forma más fácil y rápida. Los programas de esta clase reciben también el nombre de <<troyanos>>, por el legendario caballo de Troya.

En el siguiente mapa se muestran los resultados de un informe realizado por el centro de investigación Symantec, en donde se muestra que, hasta el año 2011, fueron confirmados ataques de *Duqu* en seis organismos (representados con letras) de ocho países, y no confirmados en cuatro más. Las naciones cuyos agravios han sido corroborados son: Francia, Países Bajos, Suiza, Ucrania, India, Irán, Sudán y Vietnam; mientras que los que no han sido ratificados se han suscitado en Austria, Hungría, Reino Unido e Indonesia[116].

Mapa 2

Ataques realizados por el virus Duqu hasta 2011



Fuente: *Symantec. Security Response*, "W32.Duqu The precursor to the next Stuxnet" [en línea], Dirección URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_Stuxnet.pdf, [consulta: 21 de marzo de 2014].

De acuerdo con Michael Sconzo, oficial superior de seguridad de la División de Seguridad de la Corporación EMC, empresa dedicada a la criptografía y al *software* de seguridad, aún no existe nada posible que se pueda hacer para detener un ataque *Duqu*.

[116] *Cfr. Symantec. Security Response*, "W32 Duqu. The precursor to the next *Stuxnet*", [en línea], *op. cit.*

Otros dos virus desarrollados por Estados Unidos han sido *Flame* y *Gauss*, el primero de ellos fue descubierto en mayo de 2012, sus asaltos han sido reportados en un total de quince países: Irán, Israel, Sudán, Siria, Líbano, Arabia Saudita, Egipto, Cisjordania, Hungría. Austria, Rusia, Hong Kong y Emiratos Árabes Unidos[117], pero los primeros siete Estados son los que han recibido el mayor número de agravios.

Mapa 3

Países más afectados por ataques Flame

Irán 189	Israel Palestina 98	Sudán 32	Siria 30	Líbano 18	Arabia Saudita 10	Egipto 5

Fuente: *Kaspersky Lab Experts*, "The Flame: Questions and Answers", [en línea], 28 de mayo de 2013, Dirección URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, [consulta: 11 de febrero de 2014].

Lo que lo diferencia de los virus anteriores es que su capacidad de robar documentos es mucho más avanzada, ya que no sólo lo lleva a cabo mediante extracción de bases de datos, sino que lo puede realizar de diferentes maneras como capturas de pantalla, grabaciones de audio desde el micrófono, intercepción

[117]*Cfr*. *Phys Org*, "Flame virus linked to *Stuxnet*: researchers", [en línea], Dirección URL: file:///C:/Users/Emmanuel/Downloads/2012-06-cybersleuths-link-flame-*Stuxnet*.pdf, [consulta: 21 de marzo de 2014].

de teclado, entre otras[118], esto, con la finalidad de recabar información sobre las operaciones de los Estados (principalmente de Medio Oriente), buscando cualquier información útil escondida entre correos electrónicos, mensajes, documentos, etc.

El último *malware* encontrado que lleva la firma implícita estadounidense es *Gauss*, descubierto en junio de 2012 por el Laboratorio Kaspersky, compañía global especializada en protección informática, y al igual que *Flame*, este programa dañino fue distribuido activamente a lo largo de varios países de Medio Oriente, principalmente en Líbano[119].

Así como *Duqu* y *Flame*, *Gauss* fue diseñado para apropiarse de la mayor cantidad de información de aquellos sistemas que infecta, sin embargo, se le debe de añadir algunos métodos para realizar su tarea, tales como "[…] robo de contraseñas para diversos sistemas bancarios, redes sociales, correo electrónico, mensajería instantánea de cuentas; […] intercepción de datos de sesión, cookies, contraseñas e historial del navegador"[120].

En el siguiente cuadro se muestran las principales características que poseen los altercados digitales estadounidenses, la forma en que instala los virus y los ejecuta, los objetivos que pretende alcanzar, así como algunos ejemplos de sus acciones.

[118]*Cfr*. s/a, *Kaspersky Lab Experts,* "The Flame: Questions and Answers", [en línea], 28 de mayo de 2013, Dirección URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, [consulta: 11 de febrero de 2014].
[119]*Cfr*. Boldizsár Bencsáth, Gabor Pék, *et. al., "The Cousins of Stuxnet: Duqu, Flame, and Gauss",* [en línea], Dirección Url: *https://www.mdpi.com/1999-5903/4/4/971/*pdf, [consulta: 11 de febrero de 2014].
[120]*Ídem.*

Figura 8

Características de ciberataques estadounidenses

Exploración	Posibles fuentes de obtención de información secreta
Militarización	Medios extraíbles infectados
Entrega	Bus Universal en Serie (USB, Universal Serial Bus)
Aprovechamiento	Uso de los medios de ingeniería social universales para la transmisión de datos (USB Media Use)
Instalación	Gusano, control de acceso remoto
Mando y Control	Criptografía/Establecimiento de un enlace encriptado entre un servidor y un cliente, por lo general un servidor web y un navegador (SSL)
Objetivos	Recopilación de información/Interrupción sutil del sistema (Centrados en Medio Oriente)
Modelos de tácticas, técnicas y procedimientos	*Stuxnet, Flame, Duqu* y *Gauss*

Fuente: Elaboración propia con datos de Kenneth Geers, Darien Kindlund, *et. al*., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, [en línea], Dirección URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf, [consulta: 29 de enero de 2014].

Una característica común de *Stuxnet, Duqu, Flame*, y *Gauss*, aparte de que la mayoría de los objetivos han estado localizados en la región de Medio Oriente, es que todos ellos estuvieron activos por un período prolongado que abarcaba entre un año o dos antes de que fueran descubiertos, a pesar de la enorme cantidad de computadoras que fueron infectadas por ellos.

Aunque Estados Unidos es el principal sospechoso de ser el padre de estos programas, los mismos estadounidenses están preocupados de que gusanos como *Stuxnet, Duqu, Flame* y *Gauss* sean utilizados en su contra y las consecuencias se traduzcan en la destrucción de infraestructura vital para el país. Debido a que el país norteamericano maneja cada uno de sus movimientos por medio de computadoras, es un blanco extremadamente atractivo.

2.3.2.3. República Popular Democrática de Corea

A pesar de que Corea del Norte es considerado por muchos países como un actor internacional extravagante y hermético que aún vive en la era de piedra, esta nación ha sido capaz de utilizar las ventajas de la red para llevar a cabo, con gran éxito, varios ataques cibernéticos contra diversas naciones, los cuales iniciaron en el 2009 con Estados Unidos y Corea del Sur.

El 4 de julio, una de las fechas más importantes para los ciudadanos estadounidenses, estuvo marcado por varias actividades realizadas por Corea del Norte, iniciando con la detección de varios cohetes lanzados hacia el mar, siete en total; expertos señalan que la principal razón de tal acción fue llamar la atención, ya que en "[…] el pasado ésa había sido la pauta […]: el país amenazaba, obtenía atención, ofrecía una muestra de las cosas terribles que podrían pasar, luego se ofrecía a dialogar y finamente negociaba un acuerdo que enriquecía sus cofres"[121]. Sin embargo, esta vez no sucedió de esa manera, porque las agresiones en vez de detenerse, se trasladaron al ciberespacio.

Ese día, desde muy temprano, un Ataque de Denegación de Servicio, DDoS, fue lanzado contra diversas páginas electrónicas estadounidenses pertenecientes al Departamento de Seguridad Nacional, al Departamento de Estado, el Servicio Secreto, la Comisión Federal del Comercio, el Departamento de Transporte, la NASDAQ (la bolsa de valores electrónica más grande de Estados Unidos), la Bolsa Mercantil de Nueva York, la Bolsa de Valores de Nueva York, el Washington Post, a diferentes compañías internacionales e incluso a la Casa Blanca[122], aunque ése último fracasó.

El asalto a Estados Unidos duró una semana, desde el cuatro de julio hasta el diez, y durante esos días, las miles de solicitudes por segundo que fueron recibidas en esas páginas causaron su inminente colapso. Pero a partir del décimo día, los agravios ya no eran únicamente hacía la potencia estadounidense, sino

[121] Richard A. Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, p. 44.
[122] *Ibídem*. p. 46.

que llegaron noticias acerca de que Corea del Sur también comenzaba a ser atacada.

Páginas de bancos y organismos gubernamentales comenzaron a ser inundadas con miles de peticiones de acceso, no obstante, los daños se lograron contener en poco tiempo. Después del incidente, Estados Unidos no quiso realizar ninguna señalización directa hacia Corea del Norte hasta conseguir las pruebas suficientes, sin embargo, Corea del Sur no tuvo miramiento alguno para apuntar a su vecino como autor de los asaltos, es por ello que el gobierno surcoreano adelantó sus planes acerca de la construcción de un mando para la Ciberguerra, el cual sería construido en 2012, pero después de esos sucesos, el proyecto se adelantó dos años.

Desertores norcoreanos han hablado sobre un floreciente departamento de guerra cibernética, el cual cuenta con un personal formado por 3,000 individuos, en gran parte capacitados en China y Rusia. Según ellos, Corea del Norte está muy interesado en mejorar esos ataques debido a que es una manera muy eficaz de enfrentar a sus enemigos convencionalmente superiores[123].

Es probable que ese cibercomando esté formado por las cuatro unidades especiales con las que cuenta el país: la Unidad 110, sospechosa de haber cometido los agravios en contra de Corea del Norte y Estados Unidos; Unidad 121, para la ciberguerra del Estado Mayor del Ejército Popular de Corea (EPC), la más grande de todas, especializada en la desactivación del mando, control y redes de comunicaciones militares de Corea del Sur; Unidad 204, para la ciberguerra psicológica del Departamento Secreto Enemigo especializado en los ciber elementos de la guerra de información y Unidad 35 del Departamento de Investigaciones del Partido Central, el más pequeño[124].

[123]*Cfr.* Kenneth Geers, Darien Kindlund, *et. al*., World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, *op. cit*., p. 9.
[124]*Cfr.* Richard A. Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, p. 50.

Cada una de ellas tiene miembros trabajando desde varios países como China, asentados en ciudades como Dandong y Sunyang, ambos puntos ubicados cerca de la frontera compartida entre las dos naciones, esto sucede debido a que en Corea del Norte serían identificados rápidamente porque las conexiones con las que cuenta el Estado son muy escasas.

A pesar de que cada una de esas unidades tiene funciones específicas, en términos generales, lo que busca Corea del Norte es recolectar la mayor cantidad posible de información clasificada de sus enemigos para poder usarla a su favor y así tener una posición más favorable en situaciones como negociaciones diplomáticas, futuros cambios políticos o cualquier eventualidad que se llegara a presentar.

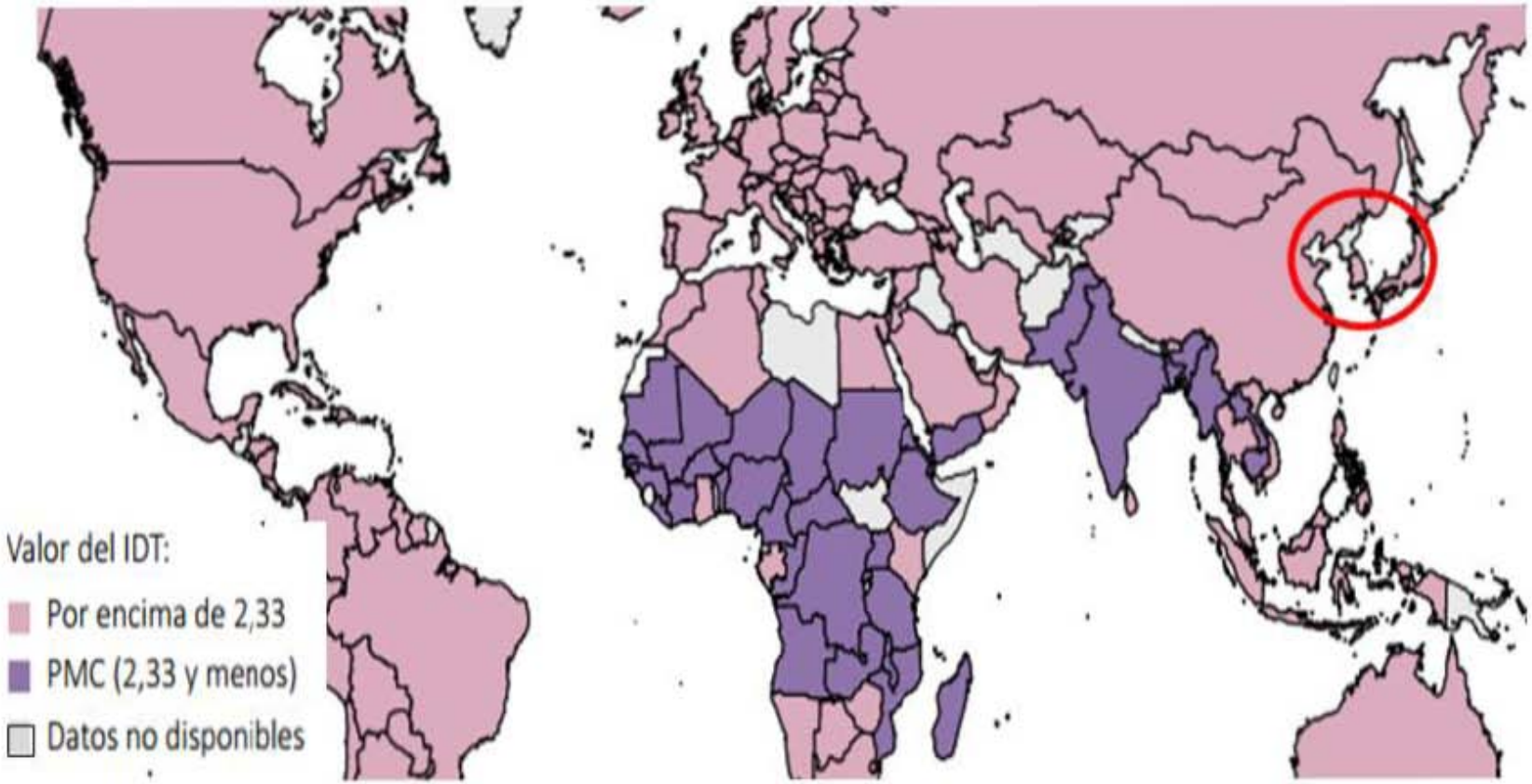
Para conseguir todo eso, el gobierno norcoreano busca tener a personas sumamente capacitadas en sus unidades, y lo realiza seleccionando estudiantes notables en escuelas primarias para adiestrarlos y convertirlos en *hackers*, ofreciéndoles formación en programación y durante la secundaria, después matriculándolos en la Universidad del Mando Automatizado en Pyongyang, donde su objetivo es aprender la manera de penetrar las redes enemigas[125].

Lo que puede resultar significativo es "[…] la capacidad de Corea del Norte para ejecutar un ataque cibernético bastante sofisticado a pesar de su estatus como una de las naciones más atrasadas del mundo"[126]. Incluso en los informes sobre "Medición de la Sociedad de la Información" realizados por la Unión Internacional de Telecomunicaciones (UIT) de la ONU en donde se mide el índice del Desarrollo de las TIC (IDT), los datos sobre la tecnología norcoreana son prácticamente nulos, como se puede observar en el siguiente mapa.

[125] *Ibídem*, p. 51.
[126] Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.,* p. 36. Traducción propia.

Mapa 4

Países menos conectados en el 2012



Fuente: Elaboración propia con datos de Unión Internacional de Telecomunicaciones, *Medición de la Sociedad de la Información*, [en línea], 2013, Dirección URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013-exec-sum_S.pdf, [consulta: 28 de marzo de 2014].

Otras fuentes, apuntan que de los veinticuatro millones de habitantes, menos de veinte mil tiene teléfonos móviles, y en cuanto a la radio y televisión, únicamente se pueden sintonizar los canales gubernamentales oficiales. Cuenta con muy pocas páginas electrónicas con la capacidad de comunicarse con el extranjero, en donde la mayoría sólo tienen información sobre su vecino. Sólo a ciertos negocios occidentales se les permite tener acceso a Internet, y la población en general sólo cuenta con una red muy limitada, que sirve prácticamente para visitar el sitio electrónico del líder norcoreano[127].

Aunque, en este caso, la falta de tecnología se podría tomar como un plus muy importante para el país asiático, pues si se llegara a dar el caso de que los países atacados por Corea del Norte quisieran responderle de la misma manera, se encontrarían con la disyuntiva de no tener grandes opciones para hacerlo, porque no posee muchos blancos que puedan ser utilizados para un ciberataque. Esa es la principal razón por la cual el país representa una gran amenaza para Estados más desarrollados como Estados Unidos o Corea del Sur.

2.3.2.4. República Popular China

A principios del 2013 el Estimado Nacional de Inteligencia (NIE), quien representa a la comunidad de inteligencia de mayor autoridad en Estados Unidos y evalúa determinados problemas de seguridad nacional, identificó a China como la nación más agresiva para varios países, especialmente para la potencia estadounidense[128], debido a que en innumerables ocasiones ha tratado de penetrar sus sistemas empresariales y gubernamentales con la intención de reunir datos útiles para obtener beneficios económicos y tecnológicos en un futuro.

---

[127]*Cfr.* Richard A. Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, pp. 49-50.

[128]*Cfr.* Ellen Nakashima, "U.S. said to be target of massive cyber-espionage campaign", [en línea], Estados Unidos, *The Washington Post*, 10 de febrero de 2013, Dirección URL: http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html, [consulta: 30 de marzo de 2014].

Varios autores, como Robert Lai, Rahman Syed, James A. Lewis, Kenneth Lieberthal, entre otros especialistas en el tema de ataques cibernéticos chinos, han señalado al país como el más activo en ciber espionaje, incluso algunos lo consideran como el primer actor internacional en usar este tipo de agravios para llevar a cabo objetivos políticos y militares[129]. China quiere reunir suficiente información política, militar, económica y científica para acortar la disparidad tecnológica que la separa de las naciones más adelantadas y de esa manera acelerar el crecimiento de sus industrias civiles y militares.

Los primeros asaltos que realizó China ocurrieron a finales de la década de los años noventa[130], el primero de ellos en 1998 contra Indonesia, inducido por un sentimiento de indignación nacional debido a disturbios realizados por la población local contra los chinos; como respuesta a ello, un grupo auto organizado de 3,000 hackers comenzaron a lanzar ataques contra páginas gubernamentales en protesta por los altercados sucedidos. El siguiente agravio fue llevado a cabo en 1999 por la Alianza Roja de Hackers Chinos contra sitios electrónicos estadounidenses, esto sucedió a causa de un bombardeo accidental hacia la embajada china en Belgrado por la OTAN.

Sin embargo, esos altercados podrían verse como "inocentes" en comparación con los que realizó tiempo después. Como se ha mencionado, los ataques que ha efectuado China han sido incalculables, pero han sido cuatro de ellos los que han ocasionado mayores secuelas: *Titan Rain*, *Aurora*, *Night Dragon* y *Shady RAT*.

El primero de ellos, *Titan Rain*, fue lanzado en el año 2002, su objetivo fue penetrar en los sistemas pertenecientes al Laboratorio Nacional Sandia[131], uno de los laboratorios más importantes de investigación y desarrollo del Departamento de Energía de Estados Unidos, esto con el fin de sondear la

[129]*Cfr*. Laura Saporito, James A. Lewis, *Cyber Incidents Attributed to China*, [en línea], Dirección URL: http://csis.org/files/publication/130311_Chinese_hacking.pdf, [consulta: 1 de abril de 2014].
[130]*Cfr*. Jeffrey Carr, Inside Cyber Warfare, *op. cit.*, p. 2.
[131]*Cfr*. Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit*, p. 32.

seguridad de las redes y encontrar sus vulnerabilidades para un posterior ataque. Este acto es considerado como uno de los más sofisticados, ya que la inmersión a las redes se realizó sin cometer un solo error.

Una vez que la recolección de datos comenzó, éstos eran enviados a computadoras ubicadas en Corea del Sur, Hong Kong y Taiwán, desde estos puntos eran reenviados a la provincia de Cantón ubicada al sur de China[132]. El agravio no fue descubierto sino hasta el 2007, por lo que el robo de datos se mantuvo a lo largo de cinco años, sin que las autoridades estadounidenses se percataran de ello.

El segundo asalto, *Aurora*, fue lanzado en enero de 2010 contra los sistemas de Google, quien anunció en junio del mismo año que información sustancial había sido robada y que entre los datos sustraídos se encontraba el llamado "código fuente" de su programa *Gaia*, es decir, la médula o el ADN virtual[133] que podía ser utilizado para encontrar con mayor facilidad las vulnerabilidades de Google y así poder realizar un ataque en cualquier momento.

Asimismo, usuarios de Google fueron atacados con programas maliciosos introducidos en un correo, aparentemente inofensivo, con el fin de permitir el acceso de manera remota a sus computadoras y extraer información valiosa. Entre las víctimas se encontraron altos funcionarios del gobierno estadounidense, activistas políticos chinos, oficiales en varias naciones de Asia (principalmente en Corea del Sur), militares y periodistas.

Sin embargo, *Aurora* también fue dirigida contra Microsoft, Hotmail, Yahoo, Adobe Systems, Juniper Networks, Rackspace, Dow Chemical, Morgan Stanley, Northrop Grumman y Symantec. "La campaña Aurora puede ser vista como una especie de reconocimiento u operación de espionaje en la cual ciber expertos

[132] *Ídem.*
[133] *Ibídem.* p. 33.

chinos reunieron información sobre competidores. […] Y la información reunida puede ser empleada para mejorar la competitividad económica de China"[134].

El tercer agravio, *Night Dragon* fue difundido el mismo año que *Aurora*, simplemente unos meses después. Este ataque estuvo dirigido hacia empresas globales de petróleo, energía y compañías petroquímicas; al inicio de las investigaciones se sospechaba de varios actores internacionales, sin embargo, después de una exhaustiva indagación, McAfee, compañía estadounidense dedicada a la seguridad informática quien estaba a cargo, rastreó la dirección de los altercados, la cual se dirigía a la provincia china Shandong[135].

El último es conocido como *Shady RAT* (*Remote Access Tool*), así como sus antecesores, la principal razón de su creación fue "el hambre masiva" de información secreta y propiedad intelectual. En esta ocasión fueron un total de setenta víctimas ubicadas en catorce países diferentes, y al igual que *Aurora*, consistió en el envió de correos electrónicos que en el momento en que éstos eran abiertos, de forma automática un virus era descargado en los sistemas.

La pauta de todos estos ataques no sólo es el robo de información confidencial militar, económica, científica y tecnológica perteneciente a gobiernos y empresas internacionales, sino también que detrás de todas esas hostilidades estuvo el grupo de *hackers* más importantes de China: *Comment Crew*, famoso no sólo por haber llevado a cabo todos los asaltos que fueron mencionados anteriormente, sino que ha sido el autor de muchos otros, la mayoría lanzados contra Estados Unidos.

[134] *Ibídem.* p. 34.
[135] *Cfr.* Laura Saporito, James A. Lewis, Cyber Incidents Attributed to China, *op. cit.*, p.3.

Figura 9

Características de ciberataques chinos

Exploración	Listas de correos/Rastreo/Minar redes sociales
Militarización	Archivos ejecutables (EXE) disfrazados para que aparezcan como formatos de archivo no ejecutable
Entrega	Direcciones electrónicas (URL) insertados en correos
Aprovechamiento	Día cero/Aplicación de vulnerabilidades
Instalación	Alta especificidad, compactar la tecnología de acceso remoto con una mínima capacidad de evasión
Mando y Control	Protocolo de transferencia de hipertexto con incrustación, codificaciones estándar, junto con codificaciones personalizadas
Objetivos	Recopilación de información/Espionaje económico, acceso persistente
Modelos de tácticas, técnicas y procedimientos	*Comment Group*

Fuente: Kenneth Geers, Darien Kindlund, *et. al*., *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*, [en línea], Dirección URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf, [consulta: 29 de enero de 2014].

Es importante mencionar las fuentes que han inspirado las estrategias que ha seguido China en cada uno de sus ataques, las cuales son una colección de sus teorías, doctrinas y metodologías[136]. Éstas incluyen:

1. Sun Tzu y el arte de la guerra;
2. Estrategias y tácticas de Mao;
3. Go, un juego estratégico;
4. El concepto de artes marciales del Tao;
5. Razonamiento de abducción.

[136] Robert Lai, Syed Rahman, *Analytic of China Cyberattack*, [en línea], Dirección URL: http://airccse.org/journal/jma/4312ijma04.pdf, [consulta: 1 de abril de 2014].

En conjunto, cada uno de estos elementos aplicados a la Ciberguerra han enseñado a China cómo golpear al enemigo cuando se encuentra más vulnerable, analizar la situación, visualizar un plan de acción contra contrincantes imaginarios antes de un combate real, utilizar métodos sencillos cuando se enfrenta a un oponente más poderos, entre otros. Es claro que esto ha funcionado mucho para dicha nación, ya que la mayoría de sus acometidas han sido efectivas y con un alto grado de complejidad.

Uno de los actores más conscientes sobre esta situación es Estados Unidos, ya que ha sido uno de los blancos más constantes no sólo para China, sino también para muchos actores internacionales, debido a su situación de nación más vulnerable hacia este tipo de altercados digitales.

3. Estados Unidos: la potencia amenazada

El siglo XX estuvo marcado por múltiples acontecimientos que fueron cambiando el rumbo de la sociedad internacional de manera constante. Durante este periodo, hechos tan importantes como la Primera y Segunda Guerras Mundiales, la llamada Guerra Fría, la implosión de la URSS, el auge de la Mundialización y Globalización entre muchos otros, tuvieron lugar a lo largo y ancho del mundo. Estos eventos, representaron grandes transformaciones para múltiples naciones, entre ellas Estados Unidos.

Para efectos de esta investigación es importante definir los términos de Globalización y Mundialización, ya que se tiende a utilizarlos de manera errónea. El Dr. Edmundo Hernández-Vela define al primero como aquel fenómeno

> […] de naturaleza o base física que abarcan todo el globo terráqueo, como el de las *telecomunicaciones*, la *informática* y las redes de *información*. Término inapropiado para referirse a los procesos de carácter eminentemente social de tendencia, alcance o extensión mundial, como el uso y contenido de las propias telecomunicaciones y redes de información, incluyendo la *Internet* y la telaraña mundial de redes, que están y son mejor comprendidos en la *mundialización*[137].

Mientras que Mundialización lo explica como el

> Proceso permanente, continuo e incrementadamente complejo, inherente a la humanidad y por lo tanto característico de su evolución y *desarrollo,* de extensión y generalización creciente y progresiva a todo el mundo de fenómenos y sucesos de naturaleza eminentemente humana de muy diversa índole conforme van surgiendo en alguna parte del planeta.
> Esta cuestión ha alcanzado enorme notoriedad y significación debido a la aceleración e intensificación que le han imprimido los recientes adelantos científico-tecnológicos, muy especialmente los enormes avances alcanzados en los campos de la *informática* y las *telecomunicaciones,* y se

[137] Edmundo Hernández-Vela Salgado, Diccionario de Política Internacional, *op. cit.*, pp. 501.

> manifiesta esencialmente en la pretendida existencia formal de un mercado libre mundial y una *sociedad de la información* del mismo rango, e influye en la conducta, las relaciones y la toma de decisiones, políticas y acciones de los sujetos de la *sociedad internacional*.
> La *mundialización* no afecta solamente las estructuras y el funcionamiento de la economía mundial, también modifica, profundamente, los modos de vida de las poblaciones y los sistemas de *información* de los habitantes de todo el pueblo planetario[138].

Desde principios de este siglo, Estados Unidos se fue ubicando como un actor sumamente importante dentro de la escena internacional, con un gran poderío político, económico y militar; el término de la Segunda Guerra Mundial perfiló la hegemonía norteamericana sobre el bloque capitalista, "[e]l predominio estadounidense reposaba sobre tres pilares: su superioridad tecnológica y económica […], el aumento de su prestigio político en el mundo […] [y] por su potencia militar […]"[139].

Pero su auto pronunciamiento como única potencia se produjo a principios de la década de los noventas, cuando finalizó el enfrentamiento bipolar entre el bloque capitalista y el socialista al colapsar la Unión de Repúblicas Socialistas Soviéticas (URSS), a partir de ese momento se posicionó como "[…] un gendarme mundial para organizar el mundo según sus conveniencias e intervenir militarmente allá donde sus intereses son vulnerados"[140].

Era impensable imaginar que alguien de manera individual o en coalición pudiera llegar a tener el poder y agallas suficientes como para encarar su hegemonía, ya que desde el final de la Guerra Fría casi todos sus rivales se habían mantenido

[138] Edmundo Hernández-Vela Salgado, *Diccionario de Política Internacional*, México, Porrúa, Tomo II, 2002, Sexta Edición, pp. 675-680.
[139] s/a, "El Mundo Capitalista. Desde la finalización de la Segunda Guerra Mundial al Siglo XXI. Los Estados Unidos, líder del mundo capitalista", [en línea], Dirección URL: http://www.iesdionisioaguado.org/joomla/Distancia/HMC/Tema15.pdf, [consulta: 20 de abril de 2014].
[140] *Ídem.*

de una u otra forma en una relación no beligerante[141]; sin embargo, fuera de todo pronóstico, a principios de este siglo, la seguridad y superioridad estadounidense fueron altamente cuestionadas.

3.1. Terrorismo, prioridad desplazada

El 11 de septiembre del 2001, el mundo entero quedó paralizado cuando comenzaron a esparcirse las primeras noticias sobre un atentado ocurrido en territorio estadounidense: las Torres Gemelas de Nueva York habían sido blanco de un ataque perpetuado por un conjunto de terroristas que conformaban una red llamada Al-Qaeda, por medio del secuestro de varios aviones que fueron impactados contra objetivos estratégicos, entre ellos el Pentágono, dejando un saldo de 2,792 muertos y más de 6,000 heridos[142].

Desde ese momento, la idea de que el terrorismo debía ser uno de los principales temas en la agenda de seguridad internacional no fue planteada únicamente por países, sino también por organismos internacionales. Es por eso que el Consejo de Seguridad (CS) de la Organización de las Naciones Unidas aprobó, pocos días después del atentado, la Resolución 1373, la cual expresa su determinación por prevenir todos los actos de ese tipo, ya que constituyen una amenaza para la paz del mundo y exhorta a todas las naciones a no contribuir con ese tipo de actividades, de manera directa o indirecta.

El once de septiembre trajo consigo "[…] un nuevo orden político-jurídico internacional, la aparición de un nuevo fenómeno: el terrorismo global"[143], el cual

---

[141]*Cfr*. Paul T.V., *Las potencias en ascenso y el equilibrio del poder en el siglo XXI*, [en línea], Dirección URL: http://www.sre.gob.mx/revistadigital/images/stories/numeros/n94/paul.pdf,[consulta: 20 de abril de 2014].

[142]*Cfr*. Laurence Thieux, *El terrorismo internacional: causas e implicaciones estratégicas*, [en línea], Dirección URL: http://biblioteca2012.hegoa.efaber.net/system/ebooks/15197/original/El_Terrorismo_Internacional._Causas_e_Implicaciones_Estrategicas.pdf, [consulta: 25 de abril de 2014].

[143] Pablo César Revilla Montoya, *El terrorismo global. Inicio, desafíos y medios político-jurídicos de enfrentamiento*, [en línea], Dirección URL: http://biblio.juridicas.unam.mx/revista/pdf/DerechoInternacional/5/art/art12.pdf, [consulta: 22 de abril de 2014].

terminó por convertirse en la amenaza más importante en la que se basarían las acciones que se realizarían a partir de ese punto. A pesar de que el terrorismo *per se*, no era un fenómeno nuevo, ya que se remontaba desde la Revolución Francesa con el "Régimen del terror", la característica de alcance global sí lo era, la diferencia entre uno y otro radica en su magnitud mundial y su capacidad para desestabilizar un régimen político en un solo día, poniendo en peligro la paz y la seguridad internacional[144].

Una de las medidas más importantes que tomó el gobierno estadounidense posterior a los agravios ocurridos en Nueva York, fue la famosa Doctrina Preventiva, invocada por el presidente George W. Bush el 20 de septiembre de ese mismo año ante el Congreso, dicha doctrina manifiesta que se atacará no sólo a los grupos terroristas, sino también se les dará caza a todas aquellas naciones que proporcionen ayuda o refugio a dichos trasgresores, antes de que se pueda configurar por completo cualquier movimiento en contra de la seguridad nacional de Estados Unidos.

Asimismo, se manifiesta que "EE.UU trataría de conseguir el respaldo internacional, pero que actuaría por su cuenta si los intereses estadounidenses y las responsabilidades 'singulares' adquiridas así lo requerían"[145]. Esto se vio reflejado en el momento en que la potencia norteamericana, tomando como base dicha doctrina, dio inicio a la guerra contra el terrorismo al lanzar un ataque contra las bases de Al Qaeda en Afganistán el 7 de octubre de 2001; posteriormente, el 20 de marzo de 2003 dio comienzo la confrontación en Iraq.

Es importante mencionar que la primera de ellas contó con la legitimación del Consejo de Seguridad de la ONU, citando el artículo 51 de la Carta de dicha organización, el cual proclama el derecho a la legítima defensa en caso de haber

---

[144] *Ídem.*

[145]Martha Crenshaw, "La guerra contra el terrorismo: ¿están ganando los Estados Unidos*?"*, [en línea], *Terrorismo Internacional,* núm. 105, 2006, Dirección URL: http://www.realinstitutoelcano.org/analisis/1058/1058_Crenshaw_EEUU_Guerra_Terrorismo.pdf, [consulta: 27 de abril de 2014].

un peligro tangente para la seguridad de una nación; sin embargo, la segunda transgresión no obtuvo ningún respaldo de la comunidad internacional, por lo que se actuó únicamente de manera unilateral, con ayuda de alianzas creadas al margen de los marcos institucionales[146].

Otras naciones que fueron señaladas por tener vínculos con organizaciones terroristas, poseer armas de destrucción masiva y armas nucleares fueron: Irán y Corea del Norte, que junto con Iraq fueron bautizadas, por el ex presidente George W. Bush, *eje del mal*.

Además de la Doctrina Preventiva, hay otros documentos oficiales que explican de manera clara la respuesta estadounidense ante esa amenaza que, durante muchos años, estuvo en primer lugar en la lista de seguridad que se emite cada año, en la cual se exponen los principales riesgos a los que se enfrenta la potencia norteamericana:[147]

1. Estrategia de Seguridad Nacional de los Estados Unidos de América, septiembre de 2002;
2. Estrategia de Seguridad Nacional I, 2002;
3. Estrategia Nacional para Combatir el Terrorismo, febrero de 2003;
4. Estrategia de Seguridad Nacional II, marzo de 2006;
5. Estrategia Nacional para Combatir el Terrorismo II, septiembre de 2006.

También se deben de tomar en cuenta todos los cambios organizativos que se realizaron, tales como: la creación del Departamento de Seguridad Nacional (DHS, *Department of Homeland Security*), 2002; la reestructuración de la Agencia Nacional de Seguridad (NSA), 2002; y la fundación del Centro Nacional Antiterrorista (NCTC, *National Counter Terrorism Center*), 2004. Lo trascendental de todo esto es que Estados Unidos no había llevado a cabo una reorganización tan profunda desde el término de la Segunda Guerra Mundial, momento en el cual

[146] *Cfr*. Laurence Thieux, El terrorismo internacional: causas e implicaciones estratégicas, [en línea], *op. cit*.
[147] *Cfr*. Martha Crenshaw, "La guerra contra el terrorismo: ¿están ganando los Estados Unidos*?"*, [en línea], *op. cit*.

fueron creados el Departamento de Defensa (DoD, *Department of Defense*), 1947, y la Agencia Central de Inteligencia (CIA, *Central Intelligence Agency*), 1947[148].

A partir del 2009, con la elección de un nuevo presidente, la política antiterrorista tomó un giro importante; sin embargo, dicha amenaza siguió permaneciendo en el primer lugar de los peligros latentes contra la seguridad nacional estadounidense durante mucho tiempo. Incluso en un discurso que Barack Obama pronunció ante la Universidad Nacional de Defensa en mayo de 2013, hizo mención al terrorismo diciendo que la incertidumbre se encontraba en "[…] afiliados de Al Qaeda dañinos, pero menos capaces; amenazas a instalaciones diplomáticas, empresas del exterior [y] extremistas criados en casa. Ese es el futuro del terrorismo"[149].

No obstante, después de varios años, durante los cuales la lista de amenazas realizada por las agencias de seguridad de Estados Unidos se mantuvo intacta en lo que se refiere al primer puesto, un nuevo peligro comenzó a escalar lugares a una velocidad sorprendente; después de doce años, el terrorismo fue desplazado por los ataques cibernéticos, una nueva preocupación reclamaba el primer sitio y las prioridades estadounidenses comenzaron a cambiar.

A principios del 2013, varias fuentes de información como periódicos, páginas de internet, televisoras, etc., comenzaron a poner en primera página declaraciones que hablaban sobre este tema; entre los comunicados que surgieron ante este nuevo fenómeno se encuentra la del ex Secretario de Defensa, Leon Panetta, quien manifestó que dicha"[…] amenaza es tan seria que por primera vez desde los ataques terroristas a las Torres Gemelas del 11-S y dos años después de la

[148] *Ídem.*

[149]IIP Digital, "Presidente Obama habla sobre el futuro de la lucha contra el terrorismo*",* [en línea], Dirección URL: http://iipdigital.usembassy.gov/st/spanish/texttrans/2013/05/20130529148119.html#ixzz35cyoWPKN, [consulta: 23 de abril de 2014].

captura del líder de Al Qaeda, Osama bin Laden, el temor a sufrir un ataque informático ha suplantado al terrorismo internacional […]"[150].

Incluso varios expertos empezaron a mencionar el miedo que se tiene a recibir un *Pearl Harbor cibernético*, es decir, ser víctimas de un asalto imprevisto como sucedió en 1941 durante la Segunda Guerra Mundial cuando Japón atacó a la flota marina estadounidense; pero esta vez, se tiene la incertidumbre de que los blancos sean las infraestructuras principales del Estado: desde la bolsa de valores, el sistema de aeropuertos hasta plantas nucleares.

A pesar de todas las declaraciones realizadas, el comunicado se hizo oficial el 29 de enero de 2014, cuando se publicó la declaración de amenazas mundiales de este año (*Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community)*, realizado por James R. Clapper, Director de Inteligencia Nacional de Estados Unidos.

Dicho documento enlista dos tipos de amenazas: globales y regionales. La primera de ellas se encuentra conformada de la siguiente manera:[151]

1. Ataques cibernéticos;
2. Espionaje cibernético;
3. Terrorismo;
4. Armas de destrucción masiva y proliferación;
5. Espacio;
6. Crimen organizado transnacional;
7. Tendencias económicas;
8. Recursos naturales;

[150]Eva Saiz Escolano, "Los ciberataques sustituyen al terrorismo como primera amenaza para EE.UU" [en línea], periódico *El País*, sección "Internacional", 13 de marzo, 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html, [consulta: 17 de marzo de 2013].

[151]*Cfr*. James R. Clapper, *Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community*, [en línea], Estados Unidos, 29 de enero de 2014, Dirección URL: http://www.intelligence.senate.gov/140129/clapper.pdf, [consulta: 02 de mayo de 2014]. Traducción propia.

9. Riesgos para la salud;
10. Atrocidades masivas.

Así que el nuevo fenómeno de los ataques cibernéticos no solamente ocupa el primer lugar, sino los dos primeros, desbancando de esa manera al terrorismo que estuvo invicto por más de una década.

En este documento se menciona cuáles son las principales preocupaciones para Estados Unidos en torno a este tema, las cuales se componen, en primer lugar, por una serie de actores internacionales que representan un peligro para su seguridad nacional por diversas razones, estos sujetos son:[152]

1. Rusia, quien busca un cambio trascendental en el manejo de internet que pueda comprometer los intereses estadounidenses;
2. China, busca lograr un crecimiento económico y militar basándose en el robo de información;
3. Irán y Corea del Norte, calificados como actores impredecibles que buscan provocar la desestabilización de Estados Unidos junto con sus aliados;
4. Organizaciones terroristas, quienes utilizan la red para reclutar personal y continuar con la propagación de sus ideas;
5. Ciber organizaciones criminales, caracterizados por el robo de información y recursos económicos.

En segundo lugar, se hace mención a la infraestructura crítica, particularmente al Control de Sistemas Industrial (ICS, *Industrial Control System*) y a la Supervisión de Control y Adquisición de Datos (SCADA, *Supervisory Control and Data Acquisition*), encargadas de ejecutar tareas primordiales como distribución de gas, agua, electricidad, etc., no obstante, este tema será tratado con mayor profundidad más adelante.

El espionaje cibernético, el cual ocupa el segundo lugar en este inventario de amenazas, está íntimamente ligado al primero, debido a que agravios como robo

[152] *Ídem.*

de información económica y militar son realizados por naciones que ya se han mencionado, pero en esta parte se hace hincapié en que Rusia y China son los países que están a la cabeza de estos ataques.

Por otra parte, por primera vez, se declara que dentro del mismo territorio estadounidense existe un peligro importante: el robo de documentos a manos de personal, aparentemente de confianza, quien se aprovecha del acceso libre que posee hacia la vasta información clasificada con el único fin de divulgarla, ya sea siguiendo instrucciones propias u obedeciendo órdenes dictadas por gobiernos extranjeros.

Estados Unidos, al ser uno de los países más poderosos, hablando en términos económicos, políticos, militares, entre muchos otros; con intereses de todo tipo en cada rincón del planeta, se ha hecho acreedor a lo largo de su historia no sólo de amigos y aliados, sino también de enemigos, por lo que se ha encontrado (y se sigue encontrando) en la mira de muchos actores internacionales, quienes buscan despojarlo de su poderío aprovechando sus debilidades.

Ya sucedió una vez, se hizo temblar a la potencia en su propio territorio: Hawaii y Nueva York han sido testigos de ello; ahora es su infraestructura la que está siendo analizada por muchas naciones, buscando una pequeña oportunidad para poder usarla a su favor.

3.2. Medidas de seguridad

La incertidumbre constante que se presenta al no conocer en su totalidad las características del nuevo campo de batalla, ha obligado a las naciones a tomar diferentes medidas para salvaguardar su seguridad nacional, además, el que aún no exista una regulación internacional adoptada por los Estados complica más las cosas, es como si tuvieran que andar a ciegas, sin saber en realidad si el sendero tomado es el correcto o no.

No todos los países han reaccionado de la misma manera ante la proliferación de ataques cibernéticos, mientras unos apenas si han tomado medidas de seguridad,

otros ya han creado varias instancias gubernamentales para poder estudiar el problema y hacerse de las herramientas necesarias para enfrentar dicho fenómeno.

Tal es el caso de Estados Unidos, quien ha atravesado por un complicado proceso para poder contar hoy con las entidades gubernamentales que están a cargo de la seguridad cibernética, ha sido una ardua pelea entre la fuerza aérea, la marina y el ejército estadounidense donde el monopolio de la nueva guerra ha estado en juego. Asimismo, se ha impulsado la creación de nuevas especialidades en universidades estadounidenses con el fin de preparar a las nuevas generaciones para ser los siguientes guerreros cibernéticos.

3.2.1. Cambios organizacionales

Como se ha hecho referencia, fue la Guerra Fría el momento histórico que vio nacer la Internet, y desde ese entonces, Estados Unidos tuvo muy presente que esta herramienta se podía utilizar como arma de guerra, no por nada fue de los primeros en llevar a cabo varios ataques cibernéticos alrededor del mundo, sin embargo, fue hasta el 2003, cuando la importancia de la Ciberguerra comenzó a hacer mayor ruido dentro de las oficinas del Pentágono.

Para ese entonces, la fuerza aérea ya se había adelantado y había creado su propia unidad especializada en la Ciberguerra: el Cibermando de la Fuerza Aérea de Estados Unidos, acción que no fue bien recibida por el Pentágono ni por las demás unidades de guerra. Sin embargo, para ser más exactos, su incursión al fenómeno comenzó desde 1995, poco después de que se llevara a cabo la Primera Guerra del Golfo, cuando creó el Centro de Guerra Informática de la Fuerza Aérea (AFIWC)[153], del cual no se tiene mucha información.

La conducta de la fuerza aérea estadounidense estuvo caracterizada por el profundo anhelo de ser ellos quienes monopolizaran todos los aspectos de la guerra cibernética, y a pesar de que la marina y los servicios de inteligencia

[153]*Cfr.* Richard Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, pp. 58-59.

también deseaban ser los protagonistas, el deseo no iba a tales extremos como los primeros, quienes exponían públicamente un tema que, se consideraba, debía ser mantenido en secreto, diciendo que ellos eran los únicos capaces para hacer frente a un altercado de esa naturaleza, además, dejaban que la población civil viera al Pentágono como un eslabón débil, revelando que recibía miles de ataques cada hora, pero que eran ellos los que se encargaban de combatirlos.

Es por eso que en 2002 se decidió que el Mando Estratégico (STRATCOM, *Strategic Command*), encargado de la fuerza nuclear estratégica, sería el responsable de centralizar los recursos para la Ciberguerra[154]. Esta decisión fue apoyada por quienes deseaban que la lucha por el control de las nuevas contiendas terminara con la unificación de las tres unidades de combate en un solo organismo, mientras que otros la criticaban por miedo a que el tema fuese a durar sólo un par de meses.

Varios expertos en el tema decían que la manera más viable para combatir al nuevo fenómeno era trabajar en equipo entre las agencias de seguridad y los organismos militares estadounidenses, el problema era que éstos últimos estaban demasiado ocupados peleando entre sí, mientras que la guerra evolucionaba a pasos agigantados.

3.2.2. Creación del Cibermando

El caso es que, el fenómeno de la Ciberguerra no fue un tema de “tan sólo unos meses”, porque comenzó a tomar cada vez mayor fuerza a una velocidad sorprendente, nunca antes vista en cualquier otro tipo de guerra. Así que, pronto el STRATCOM no tuvo cabida para un fenómeno de tal magnitud, ni siquiera contaba con los conocimientos necesarios para hacer frente a alguna emergencia en caso de que se presentara.

Es por eso que Mike McConnell y Ken Minihan, ex directores de la Agencia Nacional de Seguridad (NSA), aconsejaron convertir a la NSA en el principal

[154] *Ibídem.* p. 60.

centro mundial en todo lo referente al conocimiento del ciberespacio, transformar a la Agencia en el nuevo Cibermando. Después de esta noticia, los desacuerdos por parte de algunos militares no se hicieron esperar; su discurso era que la NSA es una organización civil, por tanto, de acuerdo con la Ley de Estados Unidos, no cuenta con el respaldo legal para librar una guerra[155], lo único que le estaba permitido hacer era recabar información, por tanto, no podía meter las manos en ningún enfrentamiento y eso dejaba al país vulnerable.

La disputa por la manzana de la discordia, llevada a cabo entre el estamento militar y los representantes de la NSA, continuó hasta que en el 2006 se nombró a un nuevo secretario de Defensa, Robert Gates, ex rector de la Universidad de Texas A&M, quien en julio de 2009 ordenó al Mando Estratégico (STRATCOM), la creación de un Cibermando (USCYBERCOM o CYBERCOM, *United States Cyber Command*)[156].

El costo total del proyecto fue de 358 millones de dólares, el cual abrió sus puertas de manera oficial el 21 de mayo de 2010 en Meade, Maryland, bajo el mando del director de la NSA: el general Keith Alexander. Dicha instancia terminó con la riña entre las unidades de combate estadounidenses, ya que el Cibermando se describe a sí mismo como "[…] un mando sub-unificado, subordinado al Mando Estratégico de los EE.UU. que incluye el Ciber Mando del Ejército de Tierra (ARFORCYBER); el Ciber Mando de las Fuerzas Aéreas [(FLTCYBERCOM)] y el Ciber Mando de los Marines (MARFORCYBER)"[157].

De esa forma, la fuerza aérea, la marina y el ejército seguirían incursionando en la Ciberguerra, serían ellos los que actuarían en cualquier contienda que aconteciera, sólo que sus unidades serían dirigidas por el Cibermando. De igual manera, dicho organismo tendría completa libertad para consultar, en cualquier

[155] *Ibídem.* p. 63.
[156] *Cfr.* Illaro Eguskiñe Lejarza, "Estados Unidos-China: equilibrio de poder en la nueva Ciberguerra Fría", [en línea], *op. cit*.
[157] *Ídem.*

momento, todos los recursos con los que cuenta la Agencia Nacional de Seguridad.

De acuerdo con su hoja fundacional, su objetivo es:

> […] planificar, coordinar, integrar, sincronizar y conducir actividades tales como: dirigir las operaciones y la defensa de determinadas redes de información pertenecientes al Departamento de Defensa; conducir, cuando se le indique, operaciones militares de alto espectro para permitir acciones en todos los dominios, asegurándose que Estados Unidos y sus aliados tengan plena libertad de acción en el ciberespacio y negar los mismo a sus adversarios. […] [Así como] coordinar las operaciones del Departamento de Defensa, la prestación de apoyo a las misiones militares, […] y reunir los recursos existentes del ciberespacio […] para defender el entorno de seguridad de la información […] de interrupciones, intrusiones y ataques[158].

Sin embargo, la crítica que se le hace al Cibercomando es que habla de protección al Departamento de Defensa, apoyo al estamento militar, incluso a los aliados de Estados Unidos, pero nunca menciona un plan de acción o amparo para defender las infraestructuras civiles, la mayor vulnerabilidad de Estados Unidos y el punto de mira de muchos de sus adversarios.

Ex directores de la NSA piensan que a pesar de que esa tarea ha sido asignada al Departamento de Seguridad Nacional (DHS, *Homeland Security*) y ha realizado grandes avances en la protección de los blancos civiles, aún no cuenta con las capacidades necesarias para defender a la nación de grandes ataques, donde su infraestructura crítica resulte gravemente amenazada.

[158] US Departament of Defense, *U.S Cyber Command Fact Sheet*, [en línea], Dirección URL: http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf, [consulta: 03 de julio de 2014]. Traducción propia.

3.2.3. Educación, posible solución

Como muchas veces lo ha remarcado la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), la educación es el motor principal para cumplir muchos de los objetivos que cualquier nación se propone para su desarrollo, y en el caso de la Ciberguerra esto no es diferente, ya que Estados Unidos ha apostado por ella para aumentar su seguridad en contra de los ataques cibernéticos, el país ya ha puesto los cimientos para el surgimiento de nuevos soldados.

Ante esta nueva forma de hacer la guerra, surgió la necesidad de crear un nuevo tipo de ejército, es por eso que la fuerza física y una excelente condición física, son características que han perdido importancia, ahora lo que se busca son conocedores de las redes, que estén capacitados no sólo para bloquear cualquier tipo de ataque cibernético, sino también para arremeter contra las redes enemigas si fuera necesario.

A pesar de que los principios de la educación en seguridad cibernética se remontan desde 1995, con la creación del Centro de Guerra Informática por parte de la fuerza aérea de Estados Unidos[159], aún no se entendía plenamente las implicaciones de la Ciberguerra, no podían visualizar el alcance que podía tener un asalto a instalaciones de la nación, ni los daños que éste podría causar.

Fue hasta finales del 2010 cuando la Universidad de Maryland, junto con la Escuela Clark A. James de Ingeniería y la Facultad de Computación, Matemáticas, y Ciencias Naturales, decidieron crear el Centro de Ciberseguridad Maryland (MC2, *Maryland Cybersecurity Center*) bajo el mando del Dr. Jonathan Katz, profesor en Ciencias de la Computación.

El MC2 trabaja en conjunto con el gobierno, la industria y otras instancias académicas que, de una u otra manera, brindan valiosas aportaciones para el

[159]*Cfr*. Richard Clarke, Robert K. Knake, Guerra en la red. Los nuevos campos de batalla, *op. cit.*, p. 59.

desarrollo de los estudiantes que comienzan a interesarse por los estudios en seguridad cibernética.

Como su nombre lo dice, el centro se localiza en Maryland, lo cual significa una gran ventaja para el programa que maneja, ya que se encuentra muy cerca de lugares clave como la Agencia Nacional de Seguridad (NSA), el Cibermando estadounidense y el Instituto Nacional de Estándares y Tecnología, los cuales mantienen sus puertas abiertas para brindar apoyo a los estudiantes.

Otra ventaja que representa el sitio donde se localiza es que, al encontrarse tan cercano a la capital estadounidense, Washington D.C. puede aprovechar que más de la mitad del tráfico de Internet de toda la nación circula a través del área metropolitana de Washington[160], lo que significa una gran oportunidad para poner en práctica sus conocimientos.

Dicho centro está compuesto no sólo por expertos en Computación, Informática o Ingeniería, sino también por eruditos en materias como Economía, Derecho, Negocios Internacionales, entre muchas otras; esto con el fin de darle una visión más global al estudio del fenómeno, tratando no sólo los aspectos técnicos, sino comprender el escenario completo en el que se desenvuelve la Ciberguerra.

El objetivo principal que se tuvo para su fundación fue llevar a cabo nuevas investigaciones que abordaran temas concernientes a la seguridad cibernética, un tema que hasta esa fecha no se le había prestado la atención pertinente, además de brindar diversas actividades como talleres, campamentos, cursos, etc., a estudiantes de secundaria y preparatoria con el fin de darles a conocer el significado y la importancia que tiene este campo de estudio, desde los elementos más sencillos como las redes sociales, creación de contraseñas seguras, hasta hablarles de criptografía, el lenguaje secreto de los ordenadores.

Sin embargo, aún no se había abordado el tema del surgimiento de una licenciatura como tal, hasta que la empresa líder en seguridad global, Northrop

[160] Maryland Cybersecurity Center, *About the Maryland Cybersecurity* Center, [en línea], Dirección URL: http://www.cyber.umd.edu/about, [consulta: 26 de marzo de 2014].

Grumman, decidió donar en el 2013 una fuerte suma de dinero para la creación del programa Experiencia en Ciberseguridad Avanzada para Estudiantes (ACES, *Advanced Cybersecurity Experience for Students*), el cual quedó a cargo del Dr. Michel Cukier.

Dicho programa no es brindado a la comunidad universitaria de Maryland en general, sino que es impartido solamente en el Honors College, es decir, a estudiantes superdotados que son aceptados en este tipo de carreras por sus enormes aptitudes intelectuales, de hecho sólo son aceptados 45 alumnos cada año.

El programa consta de cuatro años de estudio, en los cuales los primeros dos años (ACES I) son introducidos al tema de la seguridad cibernética, tanto en aspectos técnicos como no técnicos, es decir, no sólo comienzan con materias como Física, Matemáticas o Ciencias de la Computación, sino también son introducidos a temas de Economía, Política, Derecho, entre otras, con el fin de tener una visión interdisciplinaria para poder desarrollarse de una mejor manera en el campo laboral.

Durante los dos últimos años, (ACES II), el aprendizaje es estrictamente técnico, y los estudiantes cuentan con programas avanzados e interacciones constantes en cenas, comidas, talleres y conferencias con expertos en la materia, líderes corporativos y gubernamentales, quienes juegan un papel no sólo de mentores, sino también de futuros contactos profesionales.

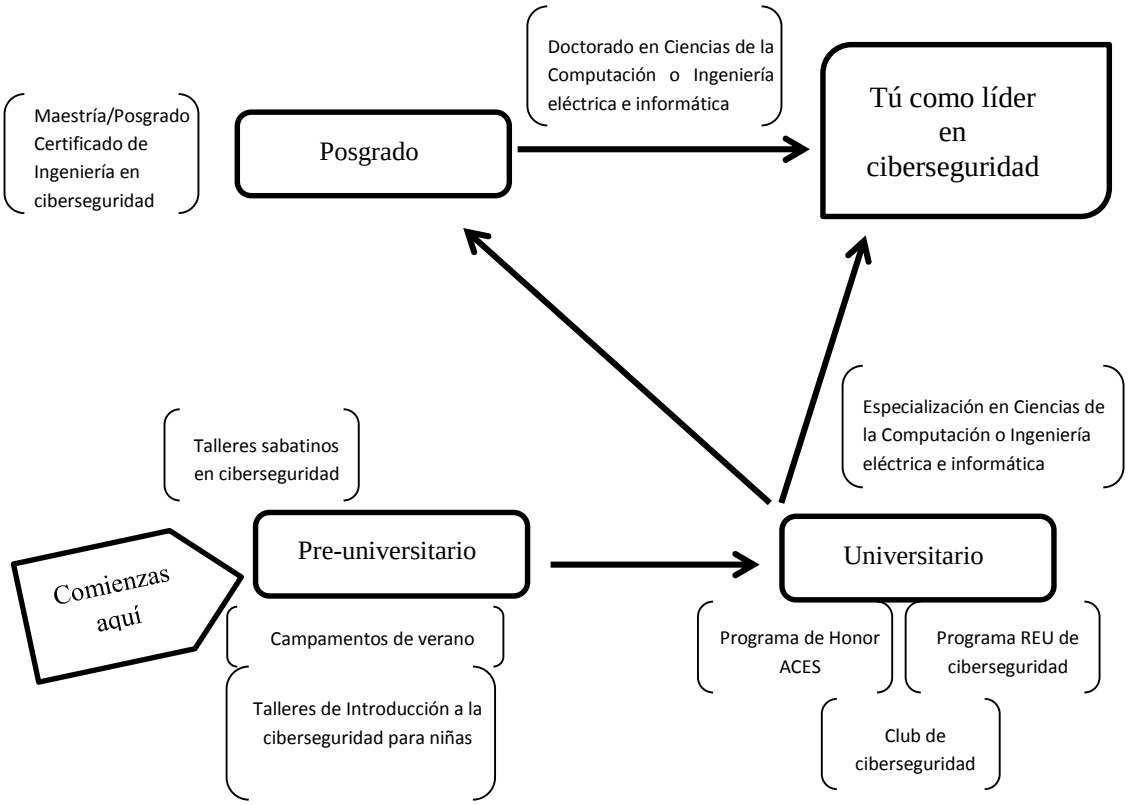
De igual manera, cuentan con amplias posibilidades para llevar el conocimiento a la práctica, como pasantías, programas de verano con agencias como la NSA, el Departamento de Defensa, empresas privadas como Parsons o Northrop Grumman e incluso pueden participar dentro de la misma Universidad de Maryland, en el CM2, o como mentores de las nuevas generaciones.

Al concluir los cuatro años tienen la opción de continuar con sus estudios en un Doctorado, ya sea en Ingeniería Informática o Ciencias de la Computación. El siguiente cuadro muestra cuál es el camino que se sigue para comenzar a

introducirse en este tema desde temprana edad hasta convertirse en un auténtico ciberguerrero.

Figura 10

Programa de educación en Ciberseguridad de la Universidad de Maryland



Fuente: Elaboración propia con datos de Maryland Cybersecurity Center, *Graduate Students*, [en línea], Dirección URL: http://www.cyber.umd.edu/education/grad, [consulta: 10 de julio de 2014].

La primera generación que saldrá de este centro se graduará en el 2017, sin embargo, ya se comienzan a ver los frutos del trabajo en equipo que ha realizado la triple hélice, es decir, la participación de las instancias educativas, el gobierno y el sector privado. Las tres esferas han trabajado conjuntamente en torno a un proyecto en común, brindado grandes aportaciones que en un plazo, no tan grande, serán enormemente recompensadas.

3.3. Debilidades de una potencia

Ocupar un lugar dentro de los países que son considerados potencias mundiales se traduce en que esas naciones cuentan con un alto desarrollo tecnológico, económico, militar y político, por lo que su poder de influencia es muy alto. Durante mucho tiempo, estos factores representaron una gran ventaja dentro de las guerras convencionales, ya que les conferían grandes oportunidades para salir airosos de las batallas.

Sin embargo, hoy en día, esa superioridad se ha transformado en grandes desventajas, los altos índices de desarrollo económico y tecnológico son vistos como vulnerabilidades colosales, que aunque cuenten con una superioridad militar desmedida, no se pueden eliminar.

3.3.1. Infraestructura crítica en la mira

Al contar con grandes adelantos tecnológicos, los países tienen la capacidad de modernizar sus servicios con gran facilidad y rapidez, añadiendo nuevas características que, de acuerdo con ellos, mejoran mucho su funcionalidad. Estados Unidos es una de esas naciones que ha realizado grandes avances en su tecnología en muchas áreas, haciendo que varios sectores como el económico o de defensa, sean más fáciles de manejar y de esa manera, hacer que la vida para los operadores y usuarios sea más sencilla.

Pero esta alta tecnificación en el estilo de vida estadounidense se ha convertido en su mayor vulnerabilidad. El hecho de que todos los sectores de Estados Unidos estén conectados a una red, ha convertido a la nación en un actor sumamente dependiente, y más cuando están incluidas todas aquellas infraestructuras clave que son pilar del poder económico, político y militar del país, tales como: energía, comunicaciones, transporte, defensa, salud, entre muchas otras.

El diccionario del Patrimonio americano define infraestructura como “[…] las instalaciones básicas y necesarias para el funcionamiento de una comunidad o sociedad, tales como transportes, sistemas de comunicación, agua, líneas

eléctricas e instituciones públicas como escuelas, oficinas postales y prisiones"[161]. Pero se convierte en crítica cuando aquellas instalaciones, al sufrir un ataque, causan "[…] la interrupción de su función significaría una crisis socio-económica con el potencial de socavar la estabilidad de una sociedad y, de ese modo, causar consecuencias políticas, estratégicas y de seguridad"[162].

Defender las infraestructuras críticas siempre ha estado dentro de las preocupaciones del país, sin embargo, el miedo ha crecido debido a la conexión que tienen todas ellas a las redes, Internet incluido, causando que un altercado se presente con mayor facilidad y rapidez, como ya se ha mencionado en las características que posee la naturaleza de un ataque cibernético.

El gobierno de Estados Unidos reconoce que son catorce sectores críticos los que necesitan de una mayor protección, ya que son los que proveen los principales bienes y servicios al Estado. El siguiente cuadro muestra cuáles son esos sectores, así como el papel que representan en la economía del país, los impactos que causarían al ser víctimas de un ataque cibernético, así como la interdependencia que existe entre ellos.

[161] John Robles Rosslin, Min-kyu Choi, Eun-suk Cho, *et. al.*, "Common Threats and Vulnerabilities of Critical Infrastructures", [en línea], Dirección URL: http://www.sersc.org/journals/IJCA/vol1_no1/papers/03.pdf, [consulta: 27 de junio de 2014]. Traducción propia.

[162]Lior Tabansky, "Critical Infrastructure Protection against Cyber Threats", [en línea], Dirección URL: http://d26e8pvoto2x3r.cloudfront.net/uploadimages/Import/(FILE)1326273687.pdf, [consulta: 27 de junio de 2014].Traducción propia.

Figura 11

Sectores estadounidenses vulnerables a un ataque cibernético

Sector	Descripción	Impactos	Depende de
Agricultura y Alimentos	Representa aproximadamente una quinta parte de la actividad económica del país	Comercial, Facilidades Gubernamentales, Defensa, Salud Pública y Servicios de Salud	Energía, Transportación
Bancario y Financiero	Columna vertebral de la economía mundial, cuyas operaciones recaen principalmente en entidades privadas	Comercial, Facilidades Gubernamentales	Energía, Tecnologías de la Información (IT), Comunicaciones
Químico	Dividido en cuatro segmentos: químicos básicos, especializados, ciencias de vida y productos de consumo	Comercio, Energía, Agricultura y Alimentación, Defensa, Servicios de Emergencia, Salud Pública y Servicios de Salud	Energía, IT, Comunicaciones
Facilidades Comerciales	Acceso abierto al público, sin la percepción de elementos de medidas de seguridad		Banca, Comunicaciones, IT, Energía, Transportación, Agua, Agricultura y Alimentos, Servicios de Emergencia
Represas	Equilibran las sequías e inundaciones, suministran agua, generan energía, funcionan como vías navegables, estabilidad ambiental y mejoras al hábitat en todo el país	Energía, Salud Pública y Servicios de la Salud, Comercio, Agricultura y Alimentación	Energía
Defensa	Realiza la investigación, desarrollo, diseño, producción y mantenimiento de sistemas de armas militares, subsistemas, piezas o componentes para satisfacer las necesidades militares.	Servicios de Emergencia	Energía, IT, Agricultura y Alimentos

Servicios de Emergencias	Forman la primera línea de defensa, prevención y reducción de consecuencias de cualquier ataque a la nación.	Todos los sectores	Comunicación, IT, Energía, Transportación, Salud Pública y Servicios de Salud, Facilidades Gubernamentales
Energético	Sin suministro de energía, la salud y el bienestar se ven amenazados y la economía del país se detiene. Dividido en tres segmentos interrelacionados: electricidad, petróleo y gas natural.	Todos los sectores	Transportación, IT, Comunicaciones
Facilidades Gubernamentales	Incluye edificios, de propiedad o en alquiler por gobiernos federales, estatales, territoriales, locales o tribales, localizadas en el territorio o en el extranjero.	Comercial, Banca, Servicios de Emergencia	IT, Energía, Agua
Tecnología de la Información	Un papel clave en asegurar el ciberespacio de la nación. Compuesto por entidades que producen y proveen *hardware*, *software*, sistemas y servicios de IT, incluyendo desarrollo, integración, comunicaciones y seguridad.	Banca, Facilidades Gubernamentales, Servicios de Emergencia, Transportación	Comunicaciones, Energía
Reactores Nucleares, Materiales y Desperdicios	Representa el 20% del consumo eléctrico de la nación. Incluye plantas de energía nuclear, plantas de reactores nucleares utilizados para investigaciones, pruebas y entrenamiento.	Todos los sectores	IT, Comunicaciones, Transportación, Defensa, Servicios de Emergencia, Energía
Salud Pública y Servicios Médicos	Desempeña un papel significativo en respuesta y recuperación a través de todos los demás sectores en el caso de una catástrofe natural o provocada por el hombre	Salud Pública	Servicios de Emergencia, IT, Comunicaciones, Transportación, Energía
Transportación	Seis subsectores claves: Aviación, Carreteras, Sistemas de Transportación Marítima, Sistemas de Transportación en Masa,	Energía, Agricultura y Alimentos, Químico, Servicios de Emergencia, Comercial	IT, Comunicaciones, Energía

	Sistemas de Canalización y Ferroviaria		
Agua	Vulnerable a una variedad de ataques a través de contaminación con agentes fatales, ataques físicos y ataques cibernéticos	Salud Pública, Agricultura y Alimentos, Comercial, Facilidades Gubernamentales	Protección del Ambiente, Extinción de Incendios, Servicios Médicos
Otros	Monumentos e Iconos Nacionales Sector Postal y de Transporte Marítimo		Energía, Comunicaciones, IT, Transportaciones

Fuente: Elaboración propia con datos de s/a, "Infraestructura crítica y recursos claves", [en línea], Dirección URL: http://www.mutualink.net/PDF/INFRAESTRUCTURA-CR%C3%8DTICA-Y-RECURSOS-CLAVES.pdf, [consulta: 27 de junio de 2014].

Cada uno de estos sectores son manejados a través de Sistemas Industriales de Control (ICS, *Industrial Control Systems*), por lo que cualquier desperfecto ocasionado por un ataque o alguna falla eléctrica no se queda aislado en un solo lugar, sino que tiende a dañar a corto o largo plazo los otros sistemas de las demás infraestructuras.

Es por eso que los expertos llaman a las instalaciones estadounidenses "sistema de sistemas", debido precisamente a la interdependencia que existe entre los sectores industriales. La interconexión significa que un incidente cibernético directo o indirecto puede afectar a otra infraestructura a través del fallo cascada[163], es decir, las consecuencias serían parecidas al efecto domino, si cae uno, caen todos.

Los Sistemas de Control Industrial están conformados por varios equipos inteligentes, cuya función es comunicarse con los operadores o proveedores a través de redes IP o internet. Por medio de los ICS se pueden monitorear y controlar el correcto funcionamiento de las infraestructuras así como procesos industriales complejos como el refinamiento de petróleo, producción química,

[163]*Cfr*. National Security Agency, "A Framework for Assessing and Improving the Security Posture of Industrial Control System (ICS)", [en línea], Dirección URL: http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf, [consulta: 18 de julio de 2014].

fabricación de productos, generación y transmisión de la energía eléctrica, entre muchas otras[164].

Los sistemas industriales que utiliza Estados Unidos son: Control de Supervisión y Adquisición de Datos (SCADA, *Supervisory Control and Data Acquisition*), Sistemas de Control Distribuido (DCS, *Distributed Control Systems*) y Controlador Lógico Programable (PLCs, *Programmable Logic Controllers*)[165]. El problema con estos tipos de *software* es que, al ser creados durante la década de los años 80 y 90, no fueron programados pensando en una manera viable para resistir tales ataques, por lo que sus funciones de seguridad eran muy escasas, y lo siguen siendo porque ninguno de los tres códigos ha sido modificado en lo absoluto.

La razón por la cual se adoptaron estos sistemas de control es porque mantener una red abierta resulta más barato que adoptar otra cerrada, es decir, se gasta menos dinero cuando las funciones de la infraestructura están conectadas a redes como Internet, donde varias personas pueden tener acceso a ellas de manera remota para poder realizar su trabajo más rápido, lo que aumenta la eficiencia de los sectores de forma considerable.

En poco tiempo, la adopción y el acceso a este tipo de redes se convirtió en imprescindible para las operaciones de cualquier instalación, sin embargo, las debilidades de los programas no se consideraron en ningún momento hasta que ya era demasiado tarde; varios actores internacionales ya se habían encargado de investigar las vulnerabilidades que contenía el *software,* es por eso que los intentos por penetrar su sistema, la mayoría de ellos llevados a cabo exitosamente, iniciaron.

Gran parte de ellos comenzaron a ser realizados por Estados, no obstante, no eran los únicos sujetos que tenían algún interés por acceder a los sistemas de la

[164] *Ídem.*
[165] *Ídem.*

infraestructura crítica estadounidense; el General Keith Alexander, director del Cibercomando, ha señalado varias veces que esa capacidad no está necesariamente restringida a los Estados, ya que tanto hackers como criminales podrían causar efectos del tamaño de una nación[166].

Es por eso que la Ciberguerra no tiene cabida en los postulados del Realismo Político, donde se argumenta que únicamente las naciones detentan el derecho a la guerra; a continuación se muestra un cuadro con la descripción de los posibles actores que cuentan no sólo con la capacidad, sino también con los recursos necesarios para efectuar una agresión exitosa, asimismo, se explica cuáles son las principales razones que los motivan a realizar tales acciones.

Figura 12

Fuentes de amenaza

Fuente de la amenaza	Descripción y motivación
Infiltrados	Es un usuario que posee acceso autorizado a sistemas privilegiados, pero ha escogido realizar acciones no autorizadas en contra de un sistema. Motivado por insatisfacción laboral, venganza o ganancias económicas.
Terroristas o activistas	Su principal motivación es atacar los intereses estadounidenses por medio de la ejecución de ataques ocasionando miles de víctimas o dañando la economía de EE.UU. Se podría atacar una planta nuclear con el objetivo de que los ciudadanos al ver el incidente en televisión se pongan en contra de los programas nucleares del país.
Hackers o ciber criminales	Motivados por la obtención de cuantiosas ganancias económicas por medio de la venta de información de tarjetas de crédito, robo de propiedad intelectual, información de redes importantes, fama, escándalo, o simplemente por la mera emoción del desafío.

[166]*Cfr.* Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'? *op. cit.,* p.2.

Naciones/Patrocinio de un Estado (Ciberguerra)	Patrocinio y/o financiamiento de programas dedicados a identificar métodos electrónicos para dañar la infraestructura crítica y la economía de los países amenazados. Las redes encargadas de monitorear y controlar la infraestructura crítica, muy probablemente, serían el principal blanco del patrocinio de los Estados.
Competidores	Robo de propiedad intelectual y sabotaje de sistemas críticos, con el objetivo de obtener beneficios económicos y/o reducir la competencia en el mercado.

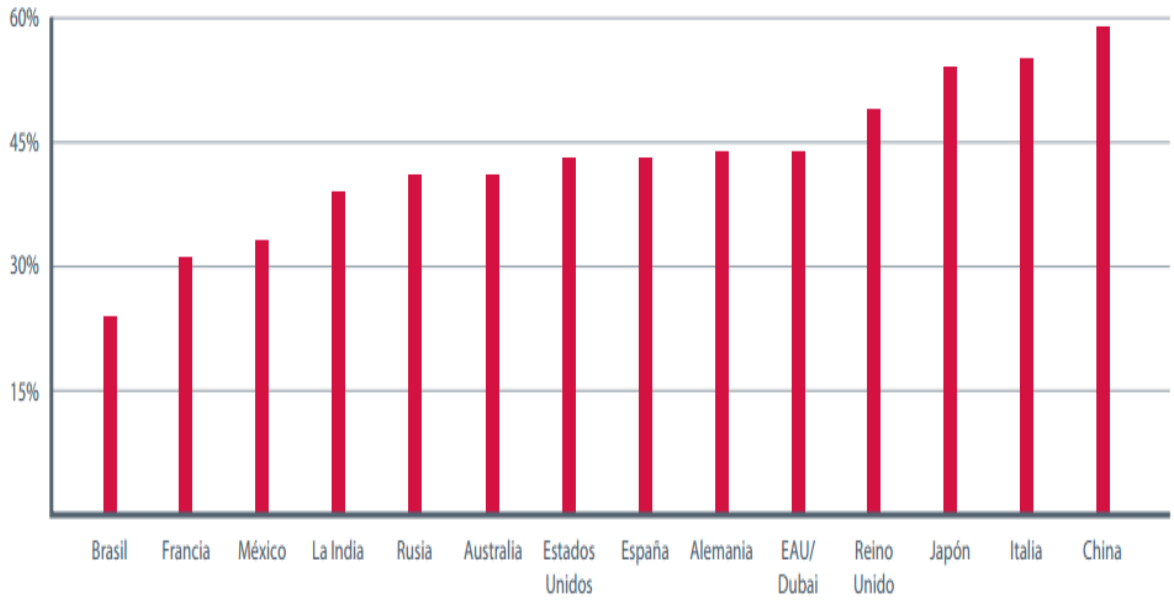
Fuente: Elaboración propia con datos de National Security Agency, "A Framework for Assessing and Improving the Security Posture of Industrial Control System (ICS)", [en línea], Dirección URL: http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf, [consulta: 18 de julio de 2014].

Actualmente, a pesar de conocer todos los riesgos que implica utilizar este tipo de sistemas de control, multiplicado por el número de fuentes que pueden hacer mal uso de ellos, las industrias siguen adoptando las ICS y peor aún, continúan conectando sus funciones a redes abiertas, donde cualquier persona puede acceder y dar pie a alguna catástrofe; además, la mayoría de las industrias no adoptan suficientes medidas de seguridad para evitar algún agravio.

En un estudio que hizo la compañía de seguridad informática, McAfee, se dieron a conocer 27 formas diferentes de salvaguardar la protección de los sistemas, con base en esto, se realizó una encuesta a los sectores más importantes provenientes de 14 naciones diferentes, entre ellas Estados Unidos, donde se les preguntaba cuáles eran las medidas de seguridad que usualmente adoptaban en sus *software*.

Figura 13

Índice de adopción de medidas de seguridad por país



Fuente: McAfee, "Amenazas en la oscuridad. Las infraestructuras críticas se enfrentan a ciberataques", [en línea], Dirección URL: http://www.mcafee.com/mx/resources/reports/rp-critical-infrastructure-protection.pdf, [consulta: 27 de junio de 2014].

Los resultados variaron mucho entre un país y otro, pero ninguno de los encuestados adoptaban ni siquiera el 60% del total de medidas; China resultó ser el país que más seguridad tenía dentro de sus sistemas, mientras que Estados Unidos no adoptaba ni la mitad de las precauciones existentes. Otro factor que se mantuvo constante entre todos ellos fue que, dentro de esas prevenciones, la mayoría de ellas se aplicaban a los sectores bancario y energético, mientras que el sector de agua y saneamiento se situaba en el último lugar[167],pero a pesar de ello aún resultan insuficientes teniendo en cuenta la importancia que poseen dichas instalaciones.

Más de la mitad de los ataques, al menos contra Estados Unidos, van dirigidos contra la red eléctrica, y como se ha visto en el cuadro de los catorce sectores

[167]*Cfr.* McAfee, "En el punto de mira. Las infraestructuras críticas en la era de la ciberguerra", [en línea], Dirección URL: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf, [consulta: 27 de junio de 2014].

estadounidenses, cada uno de ellos depende de la energía para poder funcionar de manera adecuada, todas las actividades que se realizan para la seguridad y subsistencia de los ciudadanos, y del país en sí, dependen de una buena distribución de la energía eléctrica.

Las dos razones principales por las cuales han aumentado las vulnerabilidades en este sector han sido porque[168]:

1. La mayoría de los propietarios y operadores de las redes han estado históricamente reacios a reportar los ciberataques sufridos contra sus redes o hacer los arreglos necesarios para mejorar su seguridad, debido, principalmente, al miedo de perjudicar su reputación;
2. El poder de la red eléctrica está altamente centralizado: La Interconexión del Este (*The Eastern Interconnection*), La Interconexión Occidental (*The Western Interconnection*) y La Interconexión Eléctrica de Texas (*The Electric Reliability Council of Texas Interconnection*) son las únicas redes que proveen electricidad a Estados Unidos, Canadá y una parte de México; por lo que bastaría atacar una de ellas para causar una catástrofe en una gran parte del territorio estadounidense.

El meollo del asunto es que muchas empresas aún son inconscientes del peligro que representa un ataque cibernético, no alcanzan a vislumbrar que el agravio no permanece únicamente en acciones como robo de información, sino que las consecuencias podrían ir mucho más allá, el desenlace podría ser la pérdida no sólo de miles de millones de dólares, sino también de una cuantiosa cantidad de vidas inocentes a lo largo y ancho del país.

Es precisamente esa ignorancia lo que ha causado que un alarmante número de ICS no sean protegidos ni siquiera con las medidas más básicas de protección, como la actualización frecuente del *software*, además de que las precauciones tomadas son tan arcaicas que no representan ninguna seguridad real.

[168] Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.*, p. 55.

Únicamente el 57% de los directivos emplean nombres de usuario y contraseñas para autenticar las conexiones a sus redes, los cuales son muy fáciles de adivinar, de robar o de poner en peligro de una u otra forma; mientras que sólo el 16% utiliza tecnologías más sofisticadas como el uso de *tokens* o autenticación biométrica[169].

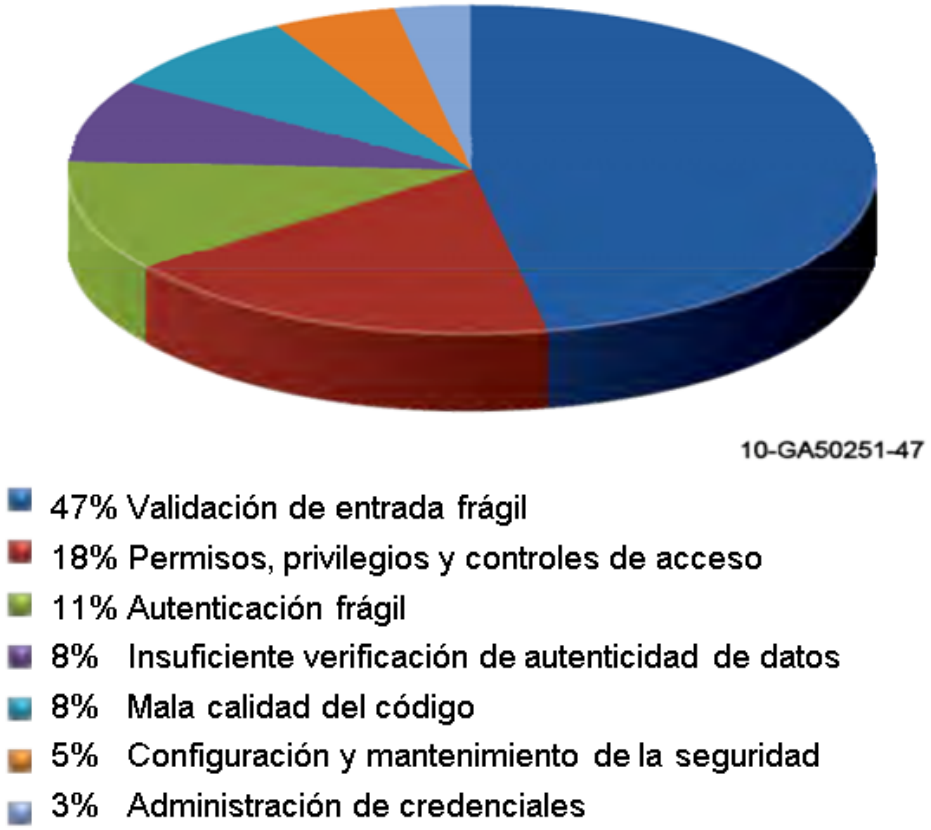
El primero de ellos se refiere al uso de una autenticación adicional a la contraseña, es decir, cada vez que se quiere acceder a una red no basta con poner una palabra secreta, sino que se debe introducir un código que es enviado a un dispositivo elegido al que muy pocas personas tienen acceso; el segundo se trata de la autenticación de ciertos rasgos físicos como las huellas dactilares, reconocimiento de voz o retina, patrones de la mano, entre otras, lo que aumenta de manera sustancial la seguridad.

La siguiente gráfica muestra cuáles son los principales errores que comete el equipo encargado de la protección de los sistemas de control, los cuales abarcan una amplia gama, desde los más básicos hasta los más complicados.

[169]*Cfr*. McAfee, "Amenazas en la oscuridad. Las infraestructuras críticas se enfrentan a ciberataques", [en línea], Dirección URL: http://www.mcafee.com/mx/resources/reports/rp-critical-infrastructure-protection.pdf, [consulta: 27 de junio de 2014].

Figura 14

Principales vulnerabilidades en los Sistemas de Control Industrial, ICS



Fuente: Control Systems Security Program National Cyber Security Division, "Common Cybersecurity Vulnerabilities in Industrial Control Systems", [en línea], *Homeland Security*, Dirección URL: https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf [consulta: 27 de junio de 2014].

La buena noticia es que la adopción de medidas de seguridad sigue creciendo, la mala es que, a diferencia de las amenazas y las vulnerabilidades, mejora muy lentamente[170]. Las causas de esto son muy variadas, además de la falta de conciencia y el alto costo que representa un sistema bien protegido, existe la débil relación entre la administración estadounidense actual y las empresas privadas (dueñas del 90% de la infraestructura del país).

[170] *Ídem.*

En un principio, la seguridad cibernética estaba a cargo únicamente del Estado, sin embargo, con el crecimiento masivo del uso de las tecnologías de la información por parte del sector privado, ésta ha pasado a ser competencia no sólo de la esfera pública sino también de la privada[171]. La paulatina dependencia hacia las redes ya no es un tema que le atañe solamente a uno, sino que se debe trabajar en equipo si se quiere lograr un resultado viable para todos.

A pesar de ello, son muy pocos los empresarios que aceptan trabajar hombro con hombro junto al gobierno para frenar las intrusiones digitales, la mayoría de ellos consideran que la administración estadounidense no cuenta con los conocimientos necesarios para brindar una protección inteligente, no obstante, se han visto obligados a someterse a algunas regulaciones que se les han impuesto.

Sus principales preocupaciones sobre las legislaciones residen principalmente en tres puntos[172]:

1. Falta de fe en los conocimientos de la administración sobre el funcionamiento sectorial;
2. Posibilidad de que una torpe legislación pueda "reducir el nivel" de seguridad en sectores muy complejos;
3. Riesgo de que la notificación obligatoria de incidentes de seguridad (por ejemplo, la pérdida de confidencialidad de datos personales), se traduzca como pérdida de confianza y mala reputación.

Aún así, hay empresas que se contradicen cuando manifiestan una profunda desconfianza hacia el gobierno, ya que hay momentos en los que argumentan que ellos ya han gastado suficientes recursos en seguridad y que defender la nación es responsabilidad exclusiva de la administración en curso.

---

[171] Robles Rosslin John, Min-kyu Choi, Eun-suk Cho, *et. al.*, "Common Threats and Vulnerabilities of Critical Infrastructures", [en línea], *op. cit.*

[172] *Cfr.* McAfee, "En el punto de mira. Las infraestructuras críticas en la era de la ciberguerra", [en línea], *op. cit*.

Hay empresas y entidades que han dado marcha atrás a su gestión de la seguridad para cumplir específicamente con lo que dictaban los requerimientos[173]. Se trata de un círculo vicioso: el gobierno impone medidas de seguridad ineficaces a las empresas, quienes a pesar de su desconfianza deben cumplir con esos requisitos normativos, lo que disminuye enormemente el tiempo que se podría utilizar en planificar su propio esbozo de protección, aumentando así las vulnerabilidades, obligando al Estado a tomar más medidas de protección.

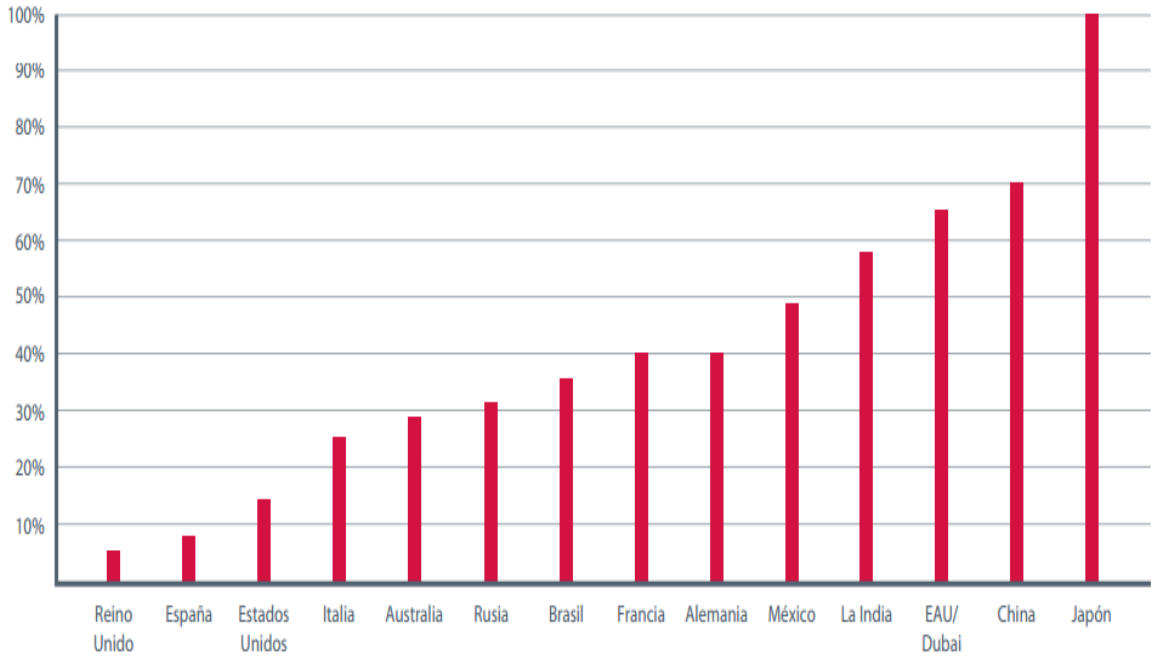
A pesar de que se han eliminado barreras legales para que las empresas y el gobierno puedan compartir información sobre las fuentes y blancos de ataque, la desconfianza no proviene únicamente del sector privado; la administración estadounidense es bastante reticente con los directivos acerca de qué datos se pueden o no compartir, en parte porque no ven una manera segura de exhibirlos ante operadores de infraestructuras críticas sin que acaben en poder de sus adversarios, ya que varios propietarios poseen una larga cadena de instalaciones en varios países[174] y no se sabe con exactitud en qué manos podrían caer documentos tan importantes.

La siguiente gráfica muestra la escasa cifra de reuniones oficiales que son organizadas entre los dueños de las empresas privadas que componen los sectores trascendentales del gobierno de Estados Unidos, las cuales son llevadas a cabo con el fin de discutir y evaluar el tema de la seguridad cibernética; como se puede observar, la potencia norteamericana ocupa uno de los últimos lugares con sólo el 20%.

[173] *Ídem.*
[174] *Ídem.*

Figura 15

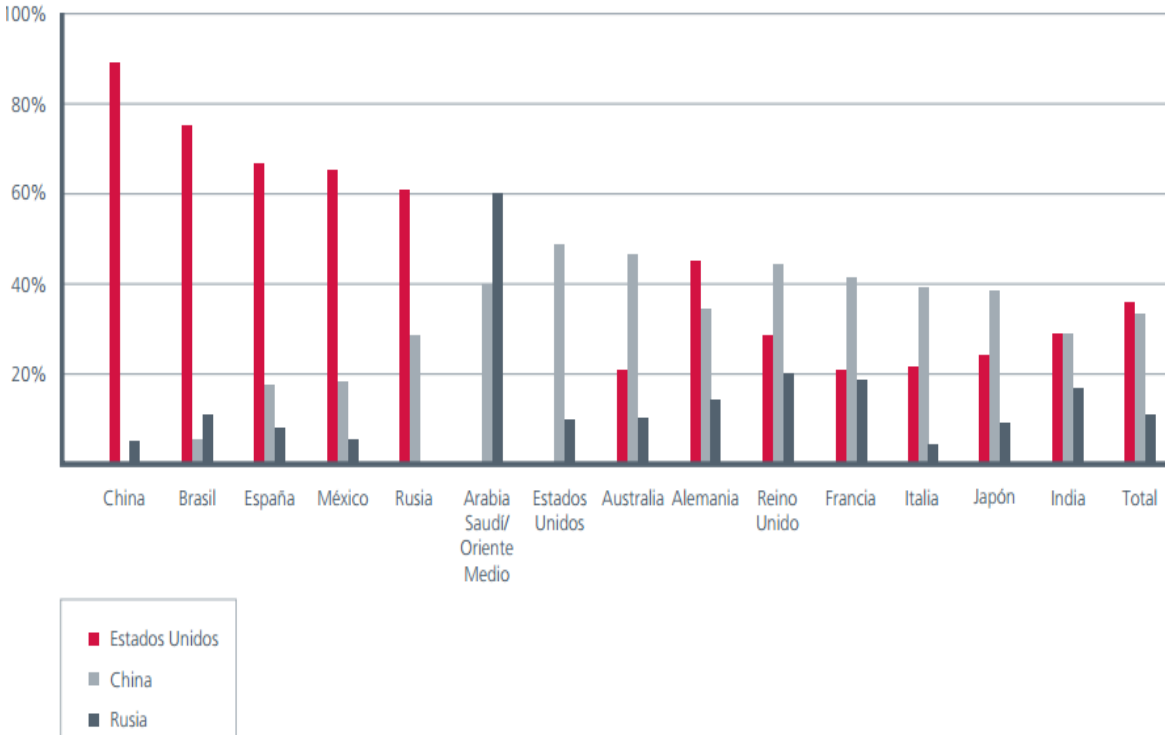
Encuentros oficiales realizados por el gobierno y el sector privado



Fuente: McAfee, "En el punto de mira. Las infraestructuras críticas en la era de la ciberguerra", [en línea], Dirección URL: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf, [consulta: 27 de junio de 2014].

Después de todos los elementos que se han proporcionado, se puede ver con mayor claridad las razones por las cuáles Estados Unidos es considerado como el país más propenso a sufrir un ataque cibernético, cosa que no ha pasado desapercibida por ningún actor internacional. En la misma encuesta que realizó McAfee, se les preguntó a todos los participantes a quién consideraban el actor más vulnerable en este nuevo fenómeno internacional, por supuesto, la potencia norteamericana ocupó el primer lugar.

Figura 16
País considerado más vulnerable



Fuente: McAfee, "En el punto de mira. Las infraestructuras críticas en la era de la ciberguerra", [en línea], Dirección URL: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf, [consulta: 27 de junio de 2014].

Richard Clarke, alto asesor de la Casa Blanca, brinda cuatro puntos importantes que resumen las vulnerabilidades a las que se enfrenta Estados Unidos[175]:

1. Su gran dependencia a los sistemas ciber controlados para hacer funcionar infraestructura crítica nacional, tales como poder eléctrico, tuberías, aerolíneas, vías férreas y la banca;
2. La mayoría de la infraestructura crítica estadounidense es propiedad privada;
3. Estados Unidos es una de las pocas naciones en el mundo en el que los propietarios de las empresas son tan políticamente poderosas que pueden evitar algunas de las regulaciones gubernamentales en sus sectores;

[175]*Cfr.* Caplan Nathalie, "Cyber War: the Challenge to National Security", *op. cit*.

4. El sector militar estadounidense es extremadamente susceptible a ciberataques.

La realidad es que, a pesar de los esfuerzos hechos por Estados Unidos, las amenazas avanzan a un paso vertiginoso, la naturaleza del ciberespacio se vuelve cada vez más compleja mientras que la incertidumbre sobre quién es el encargado de adoptar las medidas de seguridad en la infraestructura crítica podría causar graves consecuencias, no sólo en el flujo de suministros vitales y/o en el funcionamiento de los servicios esenciales, sino que su seguridad nacional y la habilidad de lanzar una acción defensiva quedarían devastadas.

Aún no existe un modelo de seguridad que mantenga el ritmo de la evolución o sofisticación de los agravios digitales, incluso, el director del Cibermando estadounidense, Keith Alexander ha declarado que la única manera en la que un país puede estar totalmente seguro es desconectándose completamente de las redes, lo que causaría la pérdida descomunal de toda clase de beneficios: económicos, políticos, defensivos y por supuesto, tecnológicos. Estados Unidos se vería transportado automáticamente a las condiciones que tenía durante el siglo XIX, con todas sus limitaciones y peligros que eso conllevaría.

Sin embargo, el peligro de un posible ataque contra la infraestructura crítica del Estado aumenta cuando las pocas medidas de seguridad, mas una cantidad importante de información crucial sobre los sistemas, son revelados por *insiders*, es decir, personas con acceso privilegiado a datos confidenciales, muchas veces llamados traidores.

3.3.2. Snowden: el secreto revelado

El 6 de junio de 2013, dos importantes periódicos, *The Guardian* y *The Washington Post*, británico y estadounidense respectivamente, publicaron una de las noticias más insólitas: Estados Unidos había desarrollado un programa de espionaje y vigilancia, el cual había estado utilizando desde el año 2007, no sólo contra sus propios ciudadanos, sino también en contra de muchos objetivos internacionales, incluyendo varios Jefes de Estado.

El origen de esta conducta se remonta a poco tiempo después de los atentados del 11 de septiembre de 2001, cuando el gobierno estadounidense aprobó la Ley Patriótica, la cual autoriza a algunas entidades intervenir cualquier tipo de comunicaciones, con el objetivo de prevenir alguna acción que esté vinculada con el terrorismo[176].

La fuente de dicha información fue Edward Snowden, antiguo empleado de la Agencia Nacional de Seguridad (NSA) y de la Agencia Central de Inteligencia (CIA), quien durante mucho tiempo recopiló una copiosa cantidad de documentos clasificados, como la descripción de los programas de vigilancia desarrollados por la NSA, principalmente los dos más activos: *PRISM* y *X Keyscore*.

Figura 17

Principales programas de inteligencia de la NSA

Año creación	Año fin	Nombre	Finalidad	Área de influencia	Operador
1945	1975	SHAMROCK	Apropiación masiva de mensajes telegráficos	EE.UU.	NSA
1962	A	ECHELON	Intercepción masiva de comunicaciones electrónicas	Todo el mundo	NSA + UKUSA
1967	1973	Minaret	Intercepción de comunicaciones electrónicas de ciudadanos bajo sospecha	EE.UU.	NSA
1982	A	Main Core	Recolección de información personal y financiera de ciudadanos bajo sospecha	EE.UU.	NSA, CIA, FBI
1990s	/	Highlander	Intercepción masiva de comunicaciones vía satélite INMARSAT	Medio Oriente	NSA
1990s	1990s	Thinthread	Intercepción masiva de datos de internet	EE.UU.	NSA
2000	/	Mainway	Recolección de metadatos de llamadas telefónicas	EE.UU.	NSA
2000	A	Bullrun	Inclusión de vulnerabilidades en *hardware* y *software* de determinados objetivos	Todo el mundo	NSA

[176]*Cfr*. Javier Sáez, "Resumen del caso Snowden", [en línea], Dirección URL: http://alponiente.com/resumen-del-caso-snowden/, [consulta: 04 de agosto de 2014].

Atentados terroristas del 11 de septiembre de 2001

2001	A	Terrorist Surveillance Program	Intercepción masiva de datos de sospechosos de actividades terroristas	Todo el mundo	NSA + UKUSA
2002	2007	Trailblazer	Intercepción masiva de datos de internet	EE.UU.	NSA
2002	/	Pinwale	Recolección de correos electrónicos	Todo el mundo	NSA
2002	A	RAGTIME	Intercepción masiva de datos de sospechosos de actividades terroristas en EE.UU	Todo el mundo	NSA
2003	/	FairView	Recolección de metadatos de llamadas telefónicas, correos electrónicos y actividad en internet de ciudadanos	Todo el mundo	NSA
2003	/	NIMO	Intercepción masiva de datos multimedia	EE.UU.	NSA
2004	A	Boundless Informant	Recolección de metadatos de llamadas telefónicas	Todo el mundo	NSA
2005	2007	Turbulence	Intercepción masiva de datos de internet	Todo el mundo	NSA
2007	A	PRISM	Recolección de información de los principales proveedores de servicios	EE.UU.	NSA
2007	A	X-Keyscore	Intercepción masiva de datos de internet	Todo el mundo	NSA + UKUSA
2007	/	Dropmine	Espionaje de las comunicaciones de embajadas y organismos internacionales	EE.UU.	NSA
2009	A	Mastering the Internet	Recolección de metadatos de llamadas telefónicas, correos electrónicos y actividad en internet de ciudadanos	Todo el mundo	UKUSA

A *–Sigue activo*

/ *–Se desconoce su estado*

UKUSA *–Alianza formada por Estados Unidos, Canadá, Reino Unido, Nueva Zelanda y Australia*

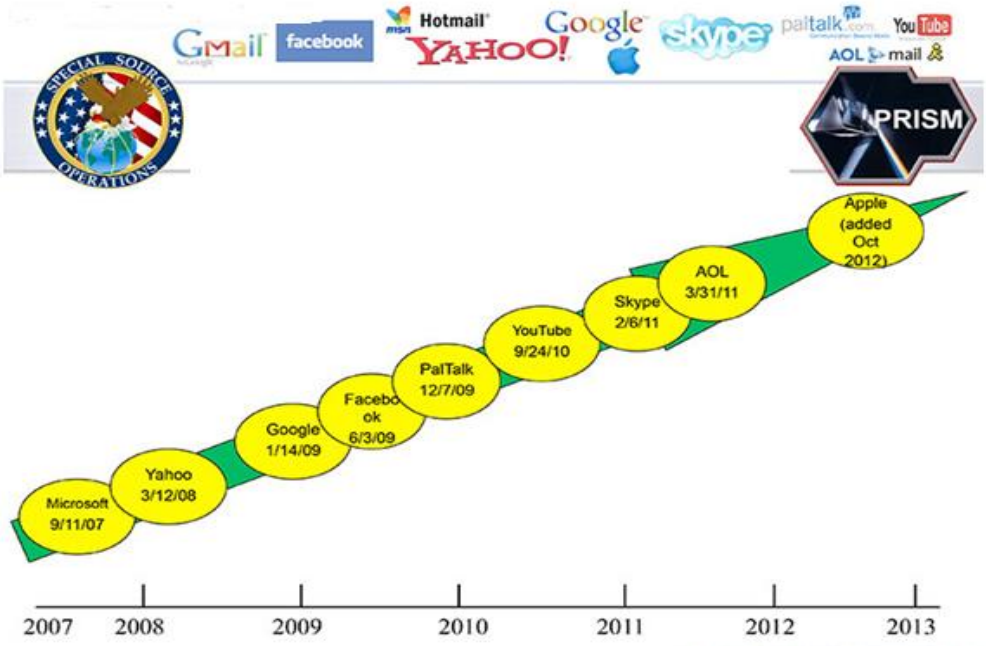
Fuente: Elaboración propia con datos de Real Instituto Elcano, "La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU", [en línea], Dirección URL: http://www.realinstitutoelcano.org/wps/wcm/connect/7366288041c9aefda642ae709b5c3216/ARI41-2013-THIBER-NSA-espionaje-publico-privada-Snowden.pdf?MOD=AJPERES&CACHEID=7366288041c9aefda642ae709b5c3216, [consulta: 04 de agosto de 2014].

El primero de ellos, se encarga de recopilar diferentes datos de comunicación como llamadas, correos electrónicos, videos, fotos, direcciones IP, transferencia de archivos y detalles de perfiles en las redes sociales, principalmente de los ciudadanos estadounidenses que residen fuera del país, o de aquellos que mantienen constante interacción con personas que habitan fuera del territorio nacional[177].

El gobierno estadounidense es capaz de acceder a toda esta información gracias a que tiene entrada libre a las bases de datos de nueve de las mayores empresas de Internet del país, las cuales tienes presencia en prácticamente cada rincón del mundo: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube y Apple.

Figura 18

Proveedores y fecha de adhesión al programa PRISM



Fuente: s/a, "NSA slides explain the Prism data-collection program", [en línea], periódico *The Washington Post*, sección "Polítics", 10 de julio, 2013, Dirección URL: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/, [consulta: 04 de agosto de 2014].

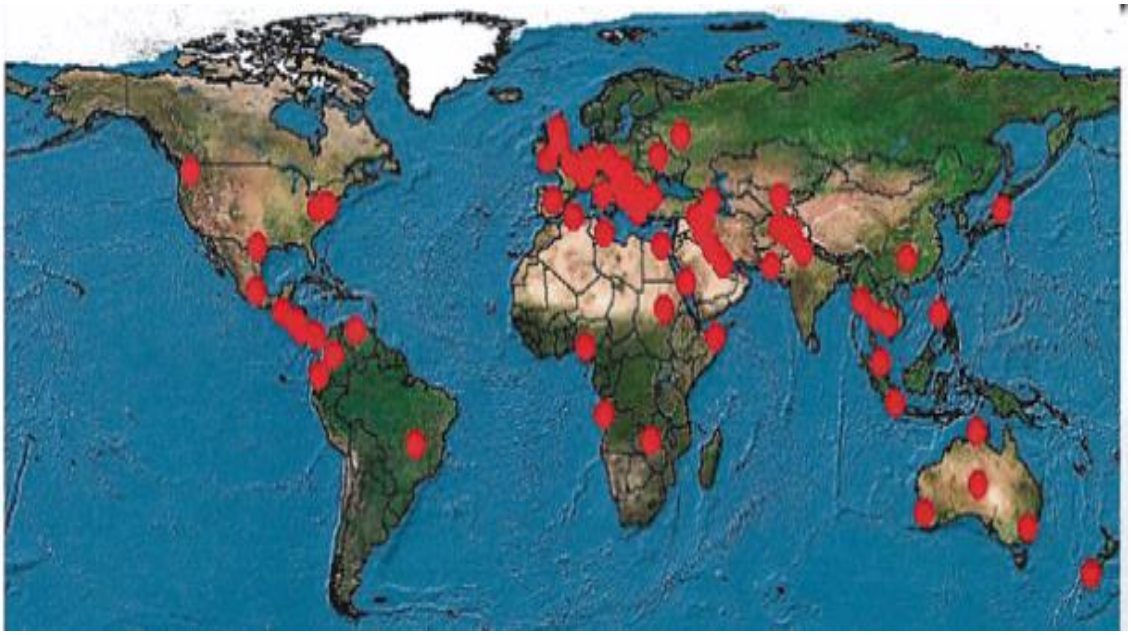
[177] s/a, "NSA slides explainthe Prism data-collection program", [en línea], periódico *The Washington Post*, sección "Polítics", 10 de julio, 2013, Dirección URL: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/, [consulta: 04 de agosto de 2014].

El siguiente programa de vigilancia se trata de *X Keyscore*, el cual posee grandes similitudes con PRISM; sin embargo, posee algunas diferencias sustanciales: cuenta con la capacidad de recaudar información en tiempo real y está calificado para conseguir los mismos datos que su compañero, sólo que a un alcance mayor: puede ver el contenido de los correos, no sólo su destinatario; los sitios visitados por el usuario; chats de Facebook, así como cualquier mensaje privado[178].

La Agencia de Seguridad Nacional ha hecho posible que este programa recolecte miles de archivos diariamente debido a que cuenta con 700 servidores apostados en 150 sitios diferentes en varias partes del mundo.

Mapa 5

Presencia mundial del programa de vigilancia X Keyscore



Fuente: s/a, "X Keyscore presentation from 2008", [en línea], periódico *The Guardian*, sección "World News", 31 de julio, 2013, Dirección URL: http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, [consulta: 04 de agosto de 2014].

[178]*Cfr*. David Brooks, "Programa de EU, capaz de intervenir toda actividad cibernética en el mundo, revelan", [en línea], periódico *La Jornada,* sección "Mundo", 1 de agosto, 2013, Dirección URL: http://www.jornada.unam.mx/2013/08/01/mundo/019n1mun, [consulta: 05 de agosto de 2014].

De acuerdo con las declaraciones del gobierno estadounidense, estos dos programas fueron desarrollados con el único fin de ayudar con la prevención de ataques terroristas, así como con la búsqueda de sus diferentes conexiones alrededor del mundo; sin embargo, Snowden reveló que si bien sí habían cumplido esa función al detener de manera exitosa varios intentos de ataque, dichos programas no fueron utilizados únicamente para tales objetivos.

Como ya se mencionó, los objetivos fueron sumamente variados, no sólo se espiaba a quienes se consideraría "natural", o al menos no tan sorpresivo, debido a la rivalidad económica o militar que mantiene con países como China y Rusia, sino también a aquellos países considerados como aliados de la potencia norteamericana.

El mapa presentado muestra de manera más clara el alcance que poseen los programas de espionaje estadounidense, la presencia va desde el color verde, en el que tenían menos vigilancia, hasta el color rojo donde su atención era considerablemente insistente. Irán fue el país que estuvo más sometido al acecho de Estados Unidos, seguido de Pakistán, Jordania, Egipto y la India.

Por otro lado, México, Brasil y Colombia se encontraron dentro de los principales objetivos de la zona de Latinoamérica, si bien se halló presencia en otros países vecinos, fueron éstos en donde la vigilancia era más pronunciada[179]. De acuerdo con varias fuentes, el principal objetivo que se buscaba en las tres naciones era la obtención de información relacionada con temas militares y secretos comerciales en materia de energía.

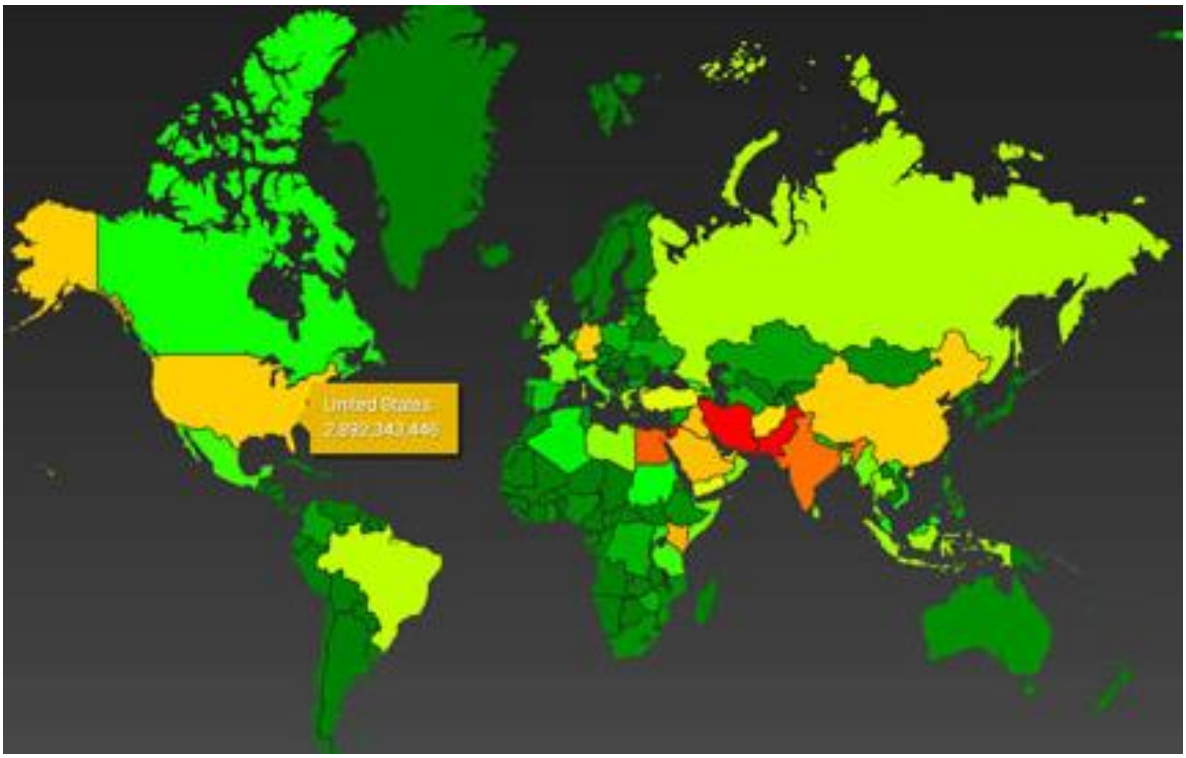
Por ejemplo, la empresa Petrobras así como su relación con las licitaciones para la explotación del combustible fue uno de los casos más mencionados en los documentos revelados por Snowden. Así que, poco después de que fueran descubiertos dichos datos comenzaron los reclamos en contra de Estados Unidos, incluso la presidenta, Dilma Rousseff, canceló una de sus reuniones, ya

[179] *Cfr*. Javier Sáez, "Resumen del caso Snowden", [en línea], Dirección URL: http://alponiente.com/resumen-del-caso-snowden/, [consulta: 04 de agosto de 2014].

programada, con el presidente Barack Obama debido al escándalo; asimismo, anunció la construcción de un satélite geoestacionario que los mantenga a salvo de cualquier interferencia[180].

Mapa 6

Nivel de espionaje estadounidense alrededor del mundo



Fuente: Glenn Greenwald, Ewen MacAskill, "Boundless Informant: the NSA's secret tool to track global surveillance data", [en línea], periódico *The Guardian*, sección "World News", 11 de junio, 2013, Dirección URL: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining, [consulta: 04 de agosto de 2014].

Después de que uno de los secretos mejor resguardados de Estados Unidos fuera develado, la interrogante sobre las razones que llevaron a Edward Snowden a poner en peligro su seguridad y su vida siguieron presentes. En las entrevistas que otorgó a los periódicos *The Guardian* y *The Washington Post* declaró que no podía permitir que el gobierno de Estados Unidos destruyera la libertad a la privacidad, no sólo la de los ciudadanos estadounidenses, sino también la del

[180] *Ídem*.

resto de la población, y que no quería seguir participando en la construcción de un mundo donde se registraba todo lo que hacía y decía. Asimismo, dijo que no tenía ninguna intención de mantener en secreto su identidad porque tenía claro que no había hecho nada malo.

Aún así, esas ideas no fueron compartidas por el gobierno de Obama, quien mostró un gran empeño, como nunca se había visto contra las personas que revelaban información confidencial, en intentar detenerlo a toda costa. En el momento en el que se supo que Edward estaba en Hong Kong esperando recibir respuesta a las peticiones de asilo político que había realizado a más de 21 países repartidos en América Latina, Europa y Asia, Estados Unidos comenzó a mover sus influencias para presionar a las naciones y que le negaran la demanda.

Ante esto, varias naciones consintieron en negarle la solicitud a Snowden, principalmente países europeos, quienes sin importar el hecho de haber sido víctimas del espionaje estadounidense, concedieron la demanda del país. Estados Unidos, no satisfecho con las presiones y amenazas, invalidó el pasaporte para menguar las posibilidades de escapar.

Es por eso que, viendo sus opciones considerablemente disminuidas, el ex agente de la NSA optó por trasladarse a Rusia, donde permaneció alrededor de un mes varado en el área de tránsito del Aeropuerto Internacional de Sheremetiévo, sin posibilidad de desplazarse a ningún otro lado sin contar con el permiso pertinente[181].

Al enterarse de su posición, se exigió al gobierno ruso la inmediata extradición del informante, no obstante, Vladimir Putin, presidente de Rusia, respondió que esa era una petición que no podía ser respondida, debido a que no existía ningún acuerdo de dicha naturaleza entre los dos países, por lo que, después de un mes,

[181] Ramiro Álvarez Ugarte, "El caso Snowden y la democracia en disputa", [en línea], *Nueva Sociedad, Opinión*, núm. 247, septiembre-octubre, 2013, Dirección URL: http://www.nuso.org/upload/articulos/3975_1.pdf, [consulta: 18 de julio de 2014].

se le concedió asilo a Snowden, con una vigencia de un año y opción de renovarlo tan sólo una vez cuando expire ese período.

Las opciones con las que contaría el *whistleblower*[182] estadounidense una vez que expirara su permiso de permanencia en territorio ruso son muy limitadas, sin embargo, existen. Venezuela, Nicaragua y Bolivia declararon que no aceptan presiones ni amenazas de nadie, por lo que están dispuestos a abrir las puertas de su país a quien tuvo el coraje de hacer lo correcto. Incluso el apoyo no termina en esos lugares, varios organismos internacionales como Amnistía Internacional, activistas, asociaciones, así como una importante cantidad de ciudadanos estadounidenses, han mostrado su total apoyo a Edward Snowden, pidiendo que se le conceda el perdón y de esa forma, tener la libertad de regresar a su lugar de origen.

Sin embargo, Estados Unidos no se ha planteado esa opción, a pesar de que ha declarado que no se aplicará pena de muerte si regresa de manera voluntaria, está claro que se abriría un proceso en su contra por la revelación de archivos sumamente confidenciales. Ha puesto en peligro las relaciones que el país tiene, la desconfianza que ha generado no sólo entre los actores internacionales sino también entre sus propios ciudadanos, son acciones que no serán pasadas por alto.

Y más importante aún, Edward Snowden ha puesto en alerta no sólo a todos aquellos que representan algún peligro importante para la seguridad nacional de Estados Unidos, sino también a quienes podrían competir contra la potencia norteamericana de alguna manera, económica y militar sobre todo, con riesgo de arrebatarle su reinado. Ha perdido el factor sorpresa y ha dado a conocer su potencial, arriesgándose a que sea igualado y puedan utilizar las mismas herramientas contra él.

[182] Personas que acceden a información privilegiada sobre algún tipo de delito o comportamiento inadecuado que se realiza al amparo de secretos oficiales y a espaldas del público, revelándolo a la prensa motivados por algún principio que estiman valioso.

3.4. Ciberguerra Fría

De acuerdo con el Dr. Edmundo Hernández-Vela Salgado, la Guerra Fría se define como la

> Situación, atmósfera o ambiente que prevaleció en la *sociedad internacional* en la segunda postguerra, desde 1946, con el reconocimiento de la caída de la *Cortina de acero* hasta, la *Declaración de Helsinki* en 1975, cuando se puede considerar completado su desmantelamiento progresivo iniciado en 1962 durante la *Crisis de los cohetes en Cuba.*
> Asimismo, la *Guerra Fría* se caracterizó por una combinación de elementos inseparables e interdependientes, cada uno de los cuales debe ser interpretado en el contexto del conjunto de ellos; es decir, que la presencia de alguno o algunos de ellos en forma aislada de ninguna manera implica el mantenimiento o el resurgimiento de la *Guerra Fría*:
> 1. La pugna ideológico-político-económica, supuestamente irreconocible, de las dos grandes potencias surgidas de la contienda, Estados Unidos y Unión Soviética, secundadas por sus respectivos "bloques", el capitalista y el socialista, separados por una *cortina de acero*.
> 2. Su desenvolvimiento:
> 2.1. En condiciones de una casi absoluta incomunicación directa y falta de *información* oportuna, creíble y confiable entre las dos partes;
> 2.2. Alimentada conjuntamente por todo tipo de conjeturas y especulaciones alarmistas y pesimistas, rayanas en la paranoia;
> 2.3. Con su obligada secuela progresiva de tensión, malestar, recelo, temor, desconfianza, e inseguridad recíprocos.
> 3. El riesgo creciente de aniquilación mutua y aun de toda la humanidad ante la ominosa y desbocada acumulación, en *escalada* de *armas nucleares* y otras *armas de destrucción en masa*, y el constante aumento de su capacidad destructiva, que:
> 3.1. Sólo permitía la exhibición oportunista de ciertos arsenales intimidatorios, así como su frecuente alusión retórica en todos los foros y ocasiones posibles;

3.2. Hacía inoperante un posible enfrentamiento militar directo entre Estados Unidos y Unión Soviética y sus respectivos aliados;

3.3. Pero requería de un desfogue de la enorme tensión acumulada, que se lograba a través de *crisis* políticas periódicas […]; y sobre todo, de conflictos que frecuentemente devenían "guerras en terreno ajeno", como la de Corea del Norte, Viet Nam, Asia Sudoccidental y Norte de Africa, Angola, Afganistán, etcétera, que libraban las superpotencias indirectamente, por medio de terceros países y en el territorio de esto, buscando, según el caso, retenerlos o integrarlos a su correspondiente *zona de influencia*.

4. La concepción, puesta en práctica y dirección por los hegemones de un conjunto de políticas y acciones, desplegadas a nivel mundial, incluyendo todo tipo de asedios y asechanzas, que se fueron desenvolviendo en *escalada,* entre las que sobresalen las enmarcadas en la *contención* del *comunismo,* la *disuasión* o la *carrera armamentista,* el *espionaje* y el acopio de *información secreta*, en formas cada vez más sutiles, complejas y avanzadas, la mal información o el *contraespionaje,* así como las también permanentes e intensivas campañas abiertas o de *acción encubierta*, de hostilización, *propaganda*, subversión y desestabilización.

5. Su desmantelamiento progresivo:

Como consecuencia de la *diplomacia epistolar* efectuada durante la llamada "Crisis del Caribe" o "Crisis de los cohetes en Cuba", en octubre de 1962, que propició el inicio de la *entente hegemónica,* y consecuentemente del avance del *desarme* […] que se fue desarrollando rápidamente, primero a nivel bilateral, soviético-estadounidense, y subsecuentemente en el multilateral, al canalizarlas principalmente a las Naciones Unidas, en casi todos los ámbitos, incluyendo el relativo a las *armas estratégicas,* la *Guerra Fría* empezó a desmantelarse, siendo gradualmente substituida por el apaciguamiento, disminución, reducción o *relajamiento de la tensión internacional* […].

6. Finalmente, debemos hacer hincapié en que para conceptuar y referirnos apropiadamente a la *Guerra Fría* debemos tener invariablemente en cuenta, de manera conjunta e indisoluble, los cinco elementos constitutivos enunciados anteriormente, ya que cada uno de ellos, por

> separado, tiene su propio significado, y no puede ni debe ser considerado parcial y aisladamente como sinónimo de aquello de lo que forma parte[183].

Hoy en día, en el contexto de la Ciberguerra, Estados Unidos continúa como uno de los protagonistas del nuevo conflicto; sin embargo, ahora es China quien ocupa el lugar de la URSS como contrincante. Como se ha ido señalando, ambos países son los dos actores internacionales que han representado un papel más activo en el fenómeno de los ataques cibernéticos, ya que uno y otro han mantenido un porcentaje alto tanto en los ataques que lanzan como en los que reciben; ambas naciones han estado llevando a cabo varias acciones que fueron muy conocidas durante el período posterior a la Segunda Guerra Mundial, lo que ha desencadenado el surgimiento del nombre: Ciberguerra Fría.

Después de las declaraciones que realizó Edward Snowden, el mundo supo que la potencia norteamericana llevaba varios años espiando los movimientos de la República Popular China, sin embargo, el gobierno chino también poseía ya una larga lista de ataques lanzados contra Estados Unidos, en los cuales buscaba efectuar, principalmente, el robo de información militar, comercial y científica, mientras que Estados Unidos había efectuado sus ataques de espionaje contra miles de usuarios de la telefonía celular, incluyendo a figuras importantes del gobierno chino, así como empresas e institutos de investigación.

El siguiente mapa muestra la forma en que son realizados los ataques en tiempo real, de un lado se puede observar a aquellos sujetos que encabezan la lista de los lugares donde se origina el ataque, y del otro, aquellos que son los objetivos principales de esos agravios; en ambas relaciones Estados Unidos y China, ésta última representada por una de sus regiones, se posicionan en el primer y segundo puesto.

[183] Edmundo Hernández-Vela Salgado, Diccionario de Política Internacional, *op. cit.*, pp. 540-542.

Mapa 7

Ciberataques en tiempo real

Fuente: s/a, “Mapa de ciberataques en tiempo real”, [en línea], Dirección URL: http://www.neoteo.com/norse-mapa-de-ciberataques-en-tiempo-real/, [consulta: 08 de agosto de 2014].

No obstante, en este nuevo giro que ha dado la guerra, las naciones ya no están divididas en bloques, no se trata de dos esferas de influencia distintas, sino de una sola: ubicarse, o mantenerse, en el puesto de potencia mundial. Aún así, hay acciones que se están llevando a cabo de la misma manera y buscando los mismos objetivos de hace casi 25 años, por ejemplo la carrera armamentista, la disuasión y pruebas militares, en este caso cibernéticas, cada una ligada a la otra.

Al mencionar la carrera armamentista, se habla de un contexto en el que la seguridad y la paz internacional se ven amenazadas por la proliferación de armas, por lo que las grandes potencias usan el pretexto de poder defenderse de sus posibles enemigos, y para crear nuevas armas cada vez más innovadoras, sin

tomar en cuenta que al hacerlo, ellos alarman a otros estados y modifican la paz y seguridad de distintas naciones[184].

Ambas potencias económicas se han convertido en los actores principales de una nueva carrera armamentista cibernética, los dos países avanzan a un ritmo impresionante creando programas maliciosos para objetivos específicos. Sin embargo, algunos autores opinan que es China quien se encuentra a la cabeza de esta competencia, ya que desde finales de la década de 1990, ha hecho todo lo que una nación haría si aspirara a tener una capacidad ofensiva en el ciberespacio y pensara, al mismo tiempo, que puede convertirse en blanco de ciberataques[185]:

1. Crear grupos de *hackers* civiles;
2. Emprender amplias labores de ciber espionaje, incluso de *hardware y software* estadounidense;
3. Adoptar varias medidas para defender su propio ciberespacio;
4. Establecer unidades militares para la Ciberguerra;
5. Plantar bombas lógicas en las infraestructuras estadounidenses.

No es que Estados Unidos haya pasado varios años sin hacer nada, es sólo que, como ya se mencionó, muchos de los encargados de seguridad no le daban gran importancia a la estabilidad de sus sistemas, por lo que sólo se centraron en desarrollar su capacidad defensiva no ofensiva, creando varias brechas que China no tiene, o bien, trabaja para cerrarlas.

Otro factor importante son las pruebas que se realizan con las nuevas armas; tanto Estados Unidos como China, han llevado a cabo varios ensayos, no sólo dentro de los límites de su territorio sino también fuera de ellos, con el fin de verificar el correcto funcionamiento de su nuevo armamento. Un claro ejemplo de esto es el programa que fue desarrollado por programadores estadounidenses

[184]*Cfr*. Saúl Mandujano Rubio, "La carrera armamentista", [en línea], Dirección URL: http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/17/pr/pr5.pdf, [consulta: 09 de agosto de 2014].
[185]*Cfr*. Clarke Richard, K. Knake Robert, Guerra en la red. Los nuevos campos de batalla, *op. cit.,* p. 84.

llamado *CyberCity*, el cual representa una ciudad ficticia donde su infraestructura crítica, la mayor vulnerabilidad de la potencia norteamericana, es atacada diariamente con diferentes tipos de *malware*, lo que permite a los ciberguerreros aprender a reaccionar en cada uno de esos casos.

De igual manera, China, ha llevado a cabo varios ataques cibernéticos en contra de múltiples países con el único fin de probar los adelantos que se han desarrollado. De acuerdo con el Pentágono, el Ejército Popular de Liberación Chino realiza frecuentes ejercicios militares, en los que demuestra no sólo los avances en tecnología de la información, sino también de manera conjunta con sus fuerzas militares convencionales[186].

Lo que lleva a otro punto: la disuasión. Comprobar el correcto funcionamiento de todas esas armas no es una acción que se realice con el único objetivo de saber si el armamento cumple con sus tareas específicas, sino también para mostrarle al mundo de lo que ese país es capaz, exponer el alcance que poseen todos sus avances y las posibles repercusiones que tendría un enfrentamiento en contra de ellos.

Sin embargo, la doctrina de disuasión podría no tener los mismos efectos que tuvo durante la Guerra Fría; en el escenario del ciberespacio, al no conocer con exactitud la identidad del agresor, no se tiene claro si el mensaje de haber mostrado el poder de sus adelantos llegó a quienes ellos deseaban o no.

Es por eso que China está siguiendo su propia estrategia; la táctica conocida como *shashoujian* (el laberinto del asesino), o guerra asimétrica, esta fue diseñada para aprovechar las debilidades creadas por una aparente superioridad de las capacidades convencionales del enemigo, por lo que se usa la ciberguerra para compensar las deficiencias cualitativas que evidencian su ejército cuando se lo

[186]*Cfr*. Illaro Eguskiñe Lejarza, "Estados Unidos-China: equilibrio de poder en la nueva Ciberguerra Fría" [en línea], *op. cit.* [consulta: 26 de junio de 2013].

compara con el de Estados Unidos, empleando armas y tácticas fuera del espectro militar tradicional[187].

Ya se tiene claro que la gran dependencia que posee la infraestructura crítica estadounidense hacia las redes representa su mayor vulnerabilidad, por lo que es en ese punto donde los ataques chinos se están enfocando. Otro punto que tiene a su favor China es que existe una estrecha relación entre el sector privado y el gobierno, todo lo contrario con lo que sucede en Estados Unidos, ya que es la administración la que controla cada una de las redes que atraviesan la nación[188], razón por la cual tendría la capacidad de desconectarlas todas en el momento en que se llegara a presentar una amenaza grave por parte de cualquier actor.

Estados Unidos, tras el estudio que realizó la compañía de seguridad MANDIANT, ya ha reclamado oficialmente a China por todos los ataques de los que ha sido objeto, sin embargo, a pesar de que las direcciones IP de todos los agravios han conducido al cuartel de la unidad 61398 del Ejército Popular de Liberación Chino[189], el país sigue negando ser el autor de dichos agravios, por lo que únicamente se han logrado obtener promesas vacías de investigación que no conducen a nada.

Mientras que en las reuniones que se han desarrollado entre los mandatarios de estos países, sólo se "[…] ha reafirmado su voluntad para construir sistemas de defensa y protección, tanto en el sector público como privado, a la vez que negocian con otros países para construir normas comunes"[190].

Si bien existen varias diferencias entre este conflicto y la Guerra Fría que se desarrolló durante la segunda mitad del siglo XX, también hay varias similitudes que comparten, una de las más importantes es la poca probabilidad que existe

[187] *Cfr.* Clarke Richard, K. Knake Robert, Guerra en la red. Los nuevos campos de batalla, *op. cit.,* p. 79.
[188] *Cfr.* Andrew Krepinevich, Cyber Warfare. A 'Nuclear Option'?, *op. cit.*, p. 27.
[189] *Cfr.* Antonio Caño, "Estados Unidos y China, ante la primera ciberguerra fría", [en línea], periódico *El País*, sección "Internacional" 20 de febrero, 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html, [consulta: 19 de marzo de 2013].
[190] Clarke Richard, K. Knake Robert, Guerra en la red. Los nuevos campos de batalla, *op. cit.,* p. 79.

acerca de trasladar los enfrentamientos indirectos a la arena física. La interdependencia que existe entre Estados Unidos y China es enorme como para poner en riesgo el futuro de la economía internacional, ambos países tienen mucho que perder, por lo que harán lo posible por mantener los enfrentamientos en el escenario virtual.

Han pasado ya varias décadas desde la creación de la Internet, y aunque actualmente se conocen con más detalle los elementos que la conforman, aún existen vacíos que no se han explorado. Todos los días se descubren nuevas formas de penetrar un sistema violando las medidas de seguridad, y a pesar de todas las muestras que se han visto sobre la ineficacia de estos sellos, todavía hay quienes aseguran que éstos no son necesarios porque no se trata de una verdadera amenaza, a pesar de haber demostrado tener la capacidad de causar un colapso en cuestión de minutos. Sin embargo, muchas veces se espera a que suceda lo peor para poder actuar, esa es la naturaleza del ser humano.

Conclusiones

El fenómeno de la Ciberguerra es un tema muy complejo que ha comenzado a ser estudiado no sólo desde la perspectiva de las ciencias duras, sino también desde las Ciencias Sociales, con el objetivo de poder entender de una manera más clara en qué consiste, cuáles son sus alcances, sus características, así como las herramientas que están siendo desarrolladas para mitigar sus efectos.

Al tratarse de un tema relativamente nuevo, existen varias incógnitas que aún no se han resuelto, todavía no se tiene claro cuáles son las magnitudes reales del problema, razón que dificulta su análisis. Las naciones se encuentran ante la misma situación que experimentaron al inicio de las nuevas guerras; al verse envueltos en una nueva controversia, no saben con exactitud cómo actuar, se trata de una cuestión de prueba y error, por lo que los resultados no han sido siempre los deseados.

A partir de la mundialización, las constantes interacciones económicas, políticas, sociales, culturales y tecnológicas que se empezaron a realizar a nivel global, terminaron por ocasionar una gran interdependencia entre los países, la sociedad comenzó a desarrollar una gran sujeción hacia todos los aspectos que estos nuevos fenómenos ofrecían, sobre todo los tecnológicos.

La tecnología se transformó en una pieza fundamental e imprescindible para el desarrollo de las naciones, principalmente en el plano económico. Internet, ha sido parte de esos avances que han contribuido enormemente a la construcción del mundo moderno, actualmente, gran parte de los Estados se encuentran conectados a esta red digital; el gobierno, las empresas y la sociedad civil gozan de este beneficio que, sin duda alguna, ha facilitado la vida de muchas maneras posibles, cosa que puede verse como una ventaja o, para cuestiones de esta investigación, como una enorme desventaja.

Los inicios del uso de la Internet se remontan a la Guerra Fría, cuando se trataban de respaldar documentos de suma importancia del bloque capitalista, más tarde, a finales del siglo XX, su empleo comenzó a generalizarse, principalmente en el

área económica, convirtiéndose en una herramienta a la cual se podía tener acceso con más facilidad; cada año, más naciones, empresas y personas podían disponer de una computadora con capacidades para ingresar a la red.

En poco tiempo, muchos de los servicios básicos, llámese banca, distribución de agua potable, electricidad, salud, entre otras, empezaron a ser dependientes de esta tecnología, muchos sectores decidieron adoptar programas que les permitieran realizar diversas actividades a través de un acceso remoto, todo ello con el fin de mejorar sus capacidades.

Al percatarse de que se podía ingresar y manejar los sistemas de manera remota a través de las redes, se comenzó a deducir que se podía realizar lo mismo, de manera anónima, con el fin de llevar a cabo acciones ilícitas. Si bien, en un inicio los ataques eran sencillos y no tan exitosos, en muy poco tiempo, empezaron a ser más complejos y difíciles de rastrear. Los objetivos dejaron de ser “inocentes” y se transformaron en una amenaza significativa, el número de víctimas aumentó de forma estrepitosa, los gobiernos y el sector privado comenzaron a ser agredidos de manera constante.

Jefes de gobierno, políticos, periódicos internacionales, empresas transnacionales infraestructuras críticas, entre muchos otros, han sufrido agravios que van más allá de una simple intromisión a una computadora, las consecuencias abarcan desde robo de información clasificada hasta la introducción de algún virus que, a corto o largo plazo, cause algún colapso colosal. Todo ello, sin tener realmente claro quién o quiénes son los autores de tales irrupciones, por lo que no resulta tan sencillo pedir explicaciones o tomar medidas en contra de los infractores.

El problema reside en que, la herramienta que se utiliza para realizar dichas intrusiones digitales, es un instrumento esencial para el estilo de vida actual, por lo que se encuentra disponible en todos los rincones del mundo, así que, al contrario de lo que ocurre con las armas convencionales, casi cualquier persona puede tener libre acceso a ella, razón por la cual no puede ser eliminada sin más.

Ya no se está hablando de un ataque físico, el cual necesita de un ejército armado con una preparación previa en el campo de batalla, sino de un grupo de informáticos sentados detrás de una computadora, quienes con el simple hecho de oprimir algunas teclas pueden elegir causar alguna catástrofe en cuestión de segundos o bien, plantar una puerta trasera para poder introducirse al sistema en otra oportunidad; incluso, varios especialistas han declarado que el alcance que podría tener este tipo conflicto puede ser comparado, únicamente, con la magnitud de destrucción que deja una bomba nuclear a su paso, debido a la facilidad en que podría colapsar un Estado en cuestión de minutos.

Ante este panorama tan desalentador, los países buscan no sólo mejorar sus medidas de seguridad, sino también instrumentos de regulación que los auxilien a actuar en este campo de batalla tan desconocido. Si bien algunos países han adoptado algunos reglamentos que los han ayudado a disminuir o prevenir las acometidas, desafortunadamente, hablar de una normatividad internacional, no resulta muy reconfortante.

A pesar de que la OTAN, a raíz de los ataques en Estonia, ordenó la creación del Manual de Tallin, éste representa únicamente un compendio de opciones para regular el mundo cibernético, guiándose solamente con ayuda de los preceptos de las guerras convencionales, razón por la cual muchos Estados no han aceptado las recomendaciones que se enmarcan en el, argumentando la existencia de lagunas en el tema. Sólo basta señalar la disparidad que existe en torno a la definición de Ciberguerra para darse cuenta que la adopción de reglas universales representa una tarea sumamente complicada.

Los altercados cibernéticos no representan la misma amenaza para todos los actores internacionales, hay quienes son prácticamente inmunes, mientras que otros, figuran en la lista de los principales objetivos. Este peligro se puede medir de acuerdo con la dependencia que posee cada país hacia la tecnología, entre más grande es ésta, los agresores cuentan con un mayor número de blancos a los cuales atacar.

Esta es una diferencia muy importante que existe entre las guerras convencionales y la Ciberguerra. Anteriormente, los países que tenían un mayor desarrollo económico y tecnológico, poseían una mejor preparación militar, por lo que resultaba muy arriesgado atacar a dichas naciones si no se contaba con el mismo nivel bélico, ya que eran ellas quienes contaban con todas las oportunidades de salir victoriosos Hoy en día, la situación no ha cambiado en cuanto a la interpretación que se hace con las naciones adelantadas, el problema es que la cantidad de arsenales que se posee ya no representa una superioridad en el contexto de la guerra cibernética, mientras que el crecimiento tecnológico sí se puede observar como una fragilidad.

Estados Unidos es el mejor ejemplo de ello, ya que, al ser el país más conectado en el mundo, automáticamente se convierte en el actor más dependiente y vulnerable de todos; cada una de las actividades que realiza, y las cuales lo mantiene en la posición de potencia, están enlazados con alguna red, principalmente abiertas (aquellas que tienen acceso a Internet), por lo que puede ser atacado desde cualquier punto poniendo en riesgo la estabilidad de la nación.

El objetivo que más peligro representa es el de la infraestructura crítica, porque cualquier irrupción realizada contra sus sectores clave podría representar la paralización total del país, quedando a merced de los infractores en cuestión de horas. Es por eso que las medidas de seguridad se han centrando en mejorar los programas de control industrial, no obstante, al ser en su mayoría propiedad privada, existe una controversia sobre quién debe de encargarse de la estabilidad de dichos sistemas, si los dueños o el gobierno, ya que el principal afectado, en caso de que se realizara un agravio digital, sería la población civil.

A pesar de que el presidente Barack Obama aprobó un estatuto que obliga a las instancias privadas y públicas a cooperar entre sí, realizando un intercambio de información con el objetivo de prevenir los ataques, aún existe cierta renuencia en delimitar qué datos se pueden o no compartir sin poner en peligro la reputación de algunas empresas o de que algún archivo se filtre y pueda parar en manos equivocadas.

Aunado a eso, sigue existiendo cierto escepticismo sobre las posibles consecuencias que un ataque a las redes tendría. Algunos encargados de la seguridad de los sectores clave estadounidenses han declarado, varias veces, no estar tan preocupados sobre lo que podría ocurrir a causa de las deficiencias en los sistemas, a pesar de todos los agravios que se han observado en los últimos años, están seguros de que todas las amenazas son exageradas, o peor aún, infundadas.

Es por eso que hace falta una toma de conciencia de la seguridad cibernética, es sorprendente que aunque se han visto los efectos en innumerables ocasiones, aún haya empresarios que quieran adoptar artefactos “inteligentes” que mejoren la eficiencia de ciertos servicios, por ejemplo de la red eléctrica, el mayor blanco de ataques en Estados Unidos. Aún no se termina de asimilar que entre más dispositivos tengan acceso a alguna red, mayor es la vulnerabilidad y el riesgo de ser atacado aumenta extremadamente.

Como si no fuera suficiente, en los últimos años, la vulnerabilidad de la potencia americana ha crecido de manera importante debido a las declaraciones realizadas por el ex agente de la CIA y de la NSA, Edward Snowden. Todos los programas que había venido desarrollando el país, quedaron al descubierto tras el robo de más de un millón de archivos confidenciales, gracias a eso, innumerables países se percataron de que habían sido blanco de espionaje cibernético por varios años, por lo que decidieron poner en marcha esos mismos programas en contra de su creador.

Es por eso que la potencia norteamericana ha apostado por la educación, la creación de programas, cursos, talleres, maestrías y posgrados en la Universidad de Maryland ha sido el primer paso para contar con una nueva generación de especialistas cibernéticos, la participación del gobierno y de las entidades privadas ha sido crucial para la formación de esos estudiantes, ya que se les ha brindado el apoyo y recursos necesarios para que sean capaces de librar las guerras del mañana.

Sin lugar a dudas, las amenazas en el quinto dominio de la guerra avanzan a un paso nunca antes visto, la complejidad de los ataques progresan más rápido de lo que son comprendidos, mientras que las medidas de seguridad recorren el camino a ritmo lento. Cada vez más países se introducen en el mundo virtual, analizando las capacidades de esta nueva guerra, otros ya han comenzado a realizar pruebas mezclando la competencia de las fuerzas convencionales con las digitales, con el fin de obtener una mayor ventaja en un posible escenario de confrontación.

Tras la investigación realizada se comprobó que la Ciberguerra representa una nueva forma de llevar a cabo un conflicto bélico; sin embargo, no sólo es realizada entre los Estados, sino que las fuentes de amenaza abarcan otros actores internacionales, tales como grupos terroristas, espías y piratas informáticos, quienes han demostrado estar tan calificados como una nación debido a las enormes capacidades y recursos que poseen para infringir la misma proporción de daños.

Asimismo, quedó asentado que la guerra virtual representa un escenario más complejo que los enfrentamientos convencionales, el peligro es mayor debido a la facilidad que se tiene para efectuar una irrupción digital, el esfuerzo y el tiempo que se requiere, ciertamente, son menores. Tras varios ejemplos, se ha expuesto que las secuelas podrían ser colosales, si bien, en una contienda convencional pueden causarse los mismos daños físicos, con un ataque cibernético pueden realizarse en cuestión de segundos, todo esto, gracias a la conexión que existe entre los servicios básicos de una nación y la Internet, el daño sería igual que el efecto domino, un colapso tras otro, hasta que no haya más que caos y destrucción.

Es claro que el contexto se torna cada vez más complicado, la complejidad de la Ciberguerra crece día a día con el nacimiento de nuevas amenazas, además, con los millones de documentos que Edward Snowden aún no ha revelado, quedan muchas líneas de investigación a las cuales dar seguimiento.

Fuentes bibliográficas

Aron Raymond, *Paz y guerra entre las naciones*, vol. I y II, Alianza Editorial, Madrid, 1984, 919 pp.

Aznar Fernández-Montesinos Federico, *Entender la guerra en el siglo XXI*, Editorial Complutense, Madrid, 2011, 298 pp.

Carr Jeffrey, *Inside Cyber Warfare,* Segunda edición, O'Reilly, Estados Unidos, 2012, 294 pp.

Castells Manuel, *La Galaxia Internet,* areté, Barcelona, 2001, 316 pp.

Clarke Richard, K. Knake Robert, *Guerra en la red. Los nuevos campos de batalla*, Ariel, Barcelona, 2011, 327 pp.

Courmont Barthélémy, *La guerra: una introducción,* Historia Alianza Editorial, Madrid, 2010, 209 pp.

García Hernán David, Catalá Martínez Ignacio, *Historia de la guerra,* Editorial Síntesis, Madrid, s.a. 304 pp.

Garlan Yvon, *La guerra en la Antigüedad,* Alderabán, Madrid, 2003, 206 pp.

Hernández-Vela Salgado Edmundo, *Diccionario de Política Internacional*, Porrúa, México, Tomos I y II, 2002, Sexta Edición, 1295 pp.

Kaldor Mary, *Las nuevas guerras. Violencia organizada en la era global,* Kriterios, TusQuets Editores, Barcelona, 2001, 242 pp.

Krepinevich Andrew, *Cyber Warfare. A 'Nuclear Option'?*, Center for Strategic and Budgetary Assessments, 2002, 85 pp.

Rosas María Cristina, Astié-Burgos Walter, *El mundo que nos tocó vivir. El siglo XXI, la Globalización y el Nuevo Orden Mundial*, Miguel Ángel Porrúa, México, 2005, 220 pp.

Sierra Campuzano Claudia, *Historia de nuestro tiempo. A la luz de los especialistas*, Esfinge Grupo Editorial, México, 2006, 578 pp.

Tzu Sun, *El arte de la guerra*, Colofón, México, 2012, 200 pp.

Von Clausewitz Karl, *De la guerra,* Labor Punto Omega, Barcelona, 1984. 616 pp.

Fuentes electrónicas

Abella Gonzalo, "A propósito de la energía nuclear", [en línea], *Visiones Alternativas*, Cuba, Dirección URL: http://www.nacionmulticultural.unam.mx/mezinal/docs/545.pdf, [consulta: 25 de noviembre de 2013].

Álvarez Ugarte Ramiro, "El caso Snowden y la democracia en disputa", [en línea], *Nueva Sociedad, Opinión*, núm. 247, septiembre-octubre, 2013, Dirección URL: http://www.nuso.org/upload/articulos/3975_1.pdf, [consulta: 18 de julio de 2014].

Bencsáth Boldizsár, Pék Gabor, *et. al., "The Cousins of Stuxnet: Duqu, Flame, and Gauss",* [en línea], Dirección Url: *https://www.mdpi.com/1999-5903/4/4/971/*pdf, [consulta: 11 de febrero de 2014].

Benedicto Solsona Miguel A., "EEUU ante el reto de los ciberataques", [en línea], *Instituto Español de Estudios Estratégicos, Opinión*, núm. 37, abril, 2013, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO37-2013_Ciberataques_BenedictoSolsona.pdf, [consulta: 26 de junio de 2014].

Brooks David, "Programa de EU, capaz de intervenir toda actividad cibernética en el mundo, revelan", [en línea], periódico *La Jornada,* sección "Mundo", 1 de agosto, 2013, Dirección URL: http://www.jornada.unam.mx/2013/08/01/mundo/019n1mun, [consulta: 05 de agosto de 2014].

Caño Antonio, “EEUU pasa a la ofensiva para frenar los ciberataques”, [en línea], periódico *El País*, sección “Internacional” 20 de febrero, 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/02/20/actualidad/1361395431_105565.html, [consulta: 19 de marzo de 2013].

Caño Antonio, “Estados Unidos y China, ante la primera ciberguerra fría”, [en línea], periódico *El País*, sección “Internacional” 20 de febrero, 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/02/19/actualidad/1361300185_954734.html, [consulta: 19 de marzo de 2013].

Caplan Nathalie, “Cyber War: the Challenge to National Security”, [en línea], vol. 4, núm. 1, *Global Security Studies,* 2013, Dirección URL: http://globalsecuritystudies.com/Caplan%20Cyber.pdf, [consulta: 20 de enero de 2014].

Caro Bejarano María José, “La protección de las infraestructuras críticas”, [en línea], *Instituto Español de Estudios Estratégicos, Opinión*, núm. 21, julio, 2011, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_analisis/2011/DIEEEA21_2011ProteccionInfraestructurasCriticas.pdf, [consulta: 18 de julio de 2014].

Clapper James R., *Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community*, [en línea], Estados Unidos, 29 de enero de 2014, Dirección URL: http://www.intelligence.senate.gov/140129/clapper.pdf, [consulta: 02 de mayo de 2014].

Control Systems Security Program National Cyber Security Division, “Common Cybersecurity Vulnerabilities in Industrial Control Systems”, [en línea], *Homeland Security,* Dirección URL: https://ics-cert.us-cert.gov/sites/default/files/documents/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf, [consulta: 27 de junio de 2014].

Crenshaw Martha, “La guerra contra el terrorismo: ¿están ganando los Estados Unidos*?”*, [en línea], *Terrorismo Internacional,* núm. 105, 2006, Dirección URL: http://www.realinstitutoelcano.org/analisis/1058/1058_Crenshaw_EEUU_Guerra_Terrorismo.pdf, [consulta: 27 de abril de 2014].

Department of Defense, “Joint Terminology for Cyberspace Operations”, [en línea], Dirección URL: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf, [consulta: 29 de noviembre de 2014].

Eguskiñe Lejarza Illaro, “Ciberguerra, los escenarios de confrontación”, [en línea], *Instituto Español de Estudios Estratégicos, Opinión*, núm. 18, febrero, 2014, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf, [consulta: 20 de abril de 2014].

Eguskiñe Lejarza Illaro, “Estados Unidos-China: equilibrio de poder en la nueva Ciberguerra Fría”, [en línea], *Instituto Español de Estudios Estratégicos, Opinión*, núm. 60, julio, 2013, Dirección URL: http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO60-2013_Ciberguerra_Fria_EEUU-China_E.Lejarza.pdf, [consulta: 26 de junio de 2014].

Forigua Rojas Emersson, “Las nuevas guerras: Un enfoque desde las estructuras organizacionales”, [en línea], Dirección URL: http://www.javeriana.edu.co/politicas/publicaciones/documents/9LASNUEVAS.pdf, [consulta: 20 de noviembre de 2013].

Geers Kenneth, Kindlund Darien, *et. al*., *World War C: Understanding Nation-State Motives Behind Today’s Advanced Cyber Attacks*, [en línea], Dirección URL: http://www.fireeye.com/resources/pdfs/fireeye-wwc-report.pdf, [consulta: 29 de enero de 2014].

Gellman Barton, Blake Aaron, “Edward Snowden comes forward as source of NSA leaks“, [en línea], periódico *The Washington Post*, sección “Política”, 10 de junio, 2013, Dirección URL: http://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html, [consulta: 04 de agosto de 2014].

Gellman Barton, Markon Jerry, “Edward Snowden says the motive behind leaks was to expose ‘surveillance state’ “, [en línea], periódico *The Washington Post*, sección “Política”, 10 de junio, 2013, Dirección URL: http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?tid=pm_politics_pop, [consulta: 04 de agosto de 2014].

Greenberg Andy, “The Real Meaning of Cyberwarfare”, [en línea], *Forbes,* marzo, 2010, Dirección URL: http://www.forbes.com/2010/03/03/jeffrey-carr-internet-technology-security10-cyberwar.html, [consulta: 20 de enero de 2014].

Greenwald Glenn, MacAskill Ewen, “Boundless Informant: the NSA’s secret tool to track global surveillance data”, [en línea], periódico *The Guardian*, sección “World News”, 11 de junio, 2013, Dirección URL: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining, [consulta: 04 de agosto de 2014].

Greenwald Glenn, MacAskill Ewen, Poitras Laura, “Edward Snowden: the whistleblower behind the NSA surveillance revelations”, [en línea], periódico *The Guardian*, sección “World News”, 10 de junio, 2013, Dirección URL: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, [consulta: 04 de agosto de 2014].

IIP Digital, “Presidente Obama habla sobre el futuro de la lucha contra el terrorismo”, [en línea], Dirección URL: http://iipdigital.usembassy.gov/st/spanish/texttrans/2013/05/20130529148119.html#ixzz35cyoWPKN, [consulta: 23 de abril de 2014].

Ingersoll Geoffrey, “Russia Turns to Typewriters to Protect Against Cyber Espionage”, [en línea], *Business Insider*, 11 de julio de 2013, Dirección URL: http://www.businessinsider.com/russia-turns-to-typewriters-for-secrets-2013-7, [consulta: 12 de febrero de 2014].

Kaldor Mary, “Un nuevo enfoque sobre las guerras”, [en línea], *Papeles*, núm. 94, 2006, Dirección URL: http://www.fcp.uncu.edu.ar/upload/nuevoenfoqueguerrasmarykaldor.pdf, [consulta: 26 de octubre de 2013].

Lai Robert, Rahman Syed, *Analytic of China Cyberattack,* [en línea], Dirección URL: http://airccse.org/journal/jma/4312ijma04.pdf, [consulta: 1 de abril de 2014].

Landau Susan, Making Sense from Snowden: What’s Significant in the NSA Surveillance Revelations, [en línea], Dirección URL: http://privacyink.org/html/MakingSense.pdf, [consulta: 18 de julio de 2014].

Leiner Barry M., Cerf Vinton G., Clark David D., *et. al*., *Internet Society,* “Brief History of the Internet” [en línea], Dirección URL: http://www.internetsociety.org/brief-history-internet, [consulta: 22 de noviembre de 2013].

Lind William S., “Comprendiendo la Guerra de Cuarta Generación”, [en línea], Dirección URL: http://usacac.leavenworth.army.mil/CAC/milreview/download/Spanish/JanFeb05/lind.pdf, [consulta: 1 de noviembre de 2013].

Luttwak Edward, “Strategy: The logic of War and Peace”, [en línea], Dirección URL: http://reasonpapers.com/pdf/20/rp_20_9.pdf, [consulta: 20 de febrero de 2015].

Mandujano Rubio Saúl, “La carrera armamentista”, [en línea], Dirección URL: http://www.juridicas.unam.mx/publica/librev/rev/jurid/cont/17/pr/pr5.pdf, [consulta: 09 de agosto de 2014].

Manyika James, Roxburgh Charles, *McKinsey Global Institute*, “The great transformer: The impact of the Internet on economic growth and prosperity”, [en línea], 2011, Dirección URL: http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_great_transformer, [consulta: 15 de noviembre de 2013].

Markoff John, “Old Trick Threatens the Newest Weapons”, [en línea], *The New York Times*, 26 de octubre de 2009, Dirección URL: http://www.nytimes.com/2009/10/27/science/27trojan.html?pagewanted=all&_r=0, [consulta: 20 de febrero de 2014].

Maryland Cybersecurity Center, *Graduate Students*, [en línea], Dirección URL: http://www.cyber.umd.edu/education/grad, [consulta: 10 de julio de 2014].

McAfee, “Amenazas en la oscuridad. Las infraestructuras críticas se enfrentan a ciberataques”, [en línea], Dirección URL: http://www.mcafee.com/mx/resources/reports/rp-critical-infrastructure-protection.pdf, [consulta: 27 de junio de 2014].

McAfee, “En el punto de mira. Las infraestructuras críticas en la era de la ciberguerra”, [en línea], Dirección URL: http://www.belt.es/expertos/CIP_report_final_es_fnl_lores.pdf, [consulta: 27 de junio de 2014].

Mueller Paul, Yadegari Babak, “The Stuxnet Worm”, [en línea], Dirección URL: http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf, [consulta: 3 de febrero de 2014].

Münkler Herfried, “Las guerras del siglo XXI”, [en línea], Madrid, *Revista Internacional de la Cruz Roja,* núm. 849, Dirección URL: http://www.yumpu.com/es/document/view/6736670/herfried-munkler-las-guerras-del-siglo-xxi-publicado-en-revista-, [consulta: 25 de septiembre de 2013].

Nakashima Ellen, “U.S. said to be target of massive cyber-espionage campaign”, [en línea], Estados Unidos, *TheWashingtonPost.com*, 10 de febrero de 2013, Dirección URL: http://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html, [consulta: 30 de marzo de 2014].

National Security Agency, “A Framework for Assessing and Improving the Security Posture of Industrial Control System (ICS)”, [en línea], Dirección URL: http://www.nsa.gov/ia/_files/ics/ics_fact_sheet.pdf, [consulta: 18 de julio de 2014].

NBC News, “What we know about NSA leaker Edward Snowden”, [en línea], Dirección URL: http://usnews.nbcnews.com/_news/2013/06/10/18882615-what-we-know-about-nsa-leaker-edward-snowden?lite, [consulta: 04 de agosto de 2014].

Organisation for Economic Co-operation and Development, *OECD Internet Economy Outlook 2012*, [en línea], Dirección URL: http://www.keepeek.com/oecd/media/science-and-technology/oecd-internet-economy-outlook-2012_9789264086463-en#page1, [consulta: 20 de noviembre de 2013].

Parsons, “Supervisory Control and Data Acquisition”, [en línea], Dirección URL: http://www.parsons.com/Media%20Library/Supervisory-Control-and-Data-Acquisition.pdf, [consulta: 18 de julio de 2014].

Phys Org, “Flame virus linked to Stuxnet: researchers”, [en línea], Dirección URL: file:///C:/Users/Emmanuel/Downloads/2012-06-cybersleuths-link-flame-Stuxnet.pdf, [consulta: 21 de marzo de 2014].

Pureza José Manuel, Moura Tatiana, “Viejas, nuevas y novísimas guerras: la conflictividad desafía la modernidad”, [en línea], 23 pp., Dirección URL: https://estudogeral.sib.uc.pt/bitstream/10316/13281/1/Viejas,%20nuevas%20y%20nov%C3%ADsimas%20guerras.pdf, [consulta: 25 de septiembre de 2013], p. 4.

PWC, “Cibercrimen: ¿Está su organización en riesgo? Encuesta Global de Delitos Económicos 2011”, [en línea], Dirección URL: http://www.pwc.com/gx/en/economic-crime-survey/assets/pwc-gecs-venezuela.pdf, [consulta: 21 de febrero de 2015].

Real Academia Española, “Dominio”, [en línea], Dirección URL:http://lema.rae.es/drae/?val=dominio, [consulta: 26 de noviembre de 2013].

Real Instituto Elcano, “La Agencia de Seguridad Nacional (NSA), el espionaje y colaboración público-privada en EEUU”, [en línea], Dirección URL: http://www.realinstitutoelcano.org/wps/wcm/connect/7366288041c9aefda642ae709b5c3216/ARI41-2013-THIBER-NSA-espionaje-publico-privada-Snowden.pdf?MOD=AJPERES&CACHEID=7366288041c9aefda642ae709b5c3216, [consulta: 04 de agosto de 2014].

Revilla Montoya Pablo César, *El terrorismo global. Inicio, desafíos y medios político-jurídicos de enfrentamiento*, [en línea], Dirección URL: http://biblio.juridicas.unam.mx/revista/pdf/DerechoInternacional/5/art/art12.pdf, [consulta: 22 de abril de 2014].

Reydams Luc, “Á la guerre comme á la guerre: tipos de conflictos armados, respuestas del derecho humanitario y nuevos desafíos”, [en línea], *International Review of the Red Cross*, núm. 864, diciembre, 2006, Dirección URL: http://www.icrc.org/spa/assets/files/other/irrc_864_reydams.pdf, [consulta: 25 de septiembre de 2013].

Robles Rosslin John, Choi Min-kyu, Cho Eun-suk, *et. al.,* “Common Threats and Vulnerabilities of Critical Infrastructures”, [en línea], Dirección URL: http://www.sersc.org/journals/IJCA/vol1_no1/papers/03.pdf, [consulta: 27 de junio de 2014].

Rosas María Cristina, “De la ciberguerra a la ciberpaz”, [en línea], Dirección URL: http://www.etcetera.com.mx/articulo/de_la_ciberguerra_a_la_ciberpaz/9759/pagina/2, [consulta: 20 de febrero de 2015].

s/a, “El impacto de los programas de vigilancia en el derecho a la vida privada de los ciudadanos de la UE”, [en línea], Dirección URL: http://www.europarl.europa.eu/eplibrary/Impact-of-surveillance-programmes-ES.pdf, [consulta: 04 de agosto de 2014].

s/a, “El Mundo Capitalista. Desde la finalización de la Segunda Guerra Mundial al Siglo XXI. Los Estados Unidos, líder del mundo capitalista”, [en línea], Dirección URL: http://www.iesdionisioaguado.org/joomla/Distancia/HMC/Tema15.pdf, [consulta: 20 de abril de 2014].

s/a, “El Renacimiento”, [en línea], 44 pp., Dirección URL: http://www.educacion.gob.es/exterior/centros/severoochoa/es/departamentos/historia/material_julia/Arte_renacimiento_2_ESO.pdf, [consulta: 1 de noviembre de 2013].

s/a, “Infraestructura crítica y recursos claves”, [en línea], Dirección URL: http://www.mutualink.net/PDF/INFRAESTRUCTURA-CR%C3%8DTICA-Y-RECURSOS-CLAVES.pdf, [consulta: 27 de junio de 2014].

s/a, “La guerra fría cibernética”, [en línea], Londres, *BBC Mundo,* sección “Internacional”, 17 de mayo de 2007, Dirección URL: http://news.bbc.co.uk/hi/spanish/international/newsid_6665000/6665367.stm, [consulta: 29 de abril de 2013].

s/a, “Mapa de ciberataques en tiempo real”, [en línea], Dirección URL: http://www.neoteo.com/norse-mapa-de-ciberataques-en-tiempo-real/, [consulta: 08 de agosto de 2014].

s/a, “NSA slides explain the Prism data-collection program”“, [en línea], periódico *The Washington Post*, sección “Polítics”, 10 de julio, 2013, Dirección URL: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/, [consulta: 04 de agosto de 2014].

s/a, “Publicación del Manual de Tallin sobre ‘Ley Internacional en la Ciberguerra’ “, España, *Ministerio de Defensa*, 22 de marzo de 2013, Dirección URL: http://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59, [consulta: 16 de abril de 2013].

s/a, “X Keyscore presentation from 2008”, [en línea], periódico *The Guardian*, sección “World News”, 31 de julio, 2013, Dirección URL: http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, [consulta: 04 de agosto de 2014].

s/a, *Kaspersky Lab Experts,* “The Flame: Questions and Answers”, [en línea], 28 de mayo de 2013, Dirección URL: http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, [consulta: 11 de febrero de 2014].

Sáez Javier, “Resumen del caso Snowden”, [en línea], Dirección URL: http://alponiente.com/resumen-del-caso-snowden/, [consulta: 04 de agosto de 2014].

Saiz Escolano Eva, “Los ciberataques sustituyen al terrorismo como primera amenaza para EE.UU” [en línea], periódico *El País*, sección “Internacional”, 13 de marzo, 2013, Dirección URL: http://internacional.elpais.com/internacional/2013/03/13/actualidad/1363187707_199021.html, [consulta: 17 de marzo de 2013].

Saporito Laura, Lewis James A., *Cyber Incidents Attributed to China*, [en línea], Dirección URL: http://csis.org/files/publication/130311_Chinese_hacking.pdf, [consulta: 1 de abril de 2014].

Stouffer Keith, Falco Joe, Scarfone Karen, “Guide to Industrial Control Systems (ICS) Security”, [en línea], *National Institute of Standards and Technology,* Dirección URL: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf [consulta: 27 de junio de 2014].

Symantec. Security Response, “W32.Duqu The precursor to the next *Stuxnet*”, [en línea], Dirección URL: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_*Stuxnet*.pdf, [consulta: 21 de marzo de 2014].

Szor Peter, “Duqu. Threat Research and Analysis”, [en línea], *McAfee Labs,* Dirección URL: http://blogs.mcafee.com/wp-content/uploads/2011/10/Duqu1.pdf, [consulta: 5 de marzo de 2014].

T.V Paul., *Las potencias en ascenso y el equilibrio del poder en el siglo XXI*, [en línea], Dirección URL: http://www.sre.gob.mx/revistadigital/images/stories/numeros/n94/paul.pdf,[consulta: 20 de abril de 2014].

Tabansky Lior, “Critical Infrastructure Protection against Cyber Threats”, [en línea], Dirección URL: http://d26e8pvoto2x3r.cloudfront.net/uploadimages/Import/(FILE)1326273687.pdf, [consulta: 27 de junio de 2014].

The National Aeronautics and Space Administration, *Visible Earth*, “Earth’s city lights”*,* [en línea], 2000, Dirección URL: http://visibleearth.nasa.gov/view.php?id=55167, [consulta: 27 de noviembre de 2013].

The White House. Washington, *Ulysses S. Grant,* [en línea], Estados Unidos, Dirección URL: http://www.whitehouse.gov/about/presidents/ulyssesgrant, [consulta: 2 de noviembre de 2013].

Thieux Laurence, *El terrorismo internacional: causas e implicaciones estratégicas,* [en línea], Dirección URL: http://biblioteca2012.hegoa.efaber.net/system/ebooks/15197/original/El_Terrorismo_Internacional._Causas_e_Implicaciones_Estrategicas.pdf, [consulta: 25 de abril de 2014].

Unión Internacional de Telecomunicaciones*, Medición de la Sociedad de la Información,* [en línea], 2013, Dirección URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2013/MIS2013-exec-sum_S.pdf, [consulta: 28 de marzo de 2014].

UPMUN, Modelo de las Naciones Unidas de la Universidad del Pacífico, “Adenda: espionaje internacional”, [en línea], Dirección URL: http://www.upmun.org/wp-content/uploads/2013/08/Adenda-a-la-Gu%C3%ADa-de-estudio-de-la-Asamblea-General-Espionaje-internacional1.pdf, [consulta: 04 de agosto de 2014].

US Department of Defense, *U.S Cyber Command Fact Sheet*, [en línea], Dirección URL: http://www.defense.gov/home/features/2010/0410_cybersec/docs/cyberfactsheet%20updated%20replaces%20may%2021%20fact%20sheet.pdf, [consulta: 03 de julio de 2014].

Vásquez Teófilo. “Las nuevas guerras y el conflicto armado en Colombia”, [en línea], Colombia, *Controversia*, núm. 190, junio 2008, Dirección URL: http://biblioteca.clacso.edu.ar/Colombia/cinep/20100926025844/lasnuevasguerras.pdf, [consultado: 26 de octubre de 2013].