UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
MAESTRÍA EN ESTUDIOS EN RELACIONES INTERNACIONALES
FACULTAD DE CIENCIAS POLÍTICAS Y SOCIALES

LA REVOLUCIÓN TECNOLÓGICO-INFORMACIONAL DE LOS ASUNTOS MILITARES Y EL DESARROLLO DE ARMAMENTO CIBERNÉTICO, CASO DE ESTUDIO: MEDIO ORIENTE (2001-2015)

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRA EN ESTUDIOS EN RELACIONES INTERNACIONALES

PRESENTA:
BERENICE FERNÁNDEZ NIETO

TUTOR: RAÚL BENITEZ MANAUT
CENTRO DE INVESTIGACIONES SOBRE AMÉRICA DEL NORTE

CIUDAD UNIVERSITARIA, CD. MX., FEBRERO 2018

ÍNDICE

LISTA DE ILUSTRACIONES

Figuras

Gráficas

Mapas

Tablas

AGRADECIMIENTOS

A mi familia por su apoyo incondicional, especialmente a mi madre por ser el impulso que me lleva siempre adelante. A mis amigos por la compañía a lo largo de estos años, y por su incondicional cariño y comprensión. Especialmente a Grecia y Lili, por llenar este proyecto de alegría. A mis amigos en Compostela a Rosario, Fabiola, Lizet y Giselle por ser cómplices de momentos que quedarán por siempre en la memoria. Y a los que conocí en el camino, por haber formado parte de mi historia.

Las cosas no valen por el tiempo que duran, sino por las huellas que dejan.
Proverbio Árabe

A mis lectores: al doctor Alejandro Chanona Burguete, el maestro Alfonso Aragón Camarena, el doctor Moisés Garduño y en especial a la doctora Camelia Tigau por todos estos años de apoyo y aprendizaje. A mi tutor el doctor Raúl Benítez Manaut por su guía en la elaboración de este trabajo, al doctor José Julio Fernández Rodríguez por su cordial bienvenida, por haber guiado mi investigación en la Universidad de Santiago de Compostela, y por ser una excelente persona. A la doctora Karina Bárcenas Barajas por su impulso, inspiración y fe en todos mis proyectos.

La mayoría de las personas son como las hojas que caen y revolotean indecisas, otras como los astros: siguen una ruta fija, ningún viento los alcanza y llevan en su interior su propia ley y trayectoria
Herman Hesse

A la Universidad Nacional Autónoma de México, a la Facultad de Ciencias Políticas y Sociales, a CONACYT, y al Centro de Estudios de Seguridad de la Universidad de Santiago de Compostela por el apoyo que facilitó la realización de este trabajo.

Si he visto más lejos es porque estoy sentado sobre hombros de gigantes
Isaac Newton

GLOSARIO

Armamento cibernético: ciber-medio de guerra (entiéndase software) que es capaz, por diseño o intención, de causar daño a personas u objetos.

Ataque de Día Cero (Zero Day): es un ciberataque contra una aplicación o sistema que tiene como objetivo la ejecución de un código malicioso gracias al conocimiento de vulnerabilidades que el fabricante del producto y los usuarios desconocen.

Botnets: conjunto de computadoras infectadas por un malware que permite que un servidor (Command & Control) las manipule remotamente para realizar trabajos de forma distribuida.

Caballo de Troya (Troyan horse): malware escondido en un programa legítimo para infectar un sistema y secuestrarlo.

Ciberespacio: ámbito artificial creado por medios informáticos.

Ciberpoder: capacidad de utilizar el ciberespacio para crear ventajas y eventos de influencia en otros entornos operativos y a través del uso de instrumentos de poder.

Ciberguerra: acción equivalente a un ataque armado, o uso de la fuerza, en el ciberespacio ejecutada por un Estado en contra de otro Estado, que puede desencadenar una respuesta militar con un uso proporcional de fuerza cinética.

Era digital: se refiere al tiempo presente, en donde la mayoría de la información se presenta en forma digital, especialmente en comparación con otras épocas en donde las computadoras no eran utilizadas.

Esteganografía: la ocultación de información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto.

Estrategia: el arte utilizado para que la fuerza concurra a alcanzar los límites de la política.

Hacking: consiste en acceder desde algún lugar del ciberespacio a un ordenador privado valiéndose de deficiencias en los sistemas de seguridad, aprovechando su vulnerabilidad u obteniendo contraseñas de acceso haciéndose pasar por usuarios legítimos.

Hacker: persona que utiliza sistemas computarizados para obtener acceso no autorizado a redes cibernéticas.

ICMP: por sus siglas en inglés, *Protocolo de Mensajes de Control de Internet*. Su función básica es el control y notificación de errores del Protocolo de Internet IP.

Logic bombs: es un programa malicioso programado para causar daño en un cierto momento, pero permanece inactivo hasta ese instante. Un activador establecido, como una fecha u hora preprogramadas, activa una bomba lógica. Una vez activada, implementa un código malicioso que causa daños a una computadora.

Malware: software malintencionado que puede tomar la forma de un virus, un gusano o un caballo de Troya.

Phishing: técnica utilizada para engañar al destinatario de un mensaje para que proporcione información confidencial, como credenciales de inicio de sesión, al pensar que el mensaje proviene de una organización legítima.

Protocolo de Internet: software diseñado para manejar la información en paquetes.

Revolución de los Asuntos Militares: un cambio en la naturaleza de la guerra provocado por la aplicación innovadora de nuevas tecnologías.

Rootkit: es un conjunto de herramientas usadas frecuentemente por los intrusos informáticos o crackers que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, a menudo con fines maliciosos.

TCP: por sus siglas en inglés, *Transmission Control Protocol*. Es un protocolo orientado a conexión, el protocolo asegura que los datos serán entregados a su destino sin errores lo que lo hace más lento a diferencia del protocolo UDP.

Ramsonware: es un software malicioso que al infectar un equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los archivos tomando el control de toda la información y datos almacenados.

Sniffer: también conocido como analizador de redes, analizador de paquetes o analizador de protocolo, es un programa de ordenador usado para controlar y analizar el tráfico red transmitido de una localización de red a otra. Un sniffer captura cada paquete de información, lo codifica y luego da a su propietario la habilidad de ver su contenido.

Stealth: capacidad de una aeronave para actuar de forma furtiva. Es decir, que la energía emitida o reflejada por el vehículo aéreo o por sus diferentes componentes es indetectable por los radares.

UDP: por sus siglas en inglés, *User Datagram Protocol*. Es un protocolo no orientado a conexión, se utiliza sobre todo cuando la velocidad es un factor importante en la transmisión de la información

Virus: Programa malicioso con la capacidad de multiplicarse y dañar el sistema infectado. Su propósito es también extenderse a otras redes.

Worm (Gusano): Programa autónomo que se replica a sí mismo y se propaga a otras computadoras a través de redes.

Zero Day: Es un grave problema de seguridad o vulnerabilidad en un programa o aplicación para el que, en ese momento, no existe una solución o actualización.

SIGLAS Y ABREVIACIONES

BMD	Ballistic Missile Defence/ Defensa con Misiles Balísticos
C3I	Comando, Control, Comunicaciones e Inteligencia
C4I	Comando, Control, Comunicaciones, Computación e Inteligencia
C4IRS	Mando, Control, Comunicaciones, Ordenadores, Inteligencia, Reconocimiento y Búsqueda
CCA	Convención sobre Ciertas Armas Convencionales
DIH	Derecho Internacional Humanitario
TIC	Tecnologías de la Información y comunicación
RTM	Revolución de los Asuntos Militares
IT-RMA	Revolución Tecnológico-Informacional de los Asuntos Militares
ICBM	Misiles Intercontinentales
ICS	Computer-Assisted Industrial Control System
IRBM	Misiles de Alcance Intermedio
ISTAR	Inteligencia, Vigilancia, Adquisición y Reconocimiento de objetivos
IP	Protocolo de Internet
MRBM	Misiles de Medio Alcance
OODA	Observar, Orientar, Decidir y Actuar
ONU	Organización de Naciones Unidas
OTAN	Organización del Tratado del Atlántico Norte
PLC	Programmable Logic Controller
SRBM	Mísiles de Corto Alcance
SCADA	Supervisory Control and Data Adquisition - Supervisión, Control y Adquisición de Datos
UAV	Unmanned Air Vehicles – Vehículos Aéreos Inanimados
UCAVs	Unmanned Combat Aerial Vehicles – Vehículos Aéreos de Combate Inanimados

INTRODUCCIÓN

La evolución del pensamiento científico y de la innovación tecnológica han influenciado de forma incuestionable la historia de la humanidad. Especialmente, hacia finales de XX y principios del XXI las comunicaciones y transportes experimentaron una transformación que evocaba el surrealismo. Se incorporaron nuevas vías comunicación y surgieron nuevas formas de transferir, resguardar y presentar datos.

De forma paralela, el comercio, la política, la diplomacia y la interacción cultural se trasladaron a la web 2.0. A gran escala, la interacción entre Estados adoptó la autopista de la información como medio de intercomunicación y en el caso particular de la seguridad internacional el espacio cibernético ganó relevancia.

En el plano de las relaciones internacionales apareció la necesidad de comprender el impacto que los nuevos medios generaban en la interacción interestatal y la forma en la que la evolución de las comunicaciones representaba también el surgimiento de nuevas vulnerabilidades.

La inserción del espacio y de las capacidades digitales en el campo militar precisan de un profundo y constante estudio, debido principalmente a tres razones:

- Están generando un reordenamiento en la estructura, práctica y doctrina militar, cuyo impacto posee alcances nacionales, regionales e internacionales
- La incorporación de Internet en la guerra moderna representa la más clara manifestación de la evolución de la práctica belicista en el siglo XXI, y está generando repercusiones en los campos jurídicos, políticos, económicos y sociales
- La innovación tecnológica y su aplicación en el campo de la defensa llama a repensar los retos de la seguridad internacional en el nuevo siglo.

Por ello, es necesario profundizar en la Revolución Tecnológico Informacional de los Asuntos Militares y en el desarrollo de armamento cibernético a fin de localizar y analizar los efectos generados por el uso de nuevo armamento en el ámbito de las relaciones internacionales y en el campo de la defensa.

En la actualidad, la mayoría de los análisis al respecto se concentran en debates deterministas que desean precisar si Internet será o no el campo de batalla de las guerras del futuro, restando importancia a la observación de eventos que hoy en día cuentan con un componente altamente tecnológico y en donde la red de redes se coloca como un elemento estratégico.

Ante este panorama, el objetivo del presente trabajo es analizar la evolución histórica de la practica belicista, especialmente aquella experimentada a la llegada de la denominada “Era digital”. Con este propósito, se adopta el término Revolución Tecnológico-Informacional de los Asuntos Militares para examinar la evolución tanto táctica como doctrinal de la guerra en el siglo XXI. Asimismo, se presta especial atención a los componentes, funcionalidad y escenarios de aplicación del nuevo armamento.

Este estudio también se orienta al análisis de operaciones militares que consideraron al ciberespacio parte integrante de la guerra moderna, tomando como referencia el caso Stuxnet, esto a pesar de representar un evento en dónde sólo se involucraron ciberataques aislados. Es decir, que no formó parte de estrategias militares complejas. Así, por ejemplo, se hace referencia a casos como, el ya mencionado, Stuxnet, Flame, *Parastoo* y entre otros.

A fin de ilustrar esta nueva etapa en la práctica de la guerra, se toma como caso de estudio Medio Oriente con una delimitación temporal que va del 2001 al 2015. Esto debido al gran número de enfrentamientos bélicos que ha sufrido la región, la multiplicidad de actores involucrados en tales conflictos, y las repercusiones generadas por la aplicación de nuevas tácticas militares desde la segunda mitad del siglo XX.

Se parte del año 2001 debido a que los ataques del 9/11 en Nueva York transformaron los paradigmas de seguridad en todo mundo. Especialmente Medio Oriente experimentó la modificación de los imperativos de seguridad estadounidenses y la aplicación de nuevo armamento en las tácticas militares, intervención que generó una serie de acontecimientos cuyos efectos perduran en la región. Asimismo, se analiza el empleo de nuevas tecnologías bélicas por parte

de actores no estatales y el papel que poseen las compañías especializadas en seguridad en el desarrollo de la guerra moderna.

Esta investigación tiene como objetivo responder a la siguientes preguntas ¿Cuáles son las consecuencias generadas por la Revolución Tecnológico Informacional de los Asuntos Militares y el desarrollo de armamento cibernético en Medio Oriente?, ¿Cuál es el papel de la Revolución Tecnológico Informacional de los Asuntos Militares y del armamento cibernético en la teoría militar y en las Relaciones Internacionales?, ¿Qué clase de operaciones ofensivas y defensivas resultan de la adopción de un paradigma digital en la doctrina militar?, ¿Cuáles son las causas del uso de ciberarmas en Medio Oriente y qué consecuencias genera a nivel regional?

Para lo cual se han establecido los siguientes objetivos:

- Analizar la Revolución Tecnológico Informacional de los Asuntos Militares y el desarrollo de armamento cibernético tomando como caso de estudio Medio Oriente del periodo de 2001 a 2015.
- Indagar en el desarrollo histórico de la guerra recurriendo a estudios clásicos realizados por Carl Von Clausewitz y Basil Liddell Hart, así como a proposiciones modernas presentadas por Alvin y Heidi Toffler, Martin L. Van Creveld y Rupert Smith, a fin de evaluar desde el enfoque neorrealista de Kenneth Waltz el impacto de la Revolución Tecnológico Informacional de los Asuntos Militares en las Relaciones Internacionales.
- Examinar la evolución del armamento convencional derivado de la adopción de nuevas tecnologías e Internet, así como el desarrollo y aplicación de nuevas tácticas de combate con el objetivo de evaluar el grado en el que la doctrina militar ha sido alterada.
- Estudiar la trasformación de la naturaleza y conducción de conflictos en Medio Oriente mediante la revisión de enfrentamientos en dicha zona que involucren el uso de ciberarmas como elemento estratégico e identificar las consecuencias de su uso a nivel regional.

El enfoque teórico bajo el que se desarrolla esta investigación es el neorrealismo. De esta forma, se adoptan las proposiciones presentadas por Kenneth Waltz respecto a la influencia del entorno en el comportamiento y evolución del sistema internacional. Desde esta perspectiva, entre sus diversos intereses, los Estados otorgan prioridad a su propia supervivencia. Sin embargo, a pesar de los intereses particulares los Estados tienden a crear alianzas, aunque también surgen carreras armamentistas. Esta aproximación es la que mejor responde a esta investigación dado que muestra que en el marco de un sistema anárquico los Estados perciben el incremento en las capacidades militares de otra nación como una amenaza a su propia seguridad, incentivando la evolución tanto del armamento como de la práctica belicista.

La hipótesis que sustenta este trabajo es que la Revolución Tecnológico Informacional de los Asuntos Militares ha transformado la concepción, generación y empleo de la fuerza en el siglo XXI. Lo cual deriva en la compra, desarrollo y empleo de armas cibernéticas, y su articulación junto al armamento convencional para potenciar el impacto de las operaciones militares en Medio Oriente, así como, en el aumento de recursos destinados a la adquisición y uso de medios de alta tecnología por parte de las fuerzas armadas.

Las hipótesis secundarias sostienen que:

1) La Revolución Tecnológico Informacional de los Asuntos Militares y el empleo de armamento cibernético generan un impacto en la correlación de fuerzas dentro del escenario internacional. Por esta razón, la teoría militar se ve obligada a incorporar el uso de nuevas armas en sus planteamientos estratégicos con el fin de potencializar la capacidad de los países en donde las fuerzas armadas emplean armamento cibernético.
2) Las operaciones ofensivas y defensivas que resultan de la adopción de un paradigma digital en la doctrina militar se materializan en acciones combinadas en donde las batallas se libran por ambos frentes (tanto en el espacio virtual como en el tangible), la incorporación de alta tecnología al armamento convencional, el

surgimiento de ejércitos electrónicos, el desarrollo de ciberarmas y su incorporación al ejército.

3) El uso de ciberarmas en las estrategias militares en Medio Oriente es producto del enfrentamiento entre gobiernos y fuerzas no estatales que obliga a los Estados a mantener actualizada la doctrina militar, también es resultado de la capacidad económica y táctica de países como Estados Unidos, Israel, Irán, Turquía, Siria, Rusia entre otros, y de la incursión de Empresas Militares Privadas en la región. La consecuencia del uso de ciberarmas en Medio Oriente presenta como curso de acción la generación de alianzas estratégicas para su desarrollo y empleo sin un marco normativo.

La presente tesis está compuesta por tres capítulos. El primero (el marco teórico), analiza la evolución de la guerra partiendo de los principios presentados por Carl Von Clausewitz sobre la guerra moderna y su reconceptualización en la época contemporánea. De igual forma, se abordan las observaciones realizadas por Basil Liddell Hart sobre la estrategia militar de la aproximación indirecta a fin de rescatar el papel de las comunicaciones en los escenarios de conflicto. Posteriormente, se examina el concepto de "ciber-relaciones internacionales" propuesto y desarrollado por el *Belfer Center for Science and International Affairs* y el Instituto Tecnológico de Massachusetts. Seguido de un estudio de la teoría neorrealista acudiendo a la interpretación de Kenneth Waltz en *Theory of International Politics*, hasta llegar al análisis de la guerra moderna en Medio Oriente y la reexaminación del choque de civilizaciones propuesto por Samuel Huntington en el marco de la era digital.

El segundo capítulo (marco conceptual) está dedicado a examinar la aparición y desarrollo del término "Revolución de los Asuntos Militares" utilizado por Andrew W. Marshall (ex director de la *Oficina de Net-Assessment* del Pentágono) en la década de los 80 y su evolución a través del tiempo hasta lo que hoy se conoce como Revolución Tecnológico Informacional de los Asuntos Militares. En adición, se estudia la incorporación del ciberespacio en el ámbito militar, profundizando en las operaciones ofensivas, las tácticas defensivas y la conducta de actores estatales y no estatales. Asimismo, se analiza la incorporación de alta tecnología en el

armamento convencional y el desarrollo de nuevo arsenal, prestando especial atención a los sistemas de inteligencia, vigilancia y reconocimiento; armamento inteligente y sistemas de defensa antimisiles, así como a los aviones no tripulados. De la misma manera, se examinan los indicadores y aspectos de la guerra cibernética y el desarrollo de ciberarmamento.

En el tercer y último capítulo, se desarrolla el estudio de caso, partiendo del análisis del concepto “Medio Oriente”, el papel de los asuntos militares en la región y las transformaciones en la seguridad y defensa experimentados tras el 11 de septiembre de 2001. Bajo esta misma línea, se analizan las características de la Operación Tormenta del Desierto (1991) como antecedente de la Revolución Tecnológico Informacional de los Asuntos Militares, para dar paso al estudio de las potencias tecnológico-militares en la región, sus agencias de inteligencia y el desarrollo de Centros de Respuesta a Ataques Cibernéticos. Seguido de la examinación de dos importantes operaciones que demuestran la evolución en la conducta de la guerra: la Operación Libertad para Iraq (2003) y la Operación Huerta (2007). Igualmente, se presenta el caso de Daesh y el empleo de Internet con fines de propaganda y reclutamiento, así como el uso de nuevas tecnologías bélicas por parte de la organización terrorista en el marco de la Guerra civil en Siria (2011-2015). Este último apartado, recurrió a herramientas metodológicas de etnografía digital para llevar acabo la observación de la narrativa y comportamiento del Daesh en los videos colocados en línea. Finalmente, se presentan las conclusiones.

En cuanto a la metodología empleada, en el primer capítulo se recurrió a material bibliográfico, principalmente a obras clásicas en el plano de la defensa. De esta forma se consultaron los análisis realizados por Clausewitz y Liddell Hart en torno a la guerra moderna. Para ilustrar el término “sociedad de la información” se consultó el trabajo desarrollado por el sociólogo Manuel Castells. Mientras que en el ámbito de las relaciones internacionales y para el desarrollo del marco teórico se recurrió a obras como *International Relations and Security in the Digital Age* de Johan Eriksson y el Dr. Giampiero Giacomello y *Cyberpolitics in*

International Relations de Nazli Choucri. Por su parte, la investigación de la guerra moderna en Medio Oriente y la reinterpretación del "choque de civilizaciones" se realizó con apoyo de material bibliográfico perteneciente a Ashraf Tahir, Mian Muhammad, Johan Eriksson, Martin Van Creveld, Rupert Smith, entre otros.

Para el segundo capítulo se consultaron fuentes especializadas en el ámbito militar. De este modo se emplearon informes, tesis, material bibliográfico y material hemerográfico enfocado en el desarrollo y aplicación de armamento altamente tecnológico. Entre las fuentes bibliográficas figuran: "Cybervictory: The efficacy of Cyber Coerción" de Brandon Valeriano y Ryan C. Maness; "Innovación y Revolución en los Asuntos Militares: una perspectiva no convencional" de Javier Jordán, *The Maturing Revolution in Military Affairs* de Barry D. Watts; *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político* de John Arquilla y David Ronfeldt, entre otros. También, se recurrió a centros de investigación e instituciones académicas como: el Instituto Tecnológico de Massachussets (EE. UU), la Escuela de Guerra del Ejército en Tierra (España), el Grupo de Estudios en Seguridad Nacional (España), el *Cooperative Cyber Defence Centre of Excellence* de la OTAN (Estonia), el *Stockholm International Peace Research Institute* (Suecia), la Universidad de Oxford (Reino Unido), entre otros.

En el tercer y último capítulo, se consultaron fuentes variadas. Desde bases de datos, agencias de noticias y centros de investigación de diversas partes del mundo. Para el análisis conceptual e histórico de Medio Oriente se recurrió al trabajo de académicos y expertos como Bernard Lewis; Edward Said; Nuri Osman Özalp; Carl L. Brown; Anoushiravan Ehteshami; Azzedine Rakkah; María de Lourdes Sierra Kobeh, entre otros. Para la revisión histórica de los asuntos militares en la región se acudió a análisis realizados por el Banco Mundial, el Grupo de Estudios de Historia Militar, el Consejo de Seguridad de la Organización de Naciones Unidas, entre otros. Así como a agencias de noticias como Al-Monitor, *The New York Times*, *The Gulf Rising*, *Al Jazeera*, *RT*, *Der* Spiegel, y a revistas como Uluslararası İlişkiler Dergisi y *Journal of Strategic Studies*.

Esta investigación contó con el apoyo de la Doctora Karina Bárcenas Barajas del Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México como guía en la observación de la actividad de Daesh en Internet y en el análisis de la narrativa del material audiovisual de la organización terrorista. Por su parte, el Doctor Brandon Valeriano de la *Marine Corps University* colaboró al análisis entorno a las tácticas defensivas y ofensivas en línea. Asimismo, el Doctor José Julio Fernández Rodríguez orientó el desarrollo del segundo capítulo de este proyecto durante la estancia de investigación en el Centro de Estudios de Seguridad de la Universidad de Santiago de Compostela de septiembre a diciembre de 2016.

CAPÍTULO 1. EVOLUCIÓN HISTÓRICA DE LA TEORÍA MILITAR

El recurso de la guerra ha sido una constante en la historia de las relaciones internacionales, su rol en la conformación de los Estados-nación ha sido determinante. En este sentido, la evolución misma de las prácticas militares refleja en buena medida la transformación de las sociedades y los gobiernos. Incluso el ordenamiento internacional moderno es producto del enfrentamiento entre diversos reinos, que durante el siglo XV derivaron en la adopción de las disposiciones contempladas en los tratados de paz de Osnabrück y Münster (el 15 de mayo y 24 de octubre de 1648 respectivamente), dando inicio así a la Paz de Westfalia y al establecimiento del sistema de equilibrio de poder en Europa.[1]

Sin embargo, la influencia de la guerra en la conformación del sistema internacional también recibe una fuerza que actúa en sentido contrario. Es decir, la influencia del entorno sobre las prácticas belicistas. De esta manera, los planteamientos operativos y armamentistas son determinados también por la evolución factores como la ciencia, la economía y por supuesto la política. En la actualidad, un factor que ejerce una importante influencia en el carácter de los enfrentamientos bélicos es la revolución de las Tecnologías de la Información y la Comunicación (TIC).

Con el arribo de Era digital la naturaleza de la guerra se transformó, experimentando un cambio en dos direcciones:

- En forma horizontal - busca aumentar nociones como alcance e intensidad, abarcando nuevas áreas e incrementando la profundidad de las operaciones.
- En forma vertical - modificando estructuras militares y cadenas de mando.

De igual forma, el armamento también ha experimentado importantes transformaciones, pues al analizar los conflictos bélicos bajo una perspectiva neorrealista, es posible afirmar que los Estados se encuentran en una posición de vulnerabilidad ante la posibilidad constante del uso de la fuerza por parte de los

[1] Kissinger, Henry. (1996). *Diplomacia*. México: Fondo de Cultura Económica

otros actores.[2] Esta circunstancia, genera una competencia continua que busca alcanzar paridad de fuerzas y de recursos militares, incentivando la producción y perfeccionamiento de armamento.

Por su parte, el campo de batalla también ejerce una fuerte influencia, pues al tiempo en que representa un desafío a superar, impulsa el desarrollo de nuevas estrategias. En la posmodernidad, el teatro de la guerra ha adoptado un nuevo espacio de acción: el espectro cibernético. Esto ha dado como resultado el desarrollo de distintos tipos de enfrentamientos. Sin embargo, la naturaleza de la web es compleja, pues representa tanto un espacio como una herramienta que el pensamiento militar moderno debe tomar en cuenta en sus planteamientos estratégicos presentes y futuros.

No obstante, para entender la actualidad es necesario recurrir al pasado, a fin de comprender la forma en la que la teoría militar ha otorgado preponderancia al empleo de las comunicaciones en general y al de la ciencia informática en particular.

Del mismo modo, es preciso examinar la transformación progresiva de las formas de hacer guerra, para ello se recurre a planteamientos clásicos presentados por Karl Von Clausewitz (1820) y Basil Liddell Hart (1941) hasta llegar a la proposición de una “guerra estratégica para el ciberespacio” desarrollada por el coronel Gregory Rattray (2001).

1.1 LA TEORÍA DE LA GUERRA EN LA SOCIEDAD INDUSTRIAL: KARL VON CLAUSEWITZ Y LIDDELL HART

Se conoce como sociedad industrial a aquella derivada de dos hechos trascendentales: la Revolución Industrial y la Revolución Francesa. Cada uno de estos acontecimientos estuvo acompañado de una amplia gama de factores que incidieron de forma directa e indirecta en la conformación de las estructuras y dinámicas sociales de finales del siglo XVIII y principios del XIX.

A nivel macro, se experimentó el surgimiento del Estado moderno y del propio sistema internacional, impulsados por un fuerte fenómeno de corte económico: el

[2] Griffiths, Martin. (1992). Fifty Key Thinkers in International Relations. EE. UU: Routledge.

capitalismo y su expansión transcontinental. La Revolución Industrial, pieza esencial de ascenso del capitalismo cuyas bases se sitúan en Inglaterra a finales del siglo XVII, engloba la evolución de la productividad y de la producción, acompañadas por la innovación en sectores estratégicos como los transportes. Surgió entonces, la producción en masa y toda una transformación de las actividades industriales. Estas transformaciones produjeron un impacto en otros sectores dando lugar a una revolución social. En este punto se transitó de una comunidad campesina medieval a una sociedad industrial, caracterizada por el traslado del campesinado a la ciudad, que terminó propiciando la conformación del proletariado industrial urbano.[3]

Por su parte, la Revolución Francesa, cuyo punto emblemático es la toma de la Bastilla el 14 de julio de 1789, estuvo enmarcada por demandas de renovación y reforma del Estado orientadas a la consecución de libertad política y de consciencia, así como a alcanzar la unidad nacional. La Revolución Francesa representa los efectos en el plano social y cultural de la Revolución industrial, emanada de una profunda transformación en el ámbito de las ideas que comenzó con la Ilustración. De esta forma, los cuestionamientos del hombre sobre el mundo que le rodeaba y sobre la autoridad que le regía, le llevó a darse cuenta de su poder en el rumbo de su propio destino y emergieron, entonces, nociones como la libertad, la igualdad y la fraternidad.[4]

En resumen, los cambios en el plano científico y económico significaron también el inicio de una nueva etapa en la relación del hombre con su entorno, transformando las estructuras políticas, los ordenamientos sociales y la forma de hacer guerra. Lo anterior, en su conjunto dio lugar al desarrollo de nuevas interpretaciones sobre la práctica belicista.

Sin embargo, la transformación de la práctica de la guerra ya había sido analizada tiempo atrás. En ese entonces, los estudios se enfocaron en el rol decisivo del uso de la fuerza para obtener la victoria en el combate. Con el paso del tiempo, filósofos

[3] Kaplan, Marcos. (2000). *Ciencia, Estado y Derecho en las Primeras Revoluciones Industriales.* México: Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas.
[4] Hobsbawm, Eric. (2009). *La Era de la Revolución, 1789-1848.* Buenos Aíres: Crítica.

y militares presentaron importantes aportes sobre el desarrollo del pensamiento estratégico como factor esencial dentro de las prácticas de guerra.[5]

Entre los primeros análisis figura Tzu Sun Tzu con *El arte de la Guerra* (500 a.C. aprox.), más adelante personajes de la talla de Nicolás Maquiavelo, Thomas Hobbes e Immanuel Kant se dedicarían a examinar tanto las características como los objetivos de la dicha práctica ancestral.[6]

No obstante, el esfuerzo más sobresaliente es el realizado por el militar e historiador prusiano Karl Von Clausewitz, al considerarse uno de los trabajos más completos y sintetizadores.[7] Los principios presentados por el estratega han tenido un efecto histórico sostenido en las prácticas militares. En su obra, *De la guerra* (1820) Clausewitz fija su atención en diversos aspectos de la práctica belicista considerando tanto la naturaleza, fines y medios como el papel de la fuerza y de la información en el combate.

Desde el pensamiento de Clausewitz la guerra es un hecho social y, por tanto, inevitablemente ligada al hombre y al propio sistema internacional. El fin último del combate es abatir al adversario con el objetivo de doblegar su voluntad y en el contexto de la era industrial la fuerza física es el principal medio para conseguirlo.

Casi medio siglo después de los postulados presentados por Clausewitz, Basil Henry Liddell Hart desarrolló sus propios aportes. El militar, historiador y teórico inglés en su obra *La Estrategia de la Aproximación Indirecta* de 1941 realiza un importante examen a la teoría militar del siglo XX, en ella lanza una crítica a la conveniencia de un ataque frontal y su efectividad en el contexto de la guerra.

La obra de Liddell Hart se centra en el análisis de numerosas contiendas históricas, especialmente las acaecidas durante la Primera y Segunda Guerra Mundial. Desde esta perspectiva, la aproximación indirecta se aprecia como una

[5] Benítez Manaut, Raúl. (1986). "El pensamiento militar de Clausewitz". *Revista Mexicana de Ciencias Políticas y Sociales*. Año XXXII. Nueva Época octubre-diciembre 1986, no. 126, pp. 97-123.
[6] *Ídem*
[7] *ídem*

verdad filosófica, pues encarna la eficacia del pensamiento para otorgar al uso de la fuerza mayor efectividad.

Impulsado quizá por los efectos de los enfrentamientos en Somme y Passchendale, de los que formó parte, Liddell Hart se concentra en evitar el uso de enfrentamientos directos cuyos costos humanos y económicos resultan cada vez más inadmisibles para cualquier nación.[8]

En adición, el militar inglés será quien apoye las nociones presentadas por J. F. C. Fuller, referentes al uso de unidades mecanizadas y blindadas en el campo de batalla, especialmente con el fin de destruir las comunicaciones y dañar los abastecimientos del enemigo.[9] A diferencia de los postulados de Fuller, que se inclinan más al uso de tanques con actuación independiente, Liddell Hart prefiere el uso de unidades combinadas que incorporen en la fuerza terrestre tanto el uso de soldados como de tanques blindados.[10]

Los escritos de Liddell Hart desde finales de 1920, que toman como base las propuestas de Fuller retoman el uso de unidades blindadas con el fin de utilizarse como fuerzas de choque, buscando reducir el costo humano de los enfrentamientos armados. De nueva cuenta, y como Clausewitz señaló, el rol de las comunicaciones resulta esencial, por lo que el uso de unidades mecanizadas se orientará a atacar las comunicaciones y a aislar al enemigo.[11]

En síntesis, los trabajos de Clausewitz y Liddell Hart se centran en el análisis de enfrentamientos históricos, uno en las guerras napoleónicas y el otro en las batallas enmarcadas en la Primera y Segunda Guerra Mundial. Asimismo, tanto Clausewitz como Liddell Hart se interesan por el legado que los hechos pasados proveen al pensamiento militar moderno. Clausewitz concentrado en la superioridad estratégica de la defensa y en la importancia del uso de la fuerza física, y Liddell

---

[8] Liddell Hart, Basil. (1989). *Estrategia: la aproximación indirecta*. Madrid: Ministerio de Defensa, Secretaría Gral. Técnica.

[9] Puyana García, Gabriel. (2003). "Teorías de la Guerra en Moltke y Liddell Hart". *Revista de Estudios Sociales*, no. 15, junio de 2003, 109-121.

[10] Centro de Estudios Superiores Navales. (1992). "Grandes Pensadores Estratégicos". *Revista del Centro de Estudios Superiores Navales*, pp.57-67.

[11] *ídem*

Hart en el desarrollo de nuevos planteamientos que reduzcan los enfrentamientos directos y el costo que estos acarrean. Empero, los aportes más significativos para este trabajo se sitúan en los conceptos de "guerra moderna" de Clausewitz y de "aproximación indirecta" de Liddell Hart.

1.1.1. Sobre la guerra moderna

La concepción moderna de la guerra en el pensamiento clausewitziano se materializa en una trinidad conformada por la hostilidad del pueblo, la incertidumbre del ejército y objetivo del gobierno, cada uno de estos con magnitud variable. La guerra, por tanto, pertenece al dominio de la inteligencia pura.[12]

Es importante recalcar que en el contexto histórico de Clausewitz, finales del siglo XVI y principios del XVII, las campañas militares involucran esencialmente el choque de las fuerzas de un Estado contra las de otro, por lo que el domino del territorio y la destrucción de fuerzas enemigas son los fines últimos de la guerra.[13]

Uno los aportes más sobresalientes de la obra *De la guerra*, es la orientación de las acciones bélicas, las cuales de acuerdo con el pensamiento clausewitziano han de encausarse allí donde se genere más daño al enemigo. Otra de las propuestas más importantes, es la incorporación del pueblo como factor esencial en las campañas, pues la guerra más que un enfrentamiento entre individuos es un todo organizado que integran muchas partes.[14]

Por su parte, el rol de la información ya desde la era industrial va a tener una importancia vital. Los datos del entorno, las dificultades para llevar la teoría a la práctica y la incertidumbre en el combate configuran lo que el estratega presenta como la fricción de la guerra.[15]

---

[12] Von Clausewitz, C. (2005). *De la guerra*. España: La Esfera de los Libros.
[13] *ídem*
[14] Benítez Manaut, *Op. Cit.*
[15] Watts, Barry D. (1996). Clausewitzian Friction and Future War. Institute for National Strategic Studies. National Defense University. [En línea]. Disponible en: <http://www.clausewitz.com/readings/Watts-Friction3.pdf>.

A grandes rasgos, la fricción se refiere a los efectos de la realidad en las ideas e intenciones de la operación militar.[16] La niebla de la guerra, por tanto, consiste en la confusión predominante en el campo de batalla, específicamente hace referencia a la existencia de información imprecisa que imposibilita la claridad de acción.[17]

Esta última propuesta cobrará un nuevo significado a la llegada de la Era digital, pues con el desarrollo de sofisticados sistemas de recolección, distribución, procesamiento y resguardo de información militar se produce también una transformación en el impacto de la niebla en la guerra moderna.

1.1.2. La estrategia de la aproximación indirecta

De acuerdo con el pensamiento de Liddell Hart existen dos clases de estrategia[18]: la aproximación directa y la indirecta, cada una de ellas ─al modo que lo plantea Clausewitz─ busca doblegar la voluntad del enemigo. En la primera, la fuerza física es primordial. En la segunda, la base son las acciones estratégicas con un eficiente impacto psicológico, en donde la fuerza se deja de lado y el fin último consiste en doblegar la moral de adversario.[19]

La estrategia de la aproximación indirecta también plantea que el rodeo más grande puede ser el camino más corto a la victoria. En este aspecto, Liddell Hart establece: “El moverse a lo largo de la línea de expectativa natural consolida el equilibrio del oponente y, al cohesionar ese equilibrio, aumenta su poder de resistencia.”[20]

En su obra, Liddell Hart analiza doce enfrentamientos que produjeron un efecto determinante en la historia de Europa. Dichos conflictos, se traducen en más de 280

[16] *ídem*
[17] Von Clausewitz, *Óp. Cit.*
[18] Se entiende por estrategia a el arte utilizado para que la fuerza concurra a alcanzar los límites de la política. Fuente: Puyana (2003)
[19] Liddell Hart. (2014), *Óp. Cit*
[20] Liddell Hart. (2014), *Óp. Cit.,* p. 13-

campañas, de las cuales sólo seis de ellas obtuvieron un resultado decisivo siguiendo la estrategia de aproximación directa.[21]

Respecto al corte comunicaciones Liddell Hart (1941) plantea, que cuanto más cerca de la fuerza se produzca el golpe más inmediato será su efecto, por lo que el daño a las comunicaciones también puede generar un fuerte efecto psicológico en la mente de las fuerzas contrarias.

En resumen, la estrategia de la aproximación indirecta busca la dislocación del equilibrio físico y psicológico de las fuerzas oponentes. La ejecución de esta estrategia debe ser indirecta, intencional y fortuita.[22] En palabras de Liddell Hart, la mejor aproximación indirecta es aquella que: "atrae o incita al oponente a dar un paso en falso de modo que […] su propio esfuerzo se convierte en la palanca de su derrota."[23]

De esta manera cada enfrentamiento bélico a través de la historia deriva en la generación de conocimiento militar. Para explicar esta transformación Alvin y Heidi Toffler (1993) proponen un modelo de evolución social que impacta en la forma de hacer guerra. Bajo este enfoque, la sociedad ha transitado por tres etapas determinadas por la adopción de nuevos modelos económicos. Dentro de este modelo aparecen tres tipos de sociedad pertenecientes a tres etapas históricas denominadas "olas".[24]

La sociedad enmarcada por la Revolución Industrial, dentro de la cual Clausewitz y Liddell Hart realizaron sus aportaciones, es denominada "Segunda Ola". La cual,

[21] Estas seis campañas son las de Isso, Gaugamela, Friedland, Wagram, Sadowa y Sedan. Fuente: Liddel Hart (2014)
[22] Liddell Hart. (2014), *Óp. Cit.,*
[23] Liddell Hart. (2014), *Óp. Cit.,* p. 18
[24] Las tres etapas históricas que Alvin y Heidi Toffler son: La primera ola, se caracteriza por el descubrimiento de la agricultura y la sociedad resultante se encuentra fuertemente apegada a la tierra. Mientras que en la guerra se utilizan herramientas primitivas, el combate es cuerpo a cuerpo y la capacidad de destrucción es limitada. La segunda ola, está determinada por la Revolución Industrial. Se trata de la era de la destrucción en masa, en ella la movilización y el reclutamiento se hace a mayor escala. De esta forma, surge la uniformidad y la especialización en las fuerzas armadas, y se desvela el máximo potencial destructivo: la bomba atómica, y la industrialización de la muerte. La tercera ola, en ella se experimenta la revolución tecnológica y aparece la llamada "sociedad del conocimiento" y en la guerra aparecen nuevos modelos acción y armas altamente tecnológicas. Fuente: Toffler, Alvin y Heidi. (1993).

es definida como de la era de la destrucción en masa, en ella la movilización y el reclutamiento se realizan a gran escala. Lo cual deriva en la uniformidad y la especialización de las fuerzas armadas, y se desvela el máximo potencial destructivo: la bomba atómica y la industrialización de la muerte.[25]

1.2. DE LA SOCIEDAD INDUSTRIAL A LA SOCIEDAD DE LA INFORMACIÓN

El tránsito de una sociedad basada en la producción en serie a otra basada en el conocimiento supone también un cambio en las prácticas de guerra.[26] Así, Alvin y Heidi Toffler señalan que la revolución tecnológica fue la fuerza impulsora de esta nueva etapa, en donde el tipo de sociedad resultante es conocida como "sociedad informacional".

En el plano sociológico Manuel Castells (2002) describe a este tipo de sociedad[27] como una nueva estructura social de carácter global, enmarcada en un nuevo modelo de desarrollo, cuya base de producción es la generación de conocimiento, el procesamiento de información y la transmisión de símbolos.

Dentro de la sociedad informacional, la guerra no sólo se libra en el frente de batalla, pues aparecen nuevos espacios de combate y la evolución del conocimiento permite el desarrollo de armas inteligentes.[28]Al mismo tiempo, la complejidad del nuevo entorno modifica la estructura militar demandando la integración de sistemas. De esta manera, la transformación económico-social impacta de forma general en el poder militar y en la tecnología bélica. [29]

A su vez, la noción de poder evoluciona, otorgando a la información un papel central y surgen conceptos como *ciberpoder*.[30] En cuanto a la tecnología bélica, se

[25] Toffler, Alvin y Heidi. (1993). War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little Brown.
[26] *Ídem.*
[27] Se adopta el concepto "sociedad informacional" y no "sociedad de la información" debido a la incorporación del elemento "poder" en los análisis del primer término.
[28] "Armas inteligentes" refiere a aquellas que implementan varios dispositivos tecnológicos, por ejemplo, sensores de proximidad, imanes, identificación por radio frecuencia, microchips y aplicaciones biométricas, para mejorar su funcionamiento. Fuente: BBC (2014).
[29] Toffler, Alvin y Heidi. *Óp. Cit.*
[30] Se entiende por Ciberpoder a la capacidad de utilizar el ciberespacio para crear ventajas y eventos de influencia en otros entornos operativos y a través del uso de instrumentos de poder. Fuente: Nye (2010).

alcanzan nuevos límites y el campo de acción se traslada también al ámbito cibernético, dando lugar al surgimiento de la *ciberguerra*.[31]

En esta nueva ola, el conocimiento es la materia principal que hace que todo el sistema funcione. Sin embargo, no se trata de la sustitución de un modelo de sociedad por otro, dejado al anterior inactivo, sino que es posible la coexistencia de diferentes modelos de sociedad, lo cual produce un choque de olas que se traduce en enfrentamientos entre diversas sociedades con sus propias técnicas belicistas.[32]

Retomando a Clausewitz y su referencia respecto al cambio en la forma de hacer guerra a través del tiempo y la necesidad de desarrollar una teoría militar que responda a las demandas de cada etapa histórica, es posible afirmar que en la posmodernidad el desarrollo de armas inteligentes requiere también de soldados tecnológicamente capaces y de una teoría que abarque la totalidad de los cambios generados.[33]

Esta última etapa se encuentra todavía en desarrollo, por lo que aún es complicado predecir el rumbo que la sociedad y la guerra han de tomar. Sin embargo, los desafíos hasta el momento son claros, la innovación tecnológica e Internet se han convertido en el *Leitmotiv*[34] de la época contemporánea, sus efectos no se limitan sólo al plano social, su impacto en el ámbito de la seguridad demanda la estructuración de nuevas tácticas ofensivas y defensivas, así como de la adecuación de la teoría militar.

1.2.1. El conocimiento científico-tecnológico como elemento de poder militar

En *Las Guerras del Futuro* Alvin y Heidi Toffler hacen referencia a los "guerreros del saber" quienes se encargan de trabajar con el conocimiento a fin de prevenir y ganar guerras. Surgen, entonces, militares intelectuales encaminados a alcanzar

[31] Se entiende por Ciberguerra a la acción equivalente a un ataque armado, o uso de la fuerza, en el ciberespacio ejecutada por un Estado en contra de otro Estado, que puede desencadenar una respuesta militar con un uso proporcional de fuerza cinética. Fuente: Theohary y Rollins (2015).
[32] Toffler, Alvin y Heidi. *Óp. Cit.*
[33] Toffler, Alvin y Heidi. (1994). *Las Guerras del Futuro.* Century. España: Plaza & Janes Editores, S.A.
[34] De acuerdo con Henry Kissinger el *Leitmotiv* consiste en un conjunto de creencias que explican el universo, que inspiran y consuelan al individuo ofreciendo una justificación a la multiplicidad de acontecimientos que lo afectan. Fuente: Orden Mundial (2016).

una estrategia de alto nivel a través de la obtención y procesamiento de información relevante sobre el adversario.[35]

De esta forma, el conocimiento científico-tecnológico, traducido en innovación, da como resultado el perfeccionamiento y desarrollo de nuevo armamento, la concentración en determinados sectores de la investigación militar, y la inclusión de nuevos espacios de acción en los planteamientos estratégicos, transformando de manera significativa el panorama de seguridad del siglo XXI.

En la era de la información el papel de la inteligencia cobra renovada importancia. El conocimiento y los datos ocupan un lugar central en la capacidad de destrucción y en la disminución de daños.[36] El logro principal de la guerra del siglo XXI es su supuesta capacidad para reducir o eliminar las bajas y daños colaterales, proposición que será examinada a lo largo de este trabajo.

En este escenario, el dominio del espectro cibernético no es exclusivo de las fuerzas armadas, pues aparecen los denominados piratas informáticos, también conocidos como *hackers*[37], cuyas habilidades en el manejo de las redes informáticas les otorgan la capacidad de irrumpir en los sistemas de seguridad más sofisticados. En consecuencia, el conocimiento se aleja del campo exclusivo de las fuerzas armadas y surgen actores no estatales con la capacidad de desafiar las medidas de seguridad más avanzadas.

De forma general, en el plano de las relaciones internacionales, el papel del conocimiento ha sido examinado por Richard N. Rosecrance en su *obra The Rise of the Virtual State* (1999). En este trabajo, Rosecrance analiza y pone a prueba los fundamentos de la política tradicional entre naciones, retomando cuestiones como el territorio, el comercio y el valor militar, las cuales enfrenta a otros conceptos como

[35] Toffler, Alvin y Heidi. *Óp. Cit.*
[36] *Ídem.*
[37] Un *hacker* es una persona que utiliza sistemas computarizados para obtener acceso no autorizado a redes cibernéticas. Fuente: Oxford Dictionaries (2016).

la educación, las habilidades y la administración del conocimiento, configurando lo que denomina "brain power".[38]

A grandes rasgos, Rosecrance considera al conocimiento como una fuente fundamental de poder nacional y de efectividad social. En ese mismo análisis, reflexiona también sobre el aspecto económico del *Estado virtual* y el papel de corporaciones como contraparte de la autoridad estatal.[39]

Así, dentro de la denominada Era digital[40] el desafío más grande es transformar la información en conocimiento. Después de todo, fue precisamente el desarrollo del conocimiento científico lo que dio paso al surgimiento de la red de redes.

1.2.2. La integración del quinto dominio

En el campo de la seguridad se conoce como "quinto dominio" al espectro cibernético (el ciberespacio), pues al igual que el mar, el aire, la tierra y el espacio constituye un campo de acción para las operaciones militares.

Definir claramente el quinto dominio no es una labor sencilla. En los estudios de seguridad y defensa existen proposiciones que incluyen en esta denominación al espectro electromagnético[41] incluyendo ondas de radio, microondas y rayos láser, quienes finalmente son responsables de la comunicación electrónica, base del funcionamiento de la red de redes. En suma, una amplia gama de operaciones militares depende de la función electromagnética, por ejemplo: la inteligencia, la vigilancia y el reconocimiento, además de los sensores tácticos.[42]

Sin embargo, al unir bajo el quinto dominio el uso de componentes electrónicos y el espectro electromagnético, se crean dificultades de carácter doctrinal que

---

[38] Rosecrance, Richard. (Julio 1, 1996). "The Rise of the Virtual State: Territory Becomes Passé". *Foreign Affairs*. Vol. 75, no. 4, pp. 45-71.
[39] *Ídem*.
[40] "Era Digital" se refiere al tiempo presente, en donde la mayoría de la información se presenta en forma digital, especialmente en comparación con otras épocas en donde las computadoras no eran utilizadas. Fuente: Cambridge Dictionaries Online (2016).
[41] Por ejemplo, Daniel Kuehl en su obra *Defining Information Power*.
[42] Butler, Sean C. (2013). "Reenfoque del Pensamiento de la Guerra Cibernética". *Air & Space Power Journal*, pp. 86-94. [En línea]. Disponible en: <http://ww w.airpower.maxwell.af.mil/apjinternational/apjs/2013/20132/2013_2_09 _but ler_s.pdf>. (Consulta 28/05/16).

consideran bajo la misma denominación acciones tan diametralmente distantes como lo son el funcionamiento de los radares y las operaciones cibernéticas. Sin embargo, la integración del ciberespacio como un campo de acción diferente al tradicional constituye un paso adelante en el pensamiento militar moderno.[43]

La inclusión progresiva del ciberespacio en las estrategias de seguridad se ha extendido por diversos países, al grado en el que se ha alentado a militares y a agencias de inteligencia a desarrollar una doctrina especial.[44]No obstante, la dificultad aparece cuando se pretende trasladar los principios aplicables al ámbito tradicional al entorno digital, de ahí que expertos como Charles H. Hall (2011), reconozcan la diferencia de los factores operacionales en el ciberespacio. Es decir, la naturaleza única de Internet hace que factores como la extensión, el tiempo y la fuerza sean difíciles de calcular. De acuerdo con Hall, tales elementos deben ser cuidadosamente equilibrados con el fin de alcanzar los objetivos en el combate.

En el contexto de la guerra digital, Internet representa tanto como herramienta y espacio de acción.[45]En este aspecto, y de acuerdo con Hall, la complejidad en la extensión del ciberespacio le acerca más a la guerra irregular que a la convencional.

Aunado a ello, la dificultad para establecer fronteras demanda la coordinación de diferentes secciones militares para ejecutar una operación. Además, existe otro problema: la diversidad de actores, pues en el espacio virtual convergen civiles, comandos militares (aunque recientemente han optado por independizarse creando intranets), entidades económicas, transacciones financieras y comerciales, corporaciones, etc. Respecto a la cuestión de la fuerza, en el quinto dominio depende directamente de la tecnología emplead, de esta manera, el armamento

[43] *Ídem*

[44] Hall, Charles H. (Mayo 4, 2011). *Operational Art in The Fifth Domain*. Joint Military Operations Department, Naval War College. [En línea]. Disponible en: <http://www.dtic.mil/dtic/tr/fulltext/u2/a546255.pdf>. (Consulta 28/05/16).

[45] Vego citado por Hall, Charles H. (Mayo 4, 2011).

cibernético[46], avanza de forma continúa aumentando su sofisticación y capacidades. [47]

1.3. LAS CIBER-RELACIONES INTERNACIONALES

En la disciplina de las Relaciones Internacionales el papel del ciberespacio ha sido estudiado desde una perspectiva limitada, relacionada únicamente con su función dentro de la economía mundial. En consecuencia, los análisis respecto a la dimensión política son menos numerosos, los más destacados pertenecen a un pequeño número de autores entre ellos Nazli Choucri (2012).

En su obra *Cyberpolitics in International Relations*, Choucri señala que los enfoques tradiciones de las Relaciones Internacionales responden a dinámicas pertenecientes a los siglos XIX y XX, por lo que son principalmente estatocentrícas. Por ende, tratan de explicar fenómenos donde el ámbito territorial y el espacio tangible constituían la principal preocupación de los Estados, reconociendo a éstos como únicos actores en el escenario internacional.

Si bien, desde la perspectiva tradicional se reconoce el influjo del entorno social y natural sobre los individuos, en el caso del espectro cibernético la atención ha sido escasa. Por ello, es preciso que la teoría reconozca el impacto del ciberespacio en las relaciones internacionales.[48]

Actualmente, la adopción de la web en múltiples modalidades de acción por parte de las naciones es reconocida como una fuente de vulnerabilidad, ya que encierra en sí misma una amenaza potencial a la seguridad nacional capaz de perturbar el orden internacional. En otras palabras, el ciberespacio ofrece nuevas oportunidades de competición, contención y conflicto, todos estos elementos fundamentales de la política y del ejercicio de las relaciones internacionales.[49]

---

[46] "Ciberarma" es considerado relativamente un concepto nuevo, por lo que aún carece de un término general. Sin embargo, el concepto más aceptado hasta el momento es el proporcionado por el Manual de Tallin sobre Derecho Internacional Aplicable a la Ciberguerra (2013), el cual refiere a un ciber medio de guerra (entiéndase software) que es capaz, por diseño o intención, de causar daño a personas u objetos.

[47] *Ídem*

[48] Choucri, Nazli. (2012). *Cyberpolitics in international relations*. Cambridge: MIT Press.

[49] *ídem*

En este contexto, el espectro cibernético y su compleja constitución proporcionan elementos que han de tomarse en cuenta en la estructuración de una óptica internacional a la vanguardia, elementos como: temporalidad, materialidad, permeabilidad, participación, atribución y responsabilidad. Los cuales, vienen a revolucionar nociones clásicas de la interacción interestatal, tales como poder y soberanía. [50]

Las transformaciones generadas por la revolución tecnológica también han impulsado, en el ámbito académico, el desarrollo de investigaciones relacionadas con el término "ciberespacio". De este modo, emerge el concepto de *ciber-relaciones internacionales*, propuesto y desarrollado por el Instituto Tecnológico de Massachusetts (MIT, por sus siglas en inglés). El concepto, sirve de base al proyecto "Explorations in Cyber International Relations", el cual busca la creación de un nuevo campo de estudio en las Relaciones Internacionales.[51]

En el marco de este proyecto se han realizado estudios que se concentran en el papel de la web como factor agravante de las tensiones entre Estados, pero también con la capacidad de evitar un conflicto directo. Al mismo tiempo, se reconoce la aparición de nuevas formas de enfrentamiento con base virtual, tales como: ciberataques, ciberterrorismo, organizaciones delictivas que emplean la web para sus operaciones, ciberespionaje, entre otros.

1.3.1. El Neorrealismo y ciberpoder

Desde la perspectiva neorrealista y de acuerdo con Kenneth Waltz, uno de los académicos más destacados en el ámbito de las Relaciones Internacionales, las causas de los conflictos entre los Estados pueden analizarse en tres niveles o "imágenes":

- La naturaleza humana
- Los sistemas económicos y políticos domésticos de los Estados
- El sistema anárquico en el que los Estados coexisten[52].

[50] *ídem*
[51] Para más información, consultar: <http://ecir.mit.edu/>
[52] Griffiths, Martin. (1992). *Fifty Key Thinkers in International Relations.* EE. UU: Routledge.

La tercera imagen posee mayor importancia, ya que describe el entorno de la política internacional. Sin embargo, son importantes también la primera y segunda imágenes, ya que sin ellas no podría existir un conocimiento pleno de los factores que determinan la política mundial. A lo largo de su trabajo Waltz se dedica a examinar la influencia de cada uno de estos niveles dentro de los conflictos internacionales.

En su obra *Theory of International Politics* (1979), Waltz se concentra en la autonomía e influencia que ejerce el componente estructural sobre el sistema internacional. En adición, el autor refiere a un acuerdo mediante el cual los Estados conviven entre sí, dicho acuerdo se mantiene a través del tiempo y limita el grado en el que se puede dar una división de trabajo entre los Estados.

Desde esta perspectiva, mientras la anarquía es constante, la estructura y la distribución de capacidades varía de Estado a Estado. Así, el balance de poder político prevalece, siempre y cuando, se den dos condiciones: 1) un orden anárquico, y 2) la existencia de unidades que deseen sobrevivir.[53]

Reconoce que en un ambiente multipolar las naciones sobreviven gracias al establecimiento de alianzas que les permiten mantener su seguridad. Sin embargo, hay tantos poderes en juego que establecer una línea clara entre aliados y adversarios es imposible. Además, el alto grado de desigualdad entre las superpotencias y los otros Estados hace que las amenazas sean difíciles de reconocer, y por consecuencia los grandes poderes se inclinan a mantener el equilibrio.[54]

Si bien, Waltz reconoce la influencia del entorno en el balance de poder entre Estados, sigue otorgando a éstos el papel como único actor en las relaciones internacionales. Por ello, como refuerzo al trabajo de Waltz, Johan Eriksson y Giampiero Giacomello (2007) analizan efectos de la revolución de la información en la seguridad internacional. Ambos especialistas realizan una revisión a la teoría neorrealista a fin de demostrar que el ámbito digital ha sido descuidado. Eriksson y

[53] *Ídem*
[54] *Ibídem.*

Giacomello, presentan cuatro proposiciones en torno a las nuevas tecnologías y su efecto en la escena mundial. (Ver Figura 1)

FIGURA 1 EFECTOS DE LAS TECNOLOGÍAS EN LAS RELACIONES INTERNACIONALES

Fuente: Elaboración propia con Información de Eriksson, Johan y Giampiero Giacomello (Eds.). (2007).

Eriksson y Giacomello recalcan la aparición de actores no estatales, sin embargo, reconocen que el Estado conserva un papel protagónico debido a su rol supremo como proveedor de seguridad, incluso en el ciberespacio. Bajo esta perspectiva, la aparición de Estados virtuales y redes económicas implica un declive en la violencia interestatal y se experimenta un incremento en la importancia de las corporaciones, en los intereses de las organizaciones, de los movimientos sociales y de las redes transnacionales. No obstante, la evolución de la tecnología implica también un desafío a la seguridad internacional[55]

En cuanto al ciberpoder, los cambios en las tecnologías de la información y en el entorno internacional generaron un impacto en las relaciones de poder entre Estados. Así, la revolución de la información derivó en la difusión de poder. Por lo que, dentro de la interacción interestatal el ciberpoder es incapaz de ser centralizado por un solo actor.[56]

[55] Eriksson, Johan y Giampiero Giacomello (Eds.). (2007). International Relations and Security in the Digital Age. Londres: Routledge.
[56] Nye, Joseph S. Jr. (Mayo, 2010). Cyber Power. Paper, Belfer Center for Science and International Affairs – Harvard University. [En línea]. Disponible en: <htt p://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>.

Al igual que Eriksson y Giacomello, Joseph S. Nye Jr. reconoce que el Estado conserva su protagonismo a la luz de tercera Revolución Industrial, no obstante, debe hacer frente a un escenario con mayor número de participantes y con un nuevo dominio en donde el control absoluto es imposible. Con este análisis Nye presenta al ciberespacio como un nuevo dominio de poder: el poder de afectar el comportamiento de otros actores.[57]

Empero, el ciberpoder no eclipsará la importancia de la dimensión geográfica ni abolirá la soberanía estatal, sino que coexistirá con estos, complicando el ejercicio del poder en dichas dimensiones. Es decir, el espacio cibernético podrá utilizarse para producir resultados deseados dentro del ciberespacio y podrán emplearse también instrumentos cibernéticos para producir resultados ventajosos en otros dominios.[58]

Por esta razón, los cambios en la naturaleza del poder deben estar acompañados por una evolución teórica, pues tanto la historia como la concepción moderna de las Relaciones Internacionales y del poder están profundamente relacionados a los intereses y capacidades del Estado en un entorno que ha quedado en el pasado.[59]

1.3.2. El desarrollo de la cyberpolitik

En 1998 David Rothkopf empleó por primera vez el término *Cyberpolitik*. En su artículo “The Changing Nature of Power in the Information Age” establece que la capacidad de los Estados para lograr sus objetivos se ha basado tradicionalmente en tres pilares:

- El poder económico
- El poder militar
- El poder político

[57] Nye, Jr. Joseph S. (Mayo, 2010). “Cyber Power”. Belfer Center for Science and International Affairs. [En línea]. Disponible en: <http://www.belfercenter.org/sites/default/files/files/publication/cyber-power.pdf>
[58] *Ídem.*
[59] *Ibídem*

Dentro del último, surge la *cyberpolitik* que se basa en la *realpolitik* de Bismarck[60] y refiere a una nueva distribución de poder entre Estados y nuevos actores de la escena internacional. Desde esta perspectiva el poder evoluciona adoptando nuevas formas y características.[61]

Rothkopf sostiene que con la revolución de las Tecnologías de la Información y Comunicación (TIC) el poder es infinitamente redistribuido y redefinido. Esta naturaleza cambiante actúa como fuerza desestabilizadora para aquellos que son incapaces de adaptarse al cambio, y al mismo tiempo favorece a quienes poseen la flexibilidad para adecuarse al nuevo medio. En la base de esta transformación, está la evolución de la información la cual conduce, posibilita e influencia cada uno de estos cambios.[62]

De esta forma, los principales rasgos de la *cyberpolitik* en las relaciones internacionales son: 1) los actores no son sólo Estados, y 2) la fuerza bruta puede ser contrarrestada o reforzada por el poder de la información. Así, mientras que el poderoso prevalece, las fuentes, instrumentos y medidas de la fuerza están cambiando drásticamente. La revolución informática, por lo tanto, rompe jerarquías y crea nuevas estructuras de poder. El Estado por su parte, cede parte de su autoridad estatal a los mercados, trasnacionales y actores no estatales. Sin embargo, en este escenario se producen también fuerzas políticas que solicitan el refuerzo de la autoridad estatal.[63]

Por lo anterior, es posible afirmar que la innovación tecnológica crea cambios políticos y militares importantes que trascienden al plano internacional. Asimismo, representa una transformación en la capacidad de influencia, la conducción de conflictos y la percepción de amenazas a nivel global.

[60] El término refiere a la idea de que las relaciones entre los Estados están determinadas por la fuerza bruta, y que el más poderoso prevalecerá. Fuente: Kissinger (1996).
[61] Rothkopf, David. *Óp. Cit.*
[62] *Ídem.*
[63] *Ídem.*

1.4. SOBRE LA GUERRA MODERNA, MEDIO ORIENTE Y HUNTINGTON EN LA ERA DE LA INFORMACIÓN

Entre los análisis orientados al estudio de la guerra moderna se encuentra el trabajo de Rupert Smith. En su obra *The Utility of Force: The art of war in the modern world* (2003) establece que las transformaciones experimentadas en el orden mundial hacia finales del siglo XX y principios del siglo XXI representan un cambio de paradigma en la naturaleza de los conflictos bélicos. Dos importantes, argumentos sustentan su proposición: 1) el fin de la gran confrontación, derivado de la ruptura del orden bipolar, y 2) la transformación de las fuerzas armadas, que actualmente tienden a reducir su número.[64]

En adición, el ataque al Word Trade Center del 11 de septiembre de 2001 significó también una importante modificación en los paradigmas de seguridad, ya que el "terrorismo" se percibió como la principal amenaza mundial. Sin embargo, al hablar de "terrorismo", plantea Smith, no se hace referencia a un enemigo formulado sino a un concepto de amenaza. Así, al no combatir un enemigo identificado resulta difícil formular una estrategia y sin una estrategia las decisiones entorno al equipamiento y las armas terminan siendo inadecuadas.

Otras características de la guerra moderna son:

- Los fines por los cuales se combate están cambiando de objetivos delimitados que deciden un objetivo político a aquellos que establecen condiciones en donde el resultado será definido
- Se pelea en medio de personas y no en un campo de batalla
- Los conflictos tienden a ser atemporales y a menudo sin fin
- Se combate para preservar la fuerza y no para alcanzar un objetivo
- En cada ocasión de encuentran mayores usos a las armas y a las organizaciones creadas en la era industrial
- Los contrincantes son mayormente actores no estatales.[65]

[64] Smith, Rupert. (2005). *The Utility of Force: The art of war in the modern world.* EE. UU: Vintage.
[65] *ídem*

En adición, Rupert resalta el papel de los medios de comunicación, los cuales son empleados para alcanzar objetivos políticos. De esta forma, mediante vías como la televisión e Internet, se cuenta una versión particular de los enfrentamientos con el fin de alinear a la opinión pública, así se une el deseo del Estado (quien emprende esas batallas), el pueblo (quien recibe el mensaje) y las fuerzas armadas (quienes libran los combates) en la trinidad planteada por Clausewitz.

Bajo esta misma línea Martin Van Creveld, examina dos casos transcendentes: Hafez Al Assad y la masacre en Hama en 1982 y la invasión a Iraq de 2003, para exponer las características de los enfrentamientos modernos. En su obra *The Changing Face of War* (2005) sostiene que el dominio de la información y de los medios de comunicación es un elemento crucial para conseguir los fines políticos, también se enfoca en el rol de las fuerzas no estatales y el empleo armamento altamente tecnológico, desarrollado en el marco de la denominada Revolución de los Asuntos Militares.[66]

En el caso particular de Medio Oriente, de acuerdo con Anthony Cordesman, durante el último cuarto de siglo la región ha transitado de enfrentamientos relativamente cortos a esfuerzos radicalmente diferentes del uso de la fuerza con el fin de disuadir o influenciar conflictos en donde se involucran actores no estatales, fuerzas extra regionales, alianzas inestables, terrorismo e insurgencia, elementos que se mueven a través de las fronteras nacionales. En últimos años, tales características han pasado de ser una excepción en la guerra en Medio Oriente a convertirse en una regla.[67]

Por ello, Cordesman se inclina a analizar los enfrentamientos modernos en la región más allá del empleo del poder militar. Desde esta aproximación es importante también examinar la forma en la que los conflictos terminan, continúan y mutan

[66] Van Creveld, Martin. (2005). *The changing face of war: combat from the Marne to Iraq.* EE. UU: Ballantine.
[67] Cordesman, Anthony. (Enero 14, 2017). The Changing Nature of War in the Middle East and North Africa. *Harvard International Review*. [En línea]. Disponible en: <http://hir.harvard.edu/article/?a=14493>.

desde una perspectiva estratégica más amplia y sin perder de vista su impacto político.[68]

En la actualidad, Medio Oriente se encuentra bajo cambios radicales debido a un importante crecimiento poblacional, una híper urbanización, sistemas de desarrollo económico insuficientes además de complicaciones políticas experimentadas por diversos sistemas de gobierno en la región. Los conflictos en Medio Oriente durante el último tercio de siglo se han caracterizado por no representar el fin de una guerra sino el preludio de enfrentamientos futuros.[69]

En este sentido, un punto crucial en el cambio en la naturaleza de la guerra en Medio Oriente fue la Segunda Guerra del Golfo Pérsico (1990-1991), pues luego que la coalición liderada por Estados Unidos consiguiera la retirada de Iraq de Kuwait, se experimentó una transformación en la forma de librar las batallas. En primer lugar, el repliegue de las fuerzas iraquíes y la derrota de Hussein generaron consecuencias como el enfrentamiento por el liderazgo regional, enmarcados en luchas ideológicas dentro y fuera de Iraq. En segundo lugar, los conflictos se caracterizaron por buscar (más que la victoria) la contención, en particular la de Saddam, lo cual derivó en divisiones internas y que Hussein optara por emplear la religión como una herramienta a su favor. En adelante, las operaciones militares se caracterizaron por ser rápidas, sin logros estratégicos duraderos, con consecuencias a largo plazo y sin ningún plan de estabilización. Surgieron, entonces, alianzas estratégicas con el fin de desarrollar poderío militar y otras que incluían a actores no estatales como grupos terroristas, en búsqueda de incrementar la influencia regional. Paralelamente, se dio también la evolución en armamento que obligó a otros Estados a perfeccionar las armas con el objetivo de responder a las capacidades de sus vecinos.[70]

Así, sucesos como los conflictos árabe-israelí, las rivalidades por el liderazgo regional entre Irán y Arabia Saudita; los enfrentamientos entre gobiernos y actores

[68] *Ídem*
[69] *Ídem*
[70] *ídem*

no estatales en Sudán, Somalia y Yemen, y la propia inestabilidad interna en diversos Estados moldearon la naturaleza de la guerra en Medio Oriente, conduciéndola hacia una cada vez más compleja mezcla de fuerzas, enmarcadas en prolongados conflictos de baja intensidad.[71]

En la actualidad cuatro importantes eventos han moldeado el carácter de las batallas regionales y sin duda determinarán las características de los enfrentamientos futuros, estos son:

1.- El incremento de ataques por parte de grupos extremistas islámicos que comenzaron con el atentado al World Trade Center en Estados Unidos (2001) y en Arabia Saudita (2003) y que luego se propagaron por Medio Oriente a países como Iraq, Siria y Yemen, resultando en la creación de movimientos extremistas más poderosos como el Estado Islámico.

2.- La retirada de las tropas militares estadounidenses de Iraq, que dejó al país en medio de la inestabilidad política, donde el Primer Ministro Nouri al-Maliki buscando el dominio del poder político se acercó al ala chií a expensas de los intereses de la población sunní y kurda, lo que incrementó la violencia interna a partir de 2010.

3.- La escalación de la tensión y la competición entre Irán y Arabia Saudita y otros países árabes, que involucra también la presencia militar de países extraregionales, especialmente a partir del inicio de la Guerra Civil Siria (en 2011)

4.- La serie de convulsiones políticas y revoluciones que comenzaron en Túnez en 2011 y que se propagaron por otros países.[72]

Sin embargo, las fricciones regionales y los efectos de la intervención de actores extraregionales en la zona han sido recurrentemente analizadas desde el ámbito académico bajo la luz del denominado “choque de civilizaciones”.

[71] *ídem*
[72] *Ídem*

El término presentado por primera vez por Samuel Huntington en un artículo de la revista *Foreign Affairs* en 1993, hace referencia a un cambio en la política mundial en la que Occidente va perdiendo influencia relativa mientras que las civilizaciones asiáticas incrementan la suya en la esfera económica, militar y política. Por su parte, el islam experimenta una explosión demográfica con consecuencias para los países musulmanes y sus vecinos.[73]

De esta forma, surge un orden mundial basado en civilizaciones, en donde los países con afinidades cooperan entre sí y se agrupan en torno a Estados dirigentes. Al tiempo en que las afinidades universalistas de Occidente le conducen al conflicto con el islam y China. Por su parte, la guerra se origina por fracturas entre los musulmanes y no musulmanes, lo que genera solidaridad entre países afines. Ante tales circunstancias, establece Huntington, es necesario que Occidente se una para reafirmar su identidad, y renovarla y preservarla frente a los ataques procedentes de sociedades no occidentales.[74]

Sin embargo, los eventos que han moldeado la guerra moderna en Medio Oriente escapan de la explicación civilizacionista de Huntington, debido a: 1) ni la civilización asiática ni la musulmana son totalmente homogéneas por lo que la posibilidad de alinear sus intereses con el fin actuar en contra occidente es improbable, 2) en el caso de Medio Oriente, las dinámicas regionales involucran algo más que sólo el islam, envuelve diversas dinámicas en las que participan múltiples etnias y minorías religiosas como las comunidades kurdas, drusas, cristianas, zoroastrianas, entre otras, quienes juegan un papel determinante en la zona, además de las fricciones originadas en el plano político derivadas del interés nacional de cada Estado en la región, 3) el enfrentamiento no sólo se dirige a occidente, como Anthony Cordesman planteó, las fricciones también surgen y se mantiene con el fin de obtener la hegemonía regional, y 4) la división de la política mundial por civilizaciones desatiende el peso de actores no estatales como las corporaciones, diásporas, los

[73] Huntington, Samuel. (2005). *El Choque de Civilizaciones y la Reconfiguracion del Orden Mundial.* Barcelona: Paidos Iberica.
[74] *Ídem*

medios de comunicación y organizaciones internacionales involucradas también en los conflictos regionales.

En el plano político la tesis del "choque de civilizaciones" ha sido empleada de forma deliberada, inapropiada e incluso contradictoria, especialmente desde aproximaciones neoconservadoras que enarbolan la lucha contra el terrorismo y la islamofobia. Un claro ejemplo, es el uso del concepto por parte del, entonces presidente de Estados Unidos, George W. Bush, con el fin de distinguir las "naciones civilizadas" de los denominados "Estados canallas". Más adelante, el 11 de septiembre de 2007 durante el Discurso presidencial a la nación refirió: "esta lucha ha sido nombrada 'choque de civilizaciones'. En verdad, es una lucha por la civilización".[75]

La imagen de la política mundial presentada por Huntington otorga el papel de guardián del orden a Occidente por lo que, retomando a Samir Amin, es universalista en el sentido en que impone a todos, la imitación de un modelo como única solución a los desafíos de nuestro tiempo. Sin embargo, es importante recalcar también que los instrumentos teóricos para analizar la realidad social son imperfectos y, tal como Samir Amin expone, se componen de paradigmas que eventualmente funcionan, pero de ninguna manera representan una fórmula infalible e imperecedera.[76]

En suma, plantea Samir, la división de culturas es una labor compleja, pues es imposible delimitar las fronteras espacio-temporales de una cultura en particular. En el caso de Medio Oriente, es difícil hablar de una cultura del mundo árabe o árabe islámica, por lo que se debe renunciar a concepciones totalizadoras y observar las especificidades de los subconjuntos, pues de lo contrario se cae mecanismos de análisis que derivan en la construcción ideológica de oriente representadas en el "orientalismo".[77]

---

[75] Eriksson, Johan. "The 'Clash of Civilizations' and Its Unexpected Liberalism". En J. Paul Barker (Ed). (Octubre, 2013). *The Clash of Civilizations: Twenty Years On*. Bristol: e-International Relations, p. 29.
[76] Amir, Samir. (1989). *El Eurocentrismo: una crítica a una ideología*. México: Siglo XXI
[77] *Ídem.*

En el plano teórico de las relaciones internacionales “el choque” tampoco responde a la compleja construcción de las alianzas internacionales, pues de acuerdo con Huntington es la afinidad cultural la que crea la línea entre aliados y enemigos, ignorando el peso del interés económico en la creación de tales alianzas. En adición, al tomar como unidad de análisis a las civilizaciones, se plantea la dificultad de definir, ¿qué es una civilización?, pues sí se toma como referencia la delimitación geográfica, propuesta por Huntington, en el caso del islam el molde resulta inaplicable.[78]

Ante tal panorama y el arribo de era informatizada el orden político internacional es reconfigurado. Paralelamente, se transforman también las dinámicas extra e intra regionales. Repensar el “choque” en el marco de un entorno globalizado, conlleva a examinar la manifestación de dichas culturas en el espectro digital, la forma en la que las civilizaciones adoptan y adaptan las tecnologías a sus necesidades, valores y visión del mundo tanto en el plano cultural, social, político, económico y militar.[79]

Así, Medio Oriente experimenta cambios derivados de eventos históricos cuyos efectos transcienden el tiempo, fricciones propiciadas por las aspiraciones de domino regional y el surgimiento de actores no estatales que se fortalecen ante la debilidad estatal.

Se trata también del surgimiento de nuevas capacidades y funcionalidades vinculadas con la tecnología que se incorporan a las dinámicas regionales existentes, generando un impacto en la percepción de poder, siendo apropiadas e implementadas por actores estatales y no estatales, y conduciendo una transformación en la naturaleza de los conflictos interestatales. Dicha evolución obedece a un proceso que inició durante la Guerra Fría y que en el plano militar dio origen al concepto de Revolución de los Asuntos Militares.

---

[78] Tahir Ashraf, Mian Muhammad. (2012). “The Clash of Civilizations? A Critique”. *Pakistan Journal of Social Sciences (PJSS)*. Vol. 32, No. 2, pp.521-527.

[79] Wheeler, Deborah. (2002). “Islam, Community, and the Internet: New possibilities in the digital age”. Interface: The Journal of Education, Community and Values. [En línea]. Disponible en: <http://commons.pacificu.edu/cgi/viewcontent.cgi?article=1010&context=inter02>.

CAPÍTULO 2. LA REVOLUCIÓN TECNOLÓGICO INFORMACIONAL DE LOS ASUNTOS MILITARES

La guerra como elemento presente en la naturaleza del hombre ha sido examinada desde tiempos remotos. Más recientemente, autores como Alvin y Heidi Toffler emplean un modelo en donde la práctica económica no sólo se relaciona sino condiciona de forma determinante el carácter de la guerra, es precisamente la aparición de su obra *Las guerras del futuro* (1994) lo que dio origen a la publicación de numerosos trabajos orientados a descifrar el grado en el que la tecnología afecta o no las prácticas belicistas. El cuestionamiento lanzado en su obra acerca de si la tecnología determina la estrategia o viceversa ha dado paso a diversos trabajos que se sitúan tanto favor como en contra del influjo de las aplicaciones tecnológicas en la guerra.

Así, en el marco de las corrientes sucesivas al pensamiento de Toffler, aparecen especialistas como Brandon Valeriano y Ryan C. Maness para quienes los avances científicos asisten a las prácticas ofensivas y defensivas, pero su poder no es del todo determinante.[80]

Desde esta óptica el poder de las estrategias y del armamento cibernético cuenta con un grado considerable de efectividad cuando no buscan alterar el comportamiento de otros actores. En su obra "Cybervictory: The efficacy of Cyber Coerción" reconocen que otorgar un papel decisivo en el combate al uso del elemento cibernético es apresurado puesto que aún se conoce muy poco sobre la ciberestrategia y el ciberpoder. Para Valeriano y Maness las estrategias de denegación resultan elementos coercitivos inefectivos y para demostrarlo recurren al análisis de ciberincidentes acaecidos a nivel macro entre el año 2000 y 2014 utilizando el Dyadic Cyber Incident and Dispute Dataset[81].

Ante tales posicionamientos, el objetivo de este capítulo es recurrir a ambas perspectivas a fin de estructurar una óptica integral en donde sea posible reconocer

[80] Valeriano, Brandon y Ryan C. Maness. (2016). "Cybervictory: The efficacy of Cyber Coerción". Artículo Inédito.

[81] Una especie de banco de datos creado por Brando Valeriano y Ryan C. Maness que documenta las dinámicas de ciberconflicto entre rivales antagonistas del año 2001 al 2011. La plataforma electrónica puede ser consultada en la siguiente dirección: <http://drryanmaness.wixsite.com/irprof/cyber-conflict-dataset>

los alcances del uso del ciberdominio y la tecnología en las estrategias militares sin exacerbar sus capacidades. Para ello, y como vínculo entre la innovación científica y el ámbito militar, se utiliza el concepto de Revolución Tecnológico Informacional de los Asuntos Militares, del cual, dada su importancia en esta investigación se realiza un breve análisis sobre su surgimiento.

El término Revolución de los Asuntos Militares (RMA, por sus siglas en inglés), fue empleado por primera vez de forma oficial en el "Informe Anual del Secretario de Defensa al Congreso de Estados Unidos" en 1998[82]. Empero, desde la década de los 80 había sido ampliamente estudiado por Andrew W. Marshall director de la Oficina de la Evaluación en Red del Pentágono.[83]

En ese entonces Marshall lo describió como:

> […] *un cambio en la naturaleza de la guerra provocado por la aplicación innovadora de nuevas tecnologías que, combinadas con cambios dramáticos en la doctrina militar y en los conceptos de funcionamiento y organización, altera fundamentalmente el carácter y la conducta de las operaciones militares*.[84]

El concepto tiene sus orígenes en el trabajo del coronel Nikolai Ogarkov quién le otorgó el nombre de Revolución Tecnológica Militar (RTM). Antes que Marshall, Ogarkov se dedicó a examinar el pensamiento militar soviético en los años 70, su análisis le llevó a vislumbrar la superioridad militar que poseía Estados Unidos y la ventaja que le otorgaban el empleo de ataques automatizados, en particular el uso de municiones de precisión, sensores de banda ancha y sistemas computarizados de comando y control.[85]

Hacia término del siglo XXI, Andrew Marshall retomó los estudios de Ogarkov y sugirió que la evolución en el armamento y su empleo estaba suscitando, también,

---

[82] Bardají, Rafael L. e Ignacio Cosidó. (2000). "La RMA y España. Algunas reflexiones sobre el camino a seguir". *Grupo de Estudios Estratégicos* (GEES). Análisis 56, mayo-junio 2000. [En línea]. Disponible en: <http://www.gees.org/articu los/la-rma-y-espana-algunas-reflexiones-sobre-el-camino-a-seguir>.)

[83] Jordán, Javier. (2014). "Innovación y Revolución en los Asuntos Militares: una perspectiva no convencional". *Grupo de Estudios en Seguridad Nacional*. [En línea]. Disponible en: <www.seguridadinternacional.es/?q=es/analisis &page=4>.

[84] McKitrick, Jeffrey et al. (1998). *The Battlefield of the Future - 21st Century Warfare Issues*. Air University, No. 3 p.65. [En línea]. Disponible en: <http://www.au.af.mil/au/cpc/books/assets/battlefield_future.pdf>.

[85] Watts, Barry D. (2011). *The Maturing the Revolution in Military Affairs*. Estados Unidos: Center for strategic and Budgetary Assessments, pp-1-2.

la evolución de la conducta de la guerra. En 1993 planteó que una posible forma en la que la guerra podría cambiar es en la inclinación hacia los ataques de larga precisión, otro cambio importante de acuerdo con Marshall es la aparición de la guerra informática.[86]

De forma general el concepto de RMA ha sido examinado y cuestionado a través del tiempo. Sus detractores sostienen que un cambio revolucionario en el ámbito militar no es sencillo y que la evolución de las instituciones militares no posee un ritmo continuo. Es decir, está acompañado de procesos de rápido avance y de estancamientos.[87]

No obstante, el concepto sigue siendo objeto de numerosos estudios. En adición, con el arribo de la era digital se ha desarrollado el concepto de Revolución Tecnológico-Informacional de los Asuntos Militares (IT-RMA, por sus siglas en inglés), especialmente orientado a analizar el influjo de la revolución de las comunicaciones sobre la práctica de la guerra. Es en esta variación moderna de la RMA en donde se han desarrollado análisis que evalúan el impacto de la innovación de las telecomunicaciones dentro de los enfrentamientos bélicos modernos, así, por ejemplo, para especialistas como Dima Adamsky y Kjell Inge Bjerga la existencia de una IT RMA no significa necesariamente una mejora operacional en la función militar. Sin embargo, reconocen que la crítica a dicho concepto sirve como fuerza impulsora para estructuración de una teoría militar moderna.[88]

En el caso concreto de las comunicaciones el surgimiento y expansión de Internet genera cambios de índole económico, cultural y social. A la par surgen nuevos tipos de enfrentamiento como las guerras en red[89] y así la estructura misma de las

[86] Watts, Barry D. *Op. Cit.*, p. 2

[87] Calvo Albero, José Luis. (2001). *La Revolución de los Asuntos Militares*. Escuela de Guerra del Ejército en Tierra. [En línea]. Disponible en: <http://csis.org/publication/real-revolution-military-affairs>.

[88] Adamsky, Dima y Kjell Inge Bjerga. (2010). "Introduction to the Information-Technology Revolution in Military Affairs". *The Journal of Strategic Studies*, Vol. 33, No. 4, pp. 463–468. [En línea]. Disponible en: <http://dx.doi.org/1 0.1080/01402390.2010.489700>.

[89] De acuerdo con John Arquilla y David Ronfeldt en su obra *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político* (2003) en las batallas modernas aparecen actores como grupos terroristas, anarquistas y grupos activistas cuya forma de organización es en red, ya que operan en unidades pequeñas, lo cual los dota de una gran rapidez. Por lo tanto, el impacto de Internet en la actualidad se refleja

amenazas transnacionales se transforma. Por ello, los organismos encargados de la seguridad requieren de nuevas estructuras y dinámicas operacionales para hacer frente a la nueva realidad.

La red de redes se ha convertido en el principal vehículo de comunicación global capaz trasladar millones de datos en cuestión de segundos. En el campo militar la abundancia de información requiere no sólo de personal capaz de administrarla sino de convertirla en conocimiento efectivo, por ello funciones como C4IRS[90]sufren cambios significativos. De esta forma, se experimenta no sólo una transformación en la conducta de la guerra sino de sus propios objetivos.[91]

En el campo militar, expertos como el Mayor Norman C. Davis, refieren a una transformación en las estructuras tradicionales de la jerarquía militar, así como a una difuminación y redistribución del poder que eventualmente favorece a aquellos que alguna vez fueron considerados actores menos importantes. Desde esta perspectiva, la transformación tecnológica de la guerra requiere de la introducción y la maduración de las nuevas tecnologías; su integración a los nuevos sistemas militares; la adopción de conceptos militares apropiados, y finalmente la adaptación organizacional. Por lo tanto, la innovación científica no es por sí misma una fuerza suficiente para dar paso a un cambio doctrinal, se necesita también de adaptabilidad organizacional.[92]

2.1. LA INCORPORACIÓN DEL CIBERESPACIO EN EL ÁMBITO MILITAR

Paralelamente a la expansión del Internet y de la propagación del uso de objetos inteligentes alrededor del mundo la vulnerabilidad de diversas funciones como las económicas, financieras, educativas, estatales y militares ha crecido de forma exponencial. La dependencia que respecto a Internet poseen procesos relacionados

---

en la aparición de una sociedad global estructurada de esta forma, lo cual supone también un fuerte impacto transformador en el orden social, político y económico tradicional.

[90] En la nomenclatura militar se conoce como Mando, Control, Comunicaciones, Ordenadores, Inteligencia, Reconocimiento y Búsqueda. Fuente: Molina Rabadán (2005)

[91] Mayor Davis, Norman C. "An Information-Based Revolution in Military Affairs". En Arquilla, John y David Ronfeldt (Edits.). (1997). *In Athena's camp. Preparing for conflict in the information age*. EE.UU : RAND Corporation, p.79

[92] *Íbidem*

con el funcionamiento del Estado (como los administrativos, de transmisión y resguardo de datos, así como los operacionales) engloba un riesgo creciente para la seguridad nacional e internacional.

En los últimos años se ha publicado abundante literatura sobre la guerra cibernética[93] la mayoría tiende a polarizar opiniones sobre la existencia o no de un ciberconflicto, para especialistas como Welton Chang y Sarah Granger, tales posicionamientos sólo llevan a ofuscar los peligros verdaderos.[94]

Por lo anterior, no es una sorpresa que ante la notable convergencia de funciones cotidianas con el entorno cibernético las operaciones militares han incorporado también el uso de Internet. Por esta razón, el presente apartado está dedicado a analizar la incorporación de ciberespacio en el ámbito militar. Aunque vale la pena recordar que la red de redes nació justamente en ese entorno, de forma que: Internet surge en el campo militar, experimenta una expansión por el ámbito civil, económico y político en donde se convierte en la principal vía de comunicación global y se reinserta nuevamente en el campo militar. Esta adecuación de la función militar conlleva a la transformación de las jerarquías tradicionales configurando lo que el Mayor Davis Norman ha denominado "redes amorfas".[95]

2.1.1. Tácticas defensivas y ofensivas

Las operaciones militares en el espacio cibernético son fuertemente influenciadas por las características del medio, por lo que la posibilidad de tener un control absoluto sobre las operaciones depende de forma directa de la naturaleza de entorno digital.

[93] Entre los más destacados figuran: Richard A. Clarke y Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It*; Martin C. Libicki, Cyberdeterrence and Cyberwar; Brandon Valeriano y Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*; Richard Stiennon, Surviving Cyberwar, entre otros.

[94] Chang, Welton y Sarah Granger. (2012). "La Guerra en el Ámbito Cibernético". *Air & Space Power Journal*, vol. 4, no. 3, p.86. [En línea]. Disponible en: <http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/20123/2012_ 3_10 _chang_s.pdf>.

[95] Mayor Davis, Norman C. *Óp. Cit.*, p. 83.

Una proposición general al respecto es que la ventaja decisiva se sitúa del lado del atacante, pues el costo de protegerse contra un ataque cibernético es diez veces mayor que el gasto que conlleva diseñar un software malicioso.[96]

Por esta razón, las estrategias defensivas en el ciberespacio difieren de forma significativa de los otros dominios. De acuerdo con David T. Fahrenkrug (2012), una estrategia de defensa integral debe constar de tres características:

1. Intentar evitar el ataque dispersando activamente las redes y la información empleando IP[97] y saltos de frecuencia; fraccionando datos; despejando nubes, y utilizando la esteganografía[98].
2. Incluye el reforzamiento de la infraestructura y la información utilizando métodos de encriptación y de blindaje de los componentes electrónicos.
3. Es capaz de detectar y responder a las intrusiones y ataques.[99]

Sin embargo, las estrategias de defensa cibernética modernas aún carecen de las capacidades suficientes que les permitan responder de manera adecuada a un ataque. Específicamente, según David T. Fahrenkrug, carecen de conceptos organizadores que puedan integrar las capacidades actuales en una estrategia flexible y adaptable.[100]

En su análisis Fahrenkrug (2012), señala la diferencia de aplicar técnicas de defensa en el espacio cibernético y en el medio tangible, pues en estas últimas se protege determinada extensión aérea, marítima o espacial, la cual es claramente

[96] Fahrenkrug, David T. (2012). *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*. NATO CCD COE Publications, Tallinn, p. 1. [En línea]. Disponible en: <https://ccdcoe.org/cycon/2012/proceedings/fahrenkrug.pdf>.

[97] Protocolo de Internet o IP (por sus siglas en inglés), se trata de un software diseñado para manejar la información en paquetes. En la arquitectura de Internet es quien hace posible la comunicación entre distintos equipos. Fuente: Estrada (2004).

[98] Del griego *steganos* (oculto) y *graphos* (escritura), la esteganografía se puede definir como la ocultación de información en un canal encubierto con el propósito de prevenir la detección de un mensaje oculto. Fuente: Observatorio de la Seguridad de la Información. (*s.f.*)

[99] Fahrenkrug, David T. (2012). *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*. NATO CCD COE Publications, Tallinn, p1. [En línea]. Disponible en: <https://ccdcoe.org/cycon/2012/proceedings/fahr enkrug.pdf>.

[100] Fahrenkrug, David T. *Óp. Cit.*, p. 198.

distinguible, mientras que en el espectro digital lo que se protegen son contenidos y funciones en un espacio indefinido.[101]

Desde esta perspectiva una operación eficaz de defensa que sea ordenada, planificada y correctamente ejecutada tiene la capacidad de aislar y rescatar a la red atacada. Mientras que, por su parte, la información que no ha sido comprometida se desvía hacia nueva infraestructura. Por lo tanto, la defensa al igual que el ataque debe de caracterizarse por su agilidad.[102]

Más ampliamente el concepto de defensa integral debe considerar:

- Dispersión. – que es la variabilidad de funciones de las redes. Mientras unas son operacionales otras se encargan del resguardo de información. De esta forma, encontrar un objetivo para atacar se hace difícil al adversario. Se trata de segmentar tanto las funciones como el almacenamiento de datos, construyendo una especie de camuflaje electrónico.
- Reforzamiento. – mientras que la dispersión se encarga de evitar un ataque el reforzamiento incrementa la probabilidad de sobrevivir a uno. Consiste en identificar la información sensible y dotarla de niveles adecuados de cifrado.
- Detección. – se objetivo es conseguir mayor consciencia sobre lo que ocurre en la batalla. Tanto en el espacio virtual como en el tangible el entorno, la amenaza y el tiempo determinan el lapso de reacción requerido para contrarrestar el ataque.[103]

En síntesis, el objetivo de las prácticas de defensa en el ciberespacio es asegurar la privacidad e integridad de información almacenada y el debido funcionamiento de las redes informáticas, para ello las estructuras militares se sirven de específicas y altamente especializadas operaciones que recaen en manos tanto de las unidades correspondientes como de los expertos en el ámbito informático.

Del lado de las tácticas defensivas, tres características del ciberespacio le otorgan una fuerte desventaja:

---

[101] Fahrenkrug, David T. *Óp. Cit.,* p. 199.
[102] *Ídem*
[103] Fahrenkrug, David T. *Óp. Cit.,* p. 200-203

- El lugar central de las vulnerabilidades
- Los diferentes ritmos de evolución en las tecnologías de defensa y ataque
- La dificultad de la atribución, pues en el ámbito cibernético es prácticamente imposible conocer con toda certeza el origen de un ataque.[104]

El ciberespacio como activo militar produce un impacto en las estrategias de seguridad de las naciones[105]. Así, de acuerdo con Andrea Locatell (2013), a través de un análisis sobre el Balance Ofensiva/Defensiva es posible observar que cuando los Estados identifican en el agresor una ventaja, responderán a través de ataques preventivos,[106] por lo que en el espectro cibernético la supremacía que un actor posee sobre otro suscitará la ejecución de ataques anticipados. Sin embargo, como se mencionó la cuestión de la atribución sigue siendo un problema importante en el mapeo de ciber -capacidades.

El empleo del potencial ofensivo en el ciberespacio es una cuestión delicada, pues cuando un Estado desea ejecutar operaciones de esta naturaleza se encuentra con dificultades como la falta de una legislación internacional en la materia, ya que muchas de las operaciones como la irrupción, substracción e incluso inhabilitación de redes informáticas no se encuentran jurídicamente reguladas, además en ocasiones el ejecutarlas se contrapone a los derechos de la población.[107]

No obstante, es preciso examinar en qué consisten las operaciones ofensivas, ya que son de naturaleza variada y se sirven de software malicioso para su ejecución, principalmente consisten en:

- Denegación de servicios
- Manipulación de información

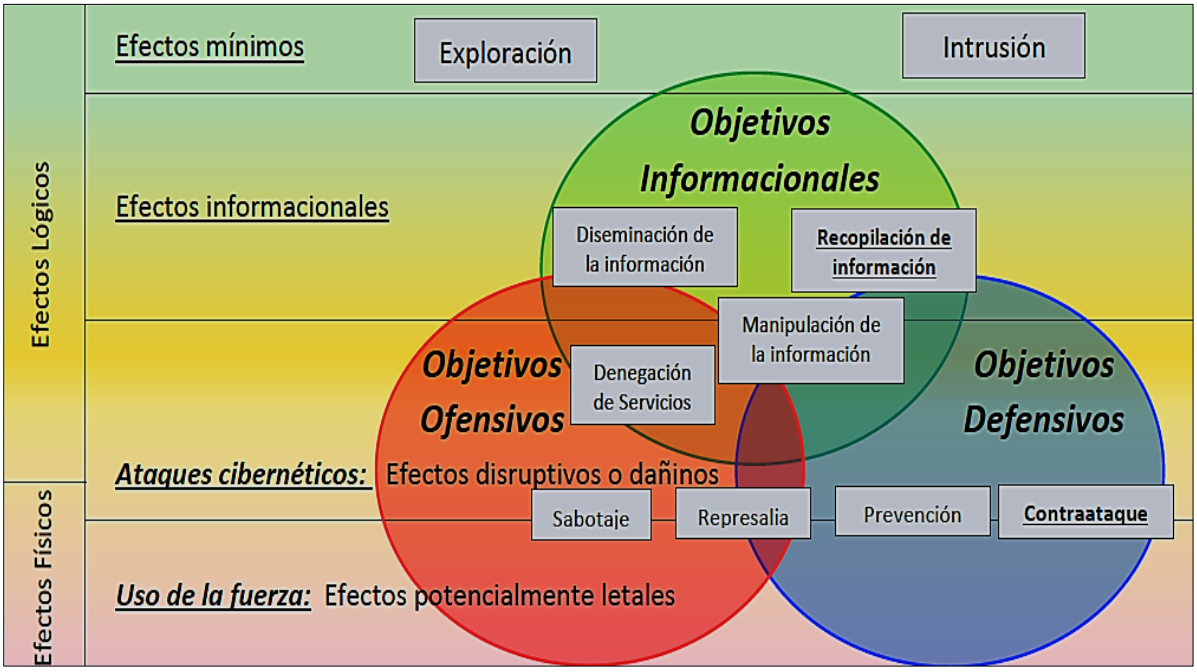
---

[104] Locatell, Andrea. (Octubre, 2013). The Offense/Defense Balance in Cyberspace. *Analysis*. No. 203, p.1. [En línea]. Disponible en: <http://www.ispionline.it/sites/default/files/pubblicazioni/analysis_203_2013.pdf>.
[105] *Ibídem*, p. 2.
[106] Locatell, Andrea, *Óp. Cit.* p. 2.
[107] Leed, Maren. (Septiembre, 2013). Offensive Cyber Capabilities at the Operational Level: The Way Ahead. Center for Strategic and International Studies (CSIS), pp.2-3. [En línea]. Disponible en: <http://csis prod.s3.amazonaws.com/s3fs-public/legacy_files/files/p ublication/130916_Leed_OffensiveCyberCapabilities_Web.pdf>.

- Diseminación de información
- Sustracción de datos
- Monitoreo de comunicaciones

De forma general, estas operaciones son clasificadas dentro de dos dimensiones: 1) las que posee efectos lógicos y 2) las que poseen efectos físicos.[108] (véase figura 2).

FIGURA 2 ACCIONES CIBERNÉTICAS EXTERNAS



Fuente: Belk, Robert y Matthew Noyes. (Marzo 20, 2012). On the Use of Offensive Cyber Capabilities, p. 6.

Las operaciones ofensivas poseen efectos lógicos y físicos, y son catalogadas como ataques cibernéticos que representan el uso de la fuerza por parte de un Estado u otro actor internacional.[109]

En resumen, la tácticas ofensivas y defensivas en el ciberespacio difieren de forma importante de los otros dominios, por ello las operaciones militares ejecutadas

[108] Belk, Robert y Matthew Noyes. (Marzo 20, 2012). On the Use of Offensive Cyber Capabilities. Creative Commons, p. 6. [En línea]. Disponible en: <http://ecir.mit.edu/ima ges/stories/cybersecurity-pae-belk-noyes%202012.pdf>.
[109] *Ibídem.*

en este medio deben de desarrollar una estrategia propia, tomando en cuenta la específica complejidad del medio e incorporarse dentro de las rígidas estructuras militares tradicionales de las cuales demandan flexibilidad y adaptación.

2.1.2. Actores estatales y no estatales

El poder de acción militar en el ciberespacio también depende de la capacidad intelectual de los expertos en informática y de la capacidad económica de los Estados para invertir los recursos necesarios en el desarrollo y empleo del ciberpoder.

Con el paso del tiempo y tras las lecciones aprendidas en Estonia[110], diversos Estados y organizaciones internacionales optaron por estructurar mecanismos de defensa especializados en dichas amenazas. Este el caso de la Organización del Tratado del Atlántico Norte (OTAN) que el 14 de junio de 2007,[111] unos días después del cese de los ciberataques contra Estonia, en el marco de una reunión en Bruselas con los Ministros de Defensa de los países miembros, reconoció la necesidad de desarrollar un marco de ciberdefensa. De esta manera, fue en Estonia donde se decidió combinar la defensa de la red con la doctrina militar planteando con ello toda una transformación a los paradigmas de seguridad tradicionales.[112]

Progresivamente, diversos países comenzaron no sólo a estructurar estrategias de defensa sino a desarrollar armamento cibernético. Entre los países cuyas capacidades tecnológicas son ampliamente conocidas figuran: Estados Unidos,

[110] Desde finales del siglo XX, Estonia se caracterizó por dar prioridad al desarrollo tecnológico con el fin de optimizar las funciones estatales, impulsando mecanismos innovadores como lo son el voto electrónico, la policía electrónica y el Documento Nacional de Identidad (DNI) electrónico, esto sólo a principios del siglo XXI. Sin embargo, pocos años más adelante en 2007 la fortaleza tecnológica se tornó en debilidad nacional, pues el 27 de abril Estonia fue blanco de una ola de ciberataques como consecuencia de la decisión gubernamental de retirar el monumento al Soldado de Bronce de Tallin. El ataque, que duró semanas, estuvo dirigido a partidos políticos, empresas especializadas en comunicaciones, ministerios, e incluso la presidencia y su parlamento. En respuesta las autoridades estatales bloquearon el tráfico internacional dejando al país aislado. Finalmente, los ataques cesaron el día 19 de mayo. Mientras que, el Ministro de Exteriores estonio, Urmas Paet, acusó directamente al gobierno ruso de los ciberataques. En el ámbito de la ciberseguridad el ataque a Estonia es ampliamente conocido debido a que representa el primer caso de un ataque cibernético de un Estado contra otro. Fuente: Fernández (2015).

[111] Fernández, Álvaro. (Agosto 12, 2015). "Estonia, baluarte de la ciberseguridad europea". *El Orden Mundial en el Siglo XXI.* [En línea]. Disponible en: <http://elordenmundial.com/2015/08/estonia-ciberseguridadeuropea/>.

[112] *Ídem.*

Israel, Irán, China, Rusia, entre otros. Cada uno de ellos acusados e incluso evidenciados[113]por el empleo de armas cibernéticas cuyas implicaciones en el plano del Derecho Internacional genera severas críticas derivadas de la ausencia de un marco regulatorio.

La situación empeora si se toma en cuenta que el conocimiento tecnológico no es exclusivo de las élites militares, pues actualmente una amplia variedad de actores no estatales (como el crimen organizado, grupos terroristas, grupos separatistas, *hacktivistas*, *hackers* etc.) poseen el conocimiento suficiente como para irrumpir en las redes informáticas militares e inhabilitar portales web estatales.

En adición, en el contexto de determinados enfrentamientos bélicos[114], han surgido facciones que adoptan la red como medio de propaganda y como espacio de acción para implementar determinadas operaciones. Se trata de guardianes o hackers patrióticos que utilizan sus altas habilidades informáticas para provocar afectaciones en portales web e instalaciones informáticas, aunque su principal objetivo es la infraestructura crítica de los países enemigos. Ante dicho escenario, las entidades estatales, como plantea Johan Sigholm (2013), podrían recurrir al uso de actores no estatales a fin de evadir las implicaciones legales que conlleva un ataque cibernético.

Los *hackers* también figuran en la lista de actores no estatales y representan uno de los primeros grupos en tener presencia en el ciberespacio, sus acciones se remontan a las décadas de los 80 y 90 del siglo pasado. Con el paso del tiempo surgieron otra clase de actores orientados por diferentes motivos como los hackers

[113] Tal es el caso de Estados Unidos que con las declaraciones del ex analista militar Edward Snowden fue evidenciado ante la comunidad internacional por el uso de dos software dedicados uno a la recolección de informes de inteligencia por todo el mundo (el programa *boundless informant*) y PRISMA dedicado a realizar operaciones de ciberespionaje a 38 embajadas y misiones diplomáticas de países como Francia, Grecia, Italia, Japón, México, Corea del sur, India, Turquía y representaciones de la Unión Europea y la Organización de Naciones Unidas. Fuentes: Alcaraz (2013) y Morris (2013).

[114] Por ejemplo, el caso del Ejército Electrónico Sirio, un grupo de hackers que apoya al gobierno de Bashar Al-Assad; el Ejército Cibernético Iraní, leal al líder supremo de Irán; *The Green Army*, el primer ejército de hackers chinos, entre otros.

patrióticos, ciberterroristas, organizaciones cibercriminales, corporaciones y cibermilicias. [115]

En el caso del *hacktivismo*, el grupo se compone de piratas informáticos que emplean sus habilidades como medio de protesta para promover una ideología o una agenda política. Sin embargo, pueden ser utilizados para alcanzar diversos fines, como por ejemplo ser empleados por parte de un Estado para causar afectaciones en los sistemas informáticos de otras naciones en busca de objetivos políticos.[116]

Uno de los actores más importantes para el ámbito de la seguridad internacional son los *hackers patrióticos*, ya que representan la adopción de Internet como un arma de gran capacidad dentro de los conflictos interestatales. Las acciones de los *hackers patrióticos* se orientan a apoyar a su propio Estado en el marco de un conflicto bélico, para ello ejecutan actividades disruptivas en contra de los sistemas informáticos del Estado enemigo. No se trata de un escenario propio de la ciencia ficción, pues para países como China estas actividades son una realidad desde hace años. Actores como la *Red Hacker Alliance* y el *Honker Union of China* han expresado abiertamente su misión patriótica.[117]

Otros actores en la red son los conocidos como *Cyber Insiders*, los cuales consisten en personas con acceso a redes y bases de datos que filtran información confidencial, también conocidos como "informantes" son capaces de tener acceso a armamento cibernético.[118] Aunque este tipo de actores es menos frecuente en comparación con los *hackers* y *hackers patrióticos* el impacto de sus acciones es significativo en el plano económico y político.[119]

Por su parte, el ciberterrorismo consiste en el traslado de la ideología y objetivos políticos de organizaciones terroristas a Internet. De este modo, la web se

[115] Sigholm, Johan. (2013). "Non-State Actors in Cyberspace Operations". *Journal of Military Studies*. no. 1, vol. 4, p. 1 [En línea]. Disponible en: <https://www.ida.liu.se/~johsi32/docs/JMS_4-1_Sigholm_NonState_Actors_in_Cyber Ops.pdf>.
[116] *Ibídem*, p.14.
[117] *Ibídem*, p.15.
[118] *Ibídem*, p.16.
[119] Tal es el caso de las filtraciones de WikiLeaks y las de Edward Snowden.

transforma en una vía para propagar el miedo público, aunque el grado en el que un ataque cibernético perpetuado por un grupo terrorista representa un riesgo para la seguridad nacional aun es objeto de debate entre los expertos en seguridad y defensa.[120]

El caso de las corporaciones es mucho más complejo pues, aunque actúan al margen de la ley, hoy en día firmas como Northrop Grumman, General Dynamics, Lockheed Martin y Raytheon cuentan con capacidades y armamento cibernético y son empleadas militarmente por el gobierno de Estados Unidos quien les ha otorgado contratos a través de sus respectivas agencias de inteligencia. Las ganancias económicas para estas firmas son importantes, pues se estima que el gobierno federal estadounidense invierte cerca 10 mil millones de dólares anuales en seguridad cibernética y la tendencia muestran que la inversión aumentará en los próximos años.[121] En adición, entidades como Northrop Grumman, General Dynamics y Raytheon Unit han desarrollado programas informáticos tanto para operaciones ofensivas como para fines de espionaje en el espectro digital.[122]

Finalmente están las milicias cibernéticas que se presentan como un grupo de expertos dispuestos a utilizar su conocimiento tecnológico para conseguir fines políticos, a diferencia de actores como las corporaciones los miembros de una cibermilicia no están obligados por medio de un contrato a prestar sus servicios y tampoco reciben remuneración por los mismos. Para expertos como Christopher Drew (2009), las unidades militares cibernéticas regulares o las ciber reservas de fuerzas nacionales no son considerados ciber milicias, pues los miembros de una cibermilicia no poseen conexiones en el mundo real. Sin embargo, aún es difícil distinguir entre un *hacker*, un *hacktivista* y un miembro de una cibermilicia. En adición, la posibilidad de apoyo por parte Estado detrás de las milicias cibernéticas es una cuestión delicada y difícil de comprobar, entre los Estados acusados de

[120] Sigholm, Johan. (2013). "Non-State Actors in Cyberspace Operations". *Journal of Military Studies*. no. 1, vol. 4, p. 17. [En línea]. Disponible en: <https://www.ida.liu.se/~johsi32/docs/JMS_4-1_Sigholm_NonState_Actors_in_Cyber Ops.pdf>.
[121] Drew, Christopher y John Markoff. (Mayo 30, 2009). "Contractors Vie for Plum Work, Hacking for U.S.". *The New York Times*. [En línea]. Disponible en: <http://www.nytimes.com/2009/05/31/us/31cyber.html>.
[122] Sigholm, *Óp. Cit., p*. 22.

utilizar este tipo de medios figuran Irán, Turquía, Israel, Corea del Norte y Corea del Sur.[123]

2.2. LA APLICACIÓN DE NUEVAS TECNOLOGÍAS EN LA FUNCIÓN MILITAR

La ciencia ha sido un indicador histórico de la evolución del conocimiento humano, en este sentido son múltiples los avances tecnológicos que representan un beneficio para la humanidad. Sin embargo, el empleo del pensamiento y las habilidades científicas también constituyen un factor crucial en el arte de la guerra. El avance de los transportes y las comunicaciones ha permitido la inclusión de diversas tecnologías en el ámbito militar, desde la aparición del telégrafo hasta los más sofisticados sistemas de radares aéreos, todos demuestran la importancia de la ciencia en el campo de batalla.

En la actualidad el significativo avance de las Tecnologías de la Información y Comunicación (TIC) ha hecho posible también la mejora en funciones de recolección y procesamiento de datos. Asimismo, el avance en la sofisticación de armamento se presenta como un elemento capaz de otorgar ventaja en el teatro de la guerra.

Muestra de esto, son las operaciones lideradas por Estados Unidos en 2003 como parte de las fuerzas de la coalición, que en Iraq confirmaron su superioridad militar.[124] El empleo de satélites de reconocimiento y sistemas de radionavegación basado en satélites (GPS, *Global Positioning System*); la mejora en las redes de Comando, Control, Comunicaciones e Inteligencia (C^3I, por sus siglas en inglés), y el uso de Vehículos Aéreos No Tripulados (*Unmanned Air Vehicles* UAVs,) demostraron una modificación en la naturaleza de la guerra.[125]

La digitalización de la guerra se ha convertido en una realidad y ha impulsado una carrera armamentista que gira en torno a la sofisticación de armamento y la

[123] Sigholm, *Óp. Cit., p*. 23.
[124] *Ídem.*
[125] Mallik, Amitav. (2004). *Technology and Security in the 21st Century A Demand-side Perspective*. SIPRI Research Report No. 20. Stockholm International Peace Research Institute y Oxford University Press. [En línea]. Disponible en: <http://books.sipri.org/files/RR/SIPRIRR20.pdf>.

estructuración de estrategias que permitan alcanzar dos objetivos: 1) disminuir el número de bajas, y 2) eliminar los daños colaterales.

Particularmente, la forma en la que la ciencia y la tecnología han reconfigurado las prácticas de seguridad y defensa en el siglo XXI se materializa en dos principales campos: 1) el armamento, y 2) la estrategia.

En el primero se han desarrollado nuevos tipos de armas que presuntamente son capaces de alcanzar los objetivos de la IT-RMA. Entre los avances más conocidos figuran:

- Armamento cibernético: definido como software y hardware especialmente diseñados para atacar sistemas y servicios ubicados en el ciberespacio o alcanzables a través de él. Este armamento es capaz de acceder a información confidencial y de alterar o impedir el funcionamiento de sistemas informáticos.[126]
- Armamento inteligente: consisten en armas que cuentan con un grado de autodirección también denominado "inteligencia" que las distingue del resto de las armas convencionales debido a que para alcanzar sus objetivos requieren de un mínimo de apoyo del exterior.[127]
- Los Vehículos No Tripulados: refiere a vehículos militares (que pueden ser utilizados en el aire, tierra, sobre y debajo del mar) que no precisan de la presencia del factor humano para su operación, por ello el costo político de su empleo es menor ya que representan una disminución de riesgo para los soldados, poseen una alta operatividad (ya que incluso pueden ser empleados en escenarios de alta amenaza como un ambiente nuclear), son sencillos de transportar y desplegar, y poseen ventajas que los hacen menos detectables que el resto de los vehículos militares.[128] Al respecto, existen dos

[126] Prieto Osés, GB. D. Ramón, et al. (Abril, 2013). *Guerra Cibernética: Aspectos organizativos*. CESEDEN, XXXIII Curso de Defensa Nacional, p. 3 [En línea]. Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf>.
[127] Serrano, Andres S. (Febrero 14, 1991). "Armas inteligentes para 'disparar y olvidarse'". *El país*. [En línea]. Disponible en: <http://elpais.com/diario/1991/02/14/internacional/666486026_850215.html>..
[128] Fernández Merino, Félix. (Marzo, 2012). *Los sistemas no tripulados*. España: Ministerio de Defensa, p.9.

modalidades de vehículos no tripulados, aquellos que son empleados con fines de reconocimiento y recolección de inteligencia, y los que han sido habilitados para llevar a cabo operaciones de combate.

En el plano organizacional y estratégico emerge la necesidad de nuevos conceptos adaptativos que puedan aplicarse a las operaciones militares que ahora incluyen el uso del ciberespacio como parte importante de las estrategias de seguridad. Aparece también la necesidad de estructurar dinámicas operacionales en red que sean capaces de asegurar el debido intercambio de información entre los integrantes militares que actúan dentro de una coalición militar, ya que la administración de información a través de las nuevas plataformas de comunicación posee un carácter primordial dentro en las operaciones militares modernas, así lo demuestran el programa multinacional de datos seguros CENTRIXS utilizado en escenarios como Afganistán (2001) e Iraq (2003).[129]

Los planteamientos estratégicos modernos se inclinan a la estructuración fuerzas especiales que cuenten con el dominio de herramientas altamente tecnológicas y el uso de Internet como espacio y arma de guerra. De acuerdo con Patrick Michael Duggan (2015), esto puede observarse en Estados como Rusia e Irán quienes han integrado el uso de tecnología asimétrica dentro de operaciones de combate no convencionales, que se han ocupado en casos como el de Ucrania y en contra del Movimiento Verde, respectivamente.[130]

Hoy en día las estrategias de seguridad orientan a las Fuerzas de Operaciones Especiales a evitar la aplicación directa de fuerza contra fuerza y a adoptar técnicas de combate que se efectúan en zonas grises entre la paz y la guerra. Al mismo tiempo, la recolección, procesamiento y distribución se convierte en una tarea mucho más compleja. Además, las nuevas tácticas militares contenidas en la

[129] Zimet, E. y Charles L. B. (2009). Military Service Cyber Overview. En L. K. Wentz, C. L. Barry y S. H. Starr, ed., *Military Perspectives on Cyberpower*. Washington, DC: The Center for Technology and National Security Policy at The National Defense University, pp. 2-4. [En línea]. Disponible en: <http://www.dtic.mil/cgi-bin/GetTRDoc ?AD=ADA 505424>.

[130] Michael Duggan, P. (2015). "Strategic Development of Special Warfare in Cyberspace". *Joint Force Quarterly 79*, pp.47-48. [En línea]. Disponible en: <http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_46-53_Dugg an.pdf> .

estrategia militar prevén la actuación de las Fuerzas de Ciber-Operaciones Especiales antes de que los soldados intervengan en el campo de batalla.[131]

2.2.1. La transformación en la naturaleza y conducción de conflictos

Hoy en día, los estrategas se inclinan más a la ejecución operaciones rápidas y efectivas que aseguren la disminución de riesgos para un ejército. Por consecuencia, el uso de aviones no tripulados representa un elemento ventajoso, aunque la disminución del daño colateral no esté asegurada. Así lo demuestran diversos informes y reportes de Amnistía Internacional y otras organizaciones internacionales.[132]

En cuanto a la estructura, se crean divisiones especializadas en el uso del ciberespacio. Dedicadas de manera abierta a la defensa, aunque las capacidades de ataque no han sido reconocidas de manera oficial por parte de ninguna entidad de esta naturaleza.[133]

En este punto vale pena mencionar a los llamados sistemas SCADA (por sus siglas en inglés *Supervisory Control And Data Adquisition*) los cuales consisten en software diseñados para la adquisición de datos, el control y supervisión de funciones dependientes de ordenadores.[134] En otras palabras, se trata de controladores autónomos programables que se utilizan en diversos tipos de redes, por ejemplo, en las de abastecimiento de energía eléctrica, agua, centrales nucleares etc., y que actualmente representan una importante fuente de vulnerabilidad para los Estados-nación.

---

[131] *Ibídem*, pp.50-51

[132] Como la declaración de Amnistía Internacional "Drone Wars: The Constitutional and Counterterrorism Implications of Targeted Killing" presentada ante el Senado de Estados Unidos el 16 de abril de 2013; el informe del Relator Especial sobre ejecuciones extrajudiciales, sumarias o arbitrarias, Christof Heyns, ante la Asamblea General de Naciones Unidas el 9 de abril de 2013; el análisis realizado por el Instituto Kroc de Estudios Internacionales de Paz "Ethical, Strategic & Legal Implications of Drone Warfare", publicado en marzo de 2013, entre otros documentos.

[133] Si bien, en abril de 2016 el gobierno estadounidense reconoció la creación de una línea de combate cibernética contra el Estado Islámico, el reconocimiento de sus capacidades ofensivas es aún cauteloso debido a las implicaciones que para el Derecho Internacional representa el uso de armas cibernéticas. Fuente: Sanger (2016).

[134] Gutiérrez Amaya, Camilo. (Enero 25, 2013). "¿Qué tan críticos son los sistemas SCADA?". *We live security*. [En línea]. Disponible en: <http://www.welivesecurity.com/la-es/2013/01/25/criticos-sistemas-scada/>.

Por lo tanto, la ciberdefensa se ha convertido en un pilar para la seguridad nacional. Por ello, en el plano militar se han desarrollado dos tipos de regímenes para el dominio del ciberespacio. El primero consiste en una red abierta en donde la colaboración, el intercambio de información y la consciencia de la situación son las principales medidas de actuación. El segundo régimen emplea redes cerradas y seguras donde la velocidad de la operación, la entrega asegurada y la integridad de la información son de suma importancia.[135] (Ver figura 3)

FIGURA 3 CIBERPODER MILITAR - APOYO DEL CIBERESPACIO A CONCEPTOS OPERACIONALES, ESTRATEGIA Y FUNCIONES PARA ALCANZAR OBJETIVOS MILITARES

Fuente: Wentz, Larry K.; Charles L. Barry, y Stuart H. Starr. (2009). *Military Perspectives on Cyberpower*. Washington, DC: The Center for Technology and National Security Policy at the National Defense University p. 5.

[135] Zimet, Elihu y Charles L. Barry. (Julio, 2009). Military Service Cyber Overview. En Wentz, Larry K.; Charles L. Barry, y Stuart H. Starr. *Military Perspectives on Cyberpower*. Washington, DC: The Center for Technology and National Security Policy at the National Defense University pp.4-5. [En línea]. Disponible en: <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA505424/>. (Consulta 10/11/2016)

2.2.2. La innovación y sofisticación del armamento convencional

La adopción de nuevas armas cambia la relación entre los componentes de una organización militar y a los propios planteamientos de actuación.[136]

De manera general, el empleo de armamento con alto grado de tecnología genera tres ventajas significativas:

- Aumento en la velocidad: la reducción en el tiempo para ejecutar una operación y para recolectar, procesar y transmitir de datos.
- Reducción de costos: se minimiza la cantidad de recursos económicos empleados.
- Mayores alcances: mayor capacidad en el nuevo armamento, los vehículos militares y del procesamiento de información.[137]

En el caso del armamento, la innovación científica busca mejorar el alcance y la letalidad, a fin de disminuir el daño colateral y las bajas en el ejército. Sin embargo, la validez de esta proposición aún es discutida en el ámbito de los Derechos Humanos.

2.2.2.1. Sistemas de Inteligencia, vigilancia y reconocimiento

Dentro de las operaciones militares la actividad sobre la que recae gran parte del éxito de las campañas es la inteligencia. El subministro de información sobre las condiciones geográficas del campo de batalla y sobre las características del enemigo son un factor clave dentro de la función militar.

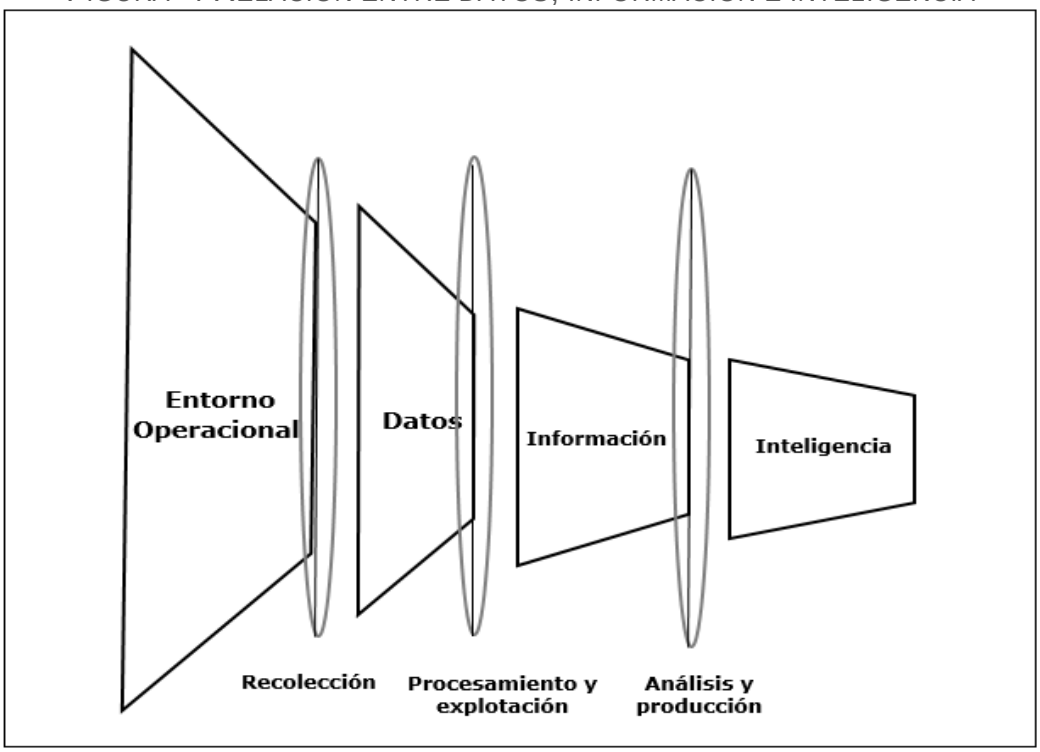
La innovación de la Tecnologías de la Información y Comunicación (TIC) ha propiciado también una transformación en la planificación, conducción y ejecución de las acciones militares a nivel operacional y táctico. Al mismo, tiempo emerge la necesidad de perfeccionar el ciclo de OODA (Observar, Orientar, Decidir y Actuar,

[136] Jordán, Javier. (Abril 28, 2014). "Una introducción al concepto de innovación militar*". Grupo de Estudios en Seguridad Internacional (GESI)*. [En línea]. Disponible: <http://www.seguridadinternacional.es/?q=es/content/una-introducci%C3%B3n-al-concepto-de-innovaci%C3%B3n-militar>. (Consulta 26/11/2016).

[137] Torres Soriano, Manuel R. (2008). Información y Conflictos Bélicos en la Era de Internet. En Fernández Rodríguez, José Julio; Javier Jordán Enamorado, y Daniel Sansó-Rubert Pascual. *Seguridad y Defensa hoy: Contruyendo el futuro*. Madrid: Plaza y Valdés, p. 34.

OODA) que configura una pieza esencial en los sistemas de mando y control. [138] (Véase figura 4)

FIGURA 4 RELACIÓN ENTRE DATOS, INFORMACIÓN E INTELIGENCIA



Fuente: Bravo Tejos, Gonzalo. (Enero, 2010). "El Proceso de Inteligencia, Vigilancia, Adquisición de blancos y reconocimiento". *Revismar*, p.59.

Otra transformación importante es el rango temporal del empleo y actualización de la información, pues mientras en épocas pasadas su aplicación sobre las operaciones militares se limitaba a la etapa de planeación, hoy en día el suministro de información es posible antes, durante y después del enfrentamiento. Antes el flujo de datos para las campañas militares dependía de las labores de vigilancia y reconocimiento ejecutadas a unas millas de distancia de la actuación de las fuerzas armadas, actualmente es posible transmitir imágenes y sonidos mientras la operación se lleva acabo.[139]

[138] Bravo Tejos, Gonzalo. (Enero, 2010). "El Proceso de Inteligencia, Vigilancia, Adquisición de blancos y reconocimiento". *Revismar*, pp. 59-60. [En línea]. Disponible en: <http://revistamarina.cl/revistas/2010/1/bravo.pdf >.

[139] *Ibídem*, p. 60.

En el campo militar la importancia de las actividades de Inteligencia, Vigilancia, Adquisición y Reconocimiento de objetivos (ISTAR por sus siglas en inglés *Intelligence, Surveillance, Target Acquisition and Reconnaissance*) experimenta una transformación en sus capacidades, lo que permite mejoras en las labores de adquisición, procesamiento y difusión coordinada de información e inteligencia que funciona de forma oportuna y precisa en las operaciones modernas.[140]

Así, las TIC afectan las prácticas de inteligencia contemporáneas en tres diferentes dimensiones: la primera se relaciona con la complejidad de las operaciones, dotándolas de nuevas modalidades de acción e incluso de un nuevo espacio de actuación: el ciberespacio. La segunda dimensión se refiere a la cantidad de datos suministrados y la necesidad de estructurar mecanismos para su análisis y difusión (por ejemplo, el programa *Boudless informant* de la NSA). La última dimensión consiste en la difusión de las fronteras tradicionales de los niveles táctico, operacional y estratégico, ya que por ejemplo en el espectro cibernético la cuestión de la soberanía es aún punto irresoluto. En adición, las capacidades de los vehículos aéreos no tripulados dotados de tecnología *stealth*[141]suscita tensiones entre Estados acusados de violar el espacio aéreo de otros.[142]

2.2.2.2. Armamento inteligente y sistemas de defensa antimisiles

A través del tiempo la aplicación de la innovación tecnológica en el plano de las armas le ha otorgado mayor automatización y un espacio más amplio de actuación debido a la incorporación de tecnologías como el rayo láser, la visión nocturna, la programación y detonación a distancia, los sensores térmicos y la alta definición, capacidades que buscan asegurar la disminución en el costo humano y económico que para un país representan los conflictos bélicos.

---

[140] *Ídem*.

[141] Esta tecnología está basada en el trabajo del matemático y científico soviético Pyotr Ufimtsev, la tecnología *stealth* refiere a la capacidad de actuar de una aeronave de forma furtiva; es decir, que la energía emitida o reflejada por el vehículo aéreo o por sus diferentes componentes es indetectable por los radares, para ello se pretende predecir mediante ecuaciones el reflejo de las ondas electromagnéticas. Fuente: Casus Belli (2016).

[142] Escuela Superior de las Fuerzas Armadas. (Octubre 16, 2014). *Apuntes de Inteligencia, Contrainteligencia y Seguridad. Fase Conjunta del Curso de Actualización de Ascenso a Comandante*. Departamento de Inteligencia y Seguridad, p. 3 [En línea]. Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/esfas/cursos/curActAscensoCte/ficheros/M5_1DocApoyoCTE_APUNTES_DE_INTELIGENCIA_CACES.pdf>.

De esta forma se califican como “inteligentes” a todo armamento que implemente varios dispositivos tecnológicos con el fin de mejorar su funcionalidad[143]. Las municiones inteligentes por su parte consisten en proyectiles lanzados por tanques, buques y morteros que son dirigidos y poseen un 90% de precisión. Un proyectil inteligente cuenta con unidades MEMS de orientación inercial, así como con controles que se valen del empleo del GPS para localizar el blanco. Al respecto, es importante apuntar que es posible transformar municiones convencionales en municiones inteligentes con la sola inclusión de unidades MEMS. En otras palabras, se trata del empleo de la denominada Inteligencia Artificial en el plano armamentista.[144]

El empleo de armamento automatizado por parte de las fuerzas armadas de diversos países plantea una serie de cuestiones éticas debido a que se teme que en el futuro la selección y neutralización de objetivos sean relegados a dispositivos electrónicos cuya única guía de actuación son básicamente algoritmos.[145]

En el plano internacional el empleo de armamento autónomo plantea también un dilema, sobre todo dentro de la comunidad científica responsable del desarrollo de la inteligencia artificial. Actores como *Human Rights Watch* y otras ONG han demandado el cese en la creación y empleo de armamento autónomo e incluso se han solicitado a la Convención sobre Ciertas Armas Convencionales (CCA) que se establezca un límite a la producción.[146]

De acuerdo con el Comité Internacional de la Cruz Roja, el uso cada vez más frecuente de armamento inteligente plantea una serie de implicaciones legales ante la posible falla de este tipo de armamento, además de que, al eliminar el factor humano del campo de batalla las fuerzas armadas son menos conscientes de las

---

[143] “Las ‘armas inteligentes’ que no quieren los defensores de las armas”. (Mayo 23, 2014). *BBC*. [En línea]. Disponible en: <http://www.bbc.com/mundo/noticias/2014/05/140523_tecnologia_arma_inteligente_oposicion_mz>.

[144] Adams, James. (1999). *La próxima guerra mundial: los ordenadores son las armas y el frente está en todas partes*. Argentina: Granica, p. 203.

[145] EFE. (Julio 28, 2015). “Miles de científicos piden que se detenga el desarrollo de armas inteligentes y autónomas”. *El diario.* [En línea]. Disponible en: <http://www.eldiario.es/turing/armamento-inteligencia_artificial-carrera_arma mentistica_0_414009439.html>.

[146] *Ibídem*.

consecuencias de sus acciones y de los efectos que infringen sobre la población civil, y se habla entonces de una deshumanización de la guerra.[147]

Por otra parte, están los denominados Sistemas de Defensa Antimisiles, cuya función a grandes rasgos consiste en neutralizar la amenaza que representan los misiles balísticos. Con el fin de analizar este sistema de defensa es preciso determinar primero en qué consisten los misiles balísticos: se tratan de misiles que una vez liberada su fuerza expulsora siguen una trayectoria programada, aproximadamente balística y determinada por la gravedad y la resistencia aerodinámica de la trayectoria que se desarrolla dentro de la atmósfera,[148] por lo que es posible afirmar que forman parte del armamento inteligente debido a su alto grado de automatización.

Los misiles balísticos son militarmente más efectivos debido a que en comparación con los misiles aerodinámicos son veloces y poseen mayores alcances, aunque su nivel de precisión es menor.[149] Los misiles balísticos en función de su alcance se clasifican en:

- Mísiles de Corto Alcance o SRBM (por sus siglas en inglés *Short-Range Ballistic Missile*). - poseen un alcance de hasta 1000 kilómetros.
- Misiles de Medio Alcance o MRBM (por sus siglas en inglés *Medium-Range Ballistic Missile*). - tiene un alcance de entre 1000 y 3000 kilómetros.
- Misiles de Alcance Intermedio o IRBM (por sus siglas en inglés *Intermediate-Range Ballistic Missile*). - pueden actuar a distancias de entre 3000 y 5500 kilómetros.

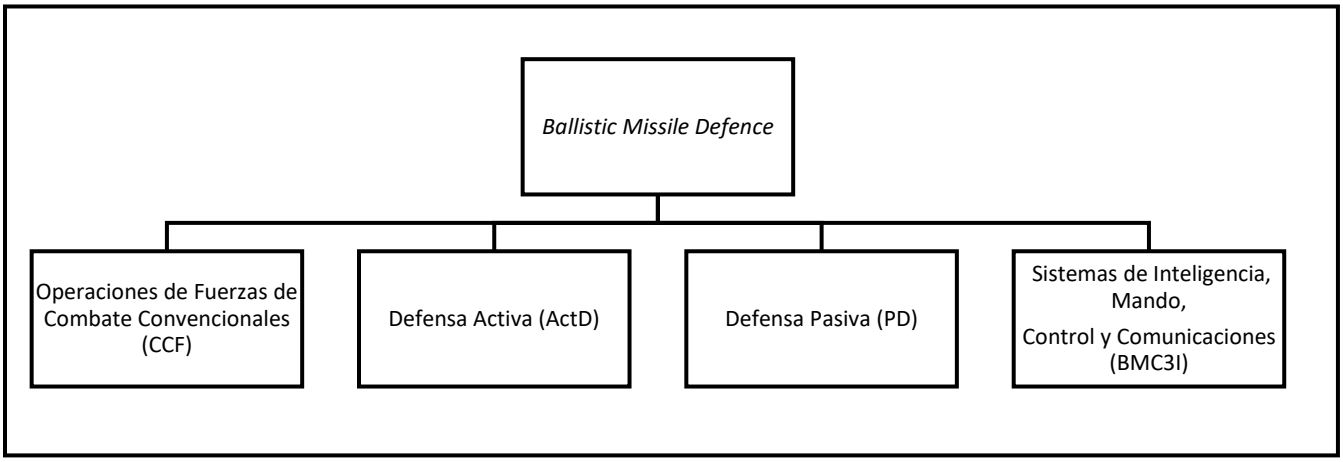
[147] Rogers, A.P.V. (Marzo 31, 2000). "Una guerra sin víctimas". *Revista Internacional de la Cruz Roja*. [En línea]. Disponible en: <https://www.icrc.org/spa/resources/documents/misc/5tdnzd.htm>.
[148] Broch Hueso, Joaquín. (Diciembre, 2012). "La Contribución del ET a la Defensa Antimisil". *Instituto Español de Estudios Estratégicos*. Documento Marco, p. 3. [En línea]. Disponible en: <http://www.ieee.es/Galerias/fichero/doc s_marco/2012/DIEEEM12-2012_ContribucionETDefensaAntimisil_JBrochHUeso.pdf>. .
[149] *Ibídem*., p. 4.

- Misiles Intercontinentales o ICBM (por sus siglas en inglés *Inter-Continental Ballistic Missile*). - con la capacidad de alcanzar objetivos ubicados a más de 5 500 kilómetros.[150]

Estos misiles poseen una velocidad de entre 4 y 8 kilómetros por segundo dependiendo de su alcance, actualmente representan una de las cuestiones más importantes en el plano de la defensa debido a que su detección e intercepción son complicadas. Entre los países que poseen esta clase de misiles figuran: Estados Unidos, Francia, Gran Bretaña, Irán, Corea de Norte, India, Pakistán, Rusia, Israel, entre otros.[151]

De forma general, se conoce como defensa antimisil a todas las medidas necesarias para proteger un territorio, población o fuerzas contra el impacto de misiles tanto balísticos como aerodinámicos. En el plano de los estudios de seguridad se le conoce como BMD, por sus siglas en inglés *Ballistic Missile Defence*. El BMD descansa en cuatro pilares (ver figura 5). El CCF, se encarga de prevenir su lanzamiento mediante la destrucción de bases; el ActD, se orienta a localizar y destruir misiles en vuelo; PD, se encarga de minimizar los ataques del enemigo, y los BMC3I, están orientados a coordinar y sincronizar el resto de las medidas.[152]

FIGURA 5 COMPONENTES DEL SISTEMA DE DEFENSA ANTIMISILES



Fuente: Elaboración propia con datos obtenidos de Broch Hueso, Joaquín. (Diciembre, 2012). "La Contribución del ET a la Defensa Antimisil". Instituto Español de Estudios Estratégicos. Documento Marco, p. 10.

[150] *Ídem*.
[151] *Ibídem.,* pp. 6-9.
[152] *Ibídem.,* p 10.

Por su parte, el escudo de defensa antimisiles se compone de radares, centros de comando y el lanzador de misiles, aunque basados en el nombre se pudiera inferir que se trata sólo de medidas de protección, el escudo antimisiles consiste en el lanzamiento de municiones encaminadas a neutralizar una amenaza en trayecto, ya sea en la fase de aceleración (boost), intermedia (midcourse) o terminal (terminal o descent).[153]

Para su funcionamiento emplea un radar, el cual le permite detectar misiles que han sido disparados y evaluar su trayectoria, acto seguido un software se encarga de lanzar dos proyectiles antimisiles que tienen el objetivo de interceptar la amenaza en el aire. Los misiles interceptores parten del lanzacohetes, que tiene la capacidad de encontrar proyectiles en trayectoria a una distancia de 4 a 70 kilómetros. Aunque debido a su sofisticación el sistema de defensa antimisiles puede parecer infalible, lo cierto es que es susceptible a ataques cibernéticos, así como a operaciones de ciberespionaje, como sucedió en el caso de Israel en donde piratas informáticos obtuvieron información altamente confidencial relacionada con los sistemas de defensa israelí e incluso con planos de aviones no tripulados.[154]

El despliegue de Sistema de Defensa Antimisiles a través de las fronteras en diversas partes del mundo es capaz de elevar tensiones entre dos o más Estados, al mismo tiempo reanima el debate en torno a la restricción y control en la producción de armamento inteligente. Fue precisamente la evolución en el alcance de los misiles de precisión lo que impulsó el desarrollo y sofisticación de los Sistemas de Defensa Antimisiles, la innovación en este sector se concentró en neutralizar los misiles intercontinentales, así como aquellos capaces de transportar carga nuclear, entonces se buscó hacer posible su intercepción más allá de la atmosfera terrestre (es decir, en la exo-atmosfera).[155]

---

[153] *Ibídem.*, p. 4.

[154] Bermúdez, Emma. (Agosto 6, 2014). "Así funciona el escudo antimisiles de Israel". *El Confidencial*. [En línea]. Disponible en: <http://www.elconfidencial.com/tecnologia/2014-08-06/asi-funciona-el-escudo-antimisiles-de-israel_172468/>.

[155] Coffey, J. I. (Diciembre 27, 1966). "The Anti-Ballistic Missile Debate". Foreign Affairs. [En línea]. Disponible en: <https://www.foreignaffairs.com/articles/1967-04-01/anti-ballistic-missile-debate>.

Además de sus capacidades defensivas, la ventaja de los Sistemas de Defensa Antimisiles recae en su potencial disuasorio, a la par de su capacidad para desalentar el desarrollo de nuevos misiles balísticos. Empero, no representan una herramienta infalible debido a que dentro de un escenario de tensión se incentivaría el desarrollo de armamento de otra naturaleza como aquellos que actúan en el agua o en tierra. [156]

2.2.2.3. Los aviones no tripulados

Uno de los adelantos tecnológicos más importantes en la guerra moderna son los Vehículos Aéreos No tripulados, utilizados desde la Segunda Guerra Mundial, aunque sólo con fines de reconocimiento.[157]No fue sino hasta el siglo XXI que se le incorporaron capacidades de combate conformando lo que hoy se conoce como UCAVs (por sus siglas en inglés *Unmanned Combat Aerial Vehicles*).[158] El uso de UCAVs como uno de los vehículos militares más innovadores conlleva dos grandes cuestiones:

1) La sofisticación tecnológica en el campo militar que ha permitido, de acuerdo con los objetivos de la Revolución Tecnológico Informacional de los Asuntos Militares, reducir el número de bajas en un ejército
2) El empleo de armamento que no se encuentra especialmente regulado y cuyo uso representa serios retos para el Derecho Internacional Humanitario (DIH), debido a las repercusiones generadas sobre la población civil.

Existen numerosos análisis sobre las consecuencias del uso de UCAVs tanto en el plano militar como el ámbito de los Derechos Humanos.[159] Por su parte, desde

[156] *Ídem.*

[157] Farley, Robert. (Febrero 26, 2015). "The 5 Most Lethal Drones of All Time". *The National Interest*. [En línea]. Disponible en: <http://nationalinterest.org/feature/the-5-most-lethal-drones-all-time-12326>..

[158]Dowd, Alan W. (2013). "Drone Wars: Risks and Warnings". Parameters. Winter/Spring 2013, p. 1. [En línea]. Disponible en: <http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Winter_2013/TheQuarterly_Win ter2013-14_v43n4.pdf>.

[159] En el ámbito de los Derechos Humanos investigaciones como "Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions" presentado por el Consejo de Derechos Humanos ante la Asamblea General de Naciones Unidas; "Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare" elaborado por el Centre for Security Policy (GCSP) y la Geneva Academy que fue presentado ante el Parlamento Europeo. En el ámbito militar trabajos como "Unmanned Aerial Vehicles:

la perspectiva de la defensa el uso de UCAVs representa ventajas considerables en comparación con los vehículos aéreos convencionales cuyo funcionamiento depende de la presencia del factor humano. Así, los UCAVs implican menor riesgo y mayor eficacia para los ejércitos de los Estados que poseen dicha tecnología. En adición, son cada vez más países los que deciden integrarlos a sus estrategias de defensa, como por ejemplo Reino Unido, Rusia, China, Turquía, Italia, Israel, India, Alemania y Francia.[160]

La integración de los UCAVs a las operaciones de defensa ha sido tan exitosa que el ejército estadounidense ha aumentado 1200% el patrullaje aéreo de combate desde 2005, por lo que sus aviones no tripulados han efectuado misiones en Pakistán, Iraq, Libia, Afganistán, Yemen, Somalia y Filipinas.[161]

En el plano económico los UCAVs representan menores costos, pues mientras un avión bombardero B-2 cuesta casi 2 mil millones de dólares, un *Drone predator* sólo 4.5 millones.[162] Empero, el empleo de UCAVs no significa la ejecución de una operación perfecta, pues existen casos en donde los vehículos no tripulados se salieron de control causando serios daños colaterales, como en 2011 cuando una de estas aeronaves chocó con un avión de carga al este de Irán. [163]

En adición, el uso de UCAVs y la inexistencia de riesgo para un soldado resultan ser incentivos para una guerra de larga duración, en donde el peligro se elimina para el ejército atacante, pero aumenta de forma significativa para las fuerzas contrarias y lo más importante para la población civil. El daño colateral sobre los no combatientes es alarmante, pues las cifras indican que en escenarios como Pakistán los UCAVs causaron cerca de 400 muertes de civiles.[164]

Implications for Military Operations" del Center for Strategy and Technology Air War College, y "Civil UAV Capability Assessment" de la NASA, entre otros.

[160] International Institute for Strategic Studies. (2016). "Drones by country: who has all the UAVs?". *The Guardian*. [En línea]. Disponible en: <https://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-by-country>..

[161] Dowd, *Op. Cit.* p. 2.

[162] Dowd, *Op. Cit*. p. 9.

[163] Dowd, *Op. Cit*. p. 10.

[164] Dowd, *Op. Cit*. p. 13.

Por ello, el uso de la fuerza de forma extraterritorial por parte de los Estados genera consecuencias legales en el plano internacional que se relacionan con cuestiones como la soberanía y la prohibición del uso de la fuerza entre Estados contenida en la Carta de Naciones Unidas.[165]Desde el marco del Derecho Internacional Humanitario (DIH) los drones no están expresamente prohibidos. Sin embargo, están sujetos a dichas normas al ser empleados en el marco de conflictos armados, por lo que quienes las emplean están obligados a diferenciar entre combatientes y civiles.[166]

En síntesis, el uso de armamento inteligente tanto con fines de defensivos u ofensivos suscita múltiples debates que giran en torno a la despersonalización de la guerra y el daño colateral de este tipo de armamento. En este sentido, el papel de Derecho Internacional Humanitario es muy importante, así por ejemplo en el caso del empleo de armamento inteligente el Protocolo I de Ginebra de 1977 insta a los Estados partes a asegurarse, antes de lanzar un ataque, que los objetivos que se pretenden atacar sean militares, incluso los países que no forman parte del Protocolo de Ginebra reciben la obligación por parte del Derecho Consuetudinario de identificar y no atacar objetivos civiles.[167]

En adición, a pesar de que el armamento inteligente cuenta con mayor precisión no es capaz de eliminar el daño colateral, además sigue dependiendo de factores secundarios tales como las características geográficas del terrero, las circunstancias bajo las que se lleva a cabo la operación y la información que sobre el objetivo se tenga.

2.3. INDICADORES Y ASPECTOS DE LA CIBERGUERRA

Como se expuso anteriormente, existen múltiples posicionamientos respecto a la existencia de una revolución en los asuntos militares. No obstante, en todos ellos el

[165] Melzer, Nils. (2013). Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare. Bélgica: European Union, p. 14. [En línea]. Disponible en: <http://www.europarl.europa.eu/RegData/etudes/etudes/join/201 3/410220/EXPO-DROI_ET(2013)410220_EN.pdf>.

[166] Comité Internacional de la Cruz Roja. (Mayo 10, 2013). "El uso de los drones armados debe estar sujeto a la ley". [En línea]. Disponible en <https://www.icrc.org/spa/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm>

[167] Rogers, *Op. Cit*.

valor e impacto del ciberespacio es indiscutible. En este campo, uno de los primeros análisis es el elaborado por John Arquilla y David F. Ronfeldt publicado en 1992 y titulado *Cyberwar is Coming¡*, en él se hace referencia a la creciente importancia de la tecnología informática en las prácticas de guerra y al papel significativo del tratamiento y difusión de la información. A partir de entonces, la producción bibliográfica alrededor de la ciberguerra se hizo más abundante, aparecieron libros como *Cyberspace and the State: Toward a strategy for cyber-power* de David J. Bentz y Tim Stevens; *Cyberwar: The next threat to national security and what to do about it* de Richard A. Clarke y Robert K. Knake; *Cyberwar will not take place* de Thomas Rid, *Cyberdeterrence and cyberwar* de Martín Libicki, entre muchos otros.

Los primeros estudios centraron su atención en el uso de la ciberguerra como medio de espionaje. Más adelante, con la aparición del virus Stuxnet[168] las agencias de seguridad de diversos países encendieron las alarmas al percatar la posibilidad del empleo de armamento cibernético para controlar o dañar infraestructura crítica nacional.[169]

Sin embargo, considerar al ciberespacio como el campo de batalla de los próximos enfrentamientos bélicos equivale a sobredimensionar sus capacidades, ya que el escenario más crítico para los expertos en seguridad es aquel en donde se combinan las operaciones militares tradicionales y los ataques cibernéticos. Empero, es preciso comprender la evolución histórica de la ciberguerra ya que al igual que las otras modalidades de enfrentamiento ha sufrido transformaciones a través del tiempo. (Ver tabla 1)

[168] Stuxnet es el nombre de un gusano electrónico que en 2010 tomó el control de 1000 máquinas que participaban en la producción de materiales nucleares y las llevó a la autodestrucción en la planta nuclear de Nantaz en Irán. Este caso en muy conocido en el ámbito de la ciberguerra ya que representa la primera vez que un ataque cibernético logró afectar una infraestructura del espacio tangible. La naturaleza de Stuxnet es única ya que fue diseñado exclusivamente para fines bélicos. EL virus actuó de la siguiente forma: 1) Fue insertado por medio de una USB infectada a la red informática de Nantaz; 2) Buscó y tomó el control del software que controlaba las máquinas centrifugadoras; 3) Provocó que las centrifugadoras giraran a una velocidad mayor, acción que repetiría por intervalos diferentes de tiempo y con duración variada, y 4) El daño provocado por la aceleración hiso que alrededor 1000 que ejecutados de forma sincronizada representan una amenaza importante para seguridad de un Estado centrifugadoras infectadas se desintegraran. Fuente: BBC (2015).

[169] Rodríguez, Alex. (2015). "Cyber: guerra, ataque, espacio y disuasión…". La Ciberguerra. Vanguardia Dossier, No. 54, Enero-Marzo 2015, p.3.

TABLA 1 FASES DE LA HISTORIA DEL CONFLICTO CIBERNÉTICO

	REALIZACIÓN	PUESTA EN MARCHA	MILITARIZACIÓN
	1980	1998	2003
Equilibrio de fuerzas	*Los agresores tienen ventaja sobre la defensa*	*Los agresores tienen ventaja sobre la defensa*	*Los agresores tienen ventaja sobre la defensa*
Quién tiene los medios	*Estados Unidos y algunos otros protagonistas poco poderosos*	*Estados Unidos, Rusia, China, y muchos otros.*	*Gran número de protagonistas (escenario mayor)*
Adversarios	*Piratas Informáticos*	*Piratas Informáticos activistas, piratas informáticos patriotas*	*Agentes de Información, fuerzas armadas, piratas informáticos activistas*
Incidentes principales	*Ver Morris (1988) Citibank (1994)*	*Moonlight Maze, Sunrise…*	*Titan Rain, ataques contra Estonia, conflicto ruso-georgiano, Stuxnet.*

Fuente: Ventre, Daniel. (2015). "Evolución de la guerra desde hace un siglo: aparición de la ciberguerra". *La ciberguerra*. Vanguardia Dossier, No. 54, Enero-Marzo 2015, p. 20.

En la actualidad, se entiende por ciberguerra a "el uso del ciberespacio en el contexto de conflictos armados interestatales o intraestatales"[170], las operaciones ejecutadas en este contexto actúan desde y/o hacia sistemas militares, redes de las fuerzas armadas, plataformas de información desplegadas en áreas de operación (por ejemplo, los sistemas de Control, Comando, Comunicaciones, Computación, Inteligencia, Vigilancia y Reconocimiento, C4ISR), aunque también pueden actuar en contra de redes informáticas de naturaleza civil.[171]

Los actores estatales y no estatales ejecutan operaciones en los diferentes estratos de acción del espectro cibernético beneficiados por el anonimato y la dificultad para atribuir un ataque. (Ver tabla 2)

[170] Ventre, Daniel. (2015). "Evolución de la guerra desde hace un siglo: aparición de la ciberguerra". *La ciberguerra*. Vanguardia Dossier, No. 54, Enero-Marzo 2015, p. 21.
[171] *Ídem*.

TABLA 2 ESTRATOS, PROTAGONISTAS Y ACCIONES EN EL CIBERESPACIO

	NIVEL DE ESTRATO	CARACTERÍSTICAS	FORMAS DE ATAQUES POSIBLES CONTRA EL ESTRATO	HECHOS
E3	Estrato Alto	*Estrato cognitivo*	*Modificar la visualización de los ordenadores, desfigurar los sitios, introducir mensajes modificadores de las percepciones, realizar operaciones de propaganda, piratería informática cognitiva*	*Desfiguraciones del sitio, piratería informática activista, WikiLeaks, uso de redes sociales para movilizar a las multitudes. Un ataque contra el estrato cognitivo consiste en manipular los contenidos para manipular a los protagonistas.*
E2	Estrato Mediano	*Estrato aplicativo: programas, estrato de bits, del código, de las normas, de los protocolos, de los datos*	*Ataques por el código: piratería informática, propagación de virus…*	*Desfiguración de sitios, piratería informática activista, pirateado de servidores de ministerios, intrusiones, ataques de denegación de servicios (DDoS en inglés), robos de datos*
E1	Estrato Bajo	*Estrato físico, material, partes materiales de un ordenador, cables, redes, satélites, ordenadores, material de comunicación, infraestructuras conectadas.*	*Cortar cables submarinos, destruir o desviar satélites de su trayectoria, bombardear edificios de servidores e infraestructuras de comunicación, uso de bombas de pulso electromagnético (EMP, en inglés)*	*Corte de cables submarinos para paralizar Internet en Egipto*

Fuente: Ventre, Daniel. (2015). "Evolución de la guerra desde hace un siglo: aparición de la ciberguerra". *La ciberguerra*. Vanguardia Dossier, No. 54, Enero-Marzo 2015, p. 24.

Sin embargo, pese a los extensos estudios sobre la guerra informática aún existen cuestiones difíciles de resolver, entre ellas se encuentran:

1) El problema de la atribución de responsabilidades, hallar el origen de un ataque cibernético es una labor complicada, aún más si te toma en cuenta que esta clase de operaciones puede llevarse a cabo a través del empleo de comandos de control remoto en donde los dispositivos son infectados con un software malicioso que se apropia de las funciones del equipo y se encarga de lanzar ataques cibernéticos desde este punto sin que el propietario se percate.
2) En el plano internacional parece prácticamente imposible establecer límites de acción en la red y determinar un espacio soberano para cada nación.

3) Establecer la condición jurídica de aquellos involucrados en el ciberconflicto, es decir, crear una distinción entre combatientes y civiles.
4) Crear medidas efectivas para la protección de la red de redes sin violar derechos de la ciudadanía tales como el derecho a la libertad de expresión y a la privacidad.
5) Crear un marco jurídico que regule las actividades militares en el ciberespacio, así como el uso del armamento cibernético.
6) Determinar qué clase de acciones constituyen un acto de guerra y pueden justificar el uso de la legitima defensa.[172]

2.3.1. El choque fuerzas asimétricas

La compleja naturaleza del espacio cibernético provee a los participantes del ciberconflicto de capacidades variadas, por ello el margen de actuación se encuentra directamente relacionado con el dominio del conocimiento informático. Otra particularidad muy importante es el espacio físico desde cual se puede lanzar un ataque, pues al contrario de las operaciones convencionales militares un ataque cibernético puede lanzarse desde cualquier lugar en donde se ubique un ordenador. El principal elemento en este panorama es el dominio del conocimiento tecnológico que como ha sido analizado escapa fuera de la esfera militar, pues hoy en día actores no estatales poseen un alto potencial cibernético, dando lugar a lo que se conoce como el choque de fuerzas asimétricas.[173]

Debido a dichas habilidades actores estatales y no estatales son capaces de prevalecer a través del uso del ciberpoder en un escenario de conflicto pese a la superioridad en personal militar y en tecnología que pueda poseer el oponente.[174] En otras palabras, se trata de la ventaja otorgada por el empleo de la ciberguerra a actores débiles para actuar al mismo nivel (e incluso en uno superior) en el espacio virtual.

---

[172] *ibídem*, p.25.
[173] Phillips, Andrew. (Octubre 14, 2012). "The Asymmetric Nature of Cyber Warfare". *USNI News*. [En línea]. Disponible en: <https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare>.
[174] Sigholm, Johan. (2013). "Non-State Actors in Cyberspace Operations". *Journal of Military Studies*. no. 1, vol. 4, p. 24. [En línea]. Disponible en: <https://www.ida.liu.se/~johsi32/docs/JMS_4-1_Sigholm_Non-State_Actors_in_Cyber Ops.pdf>.

La asimetría también existe en el espacio tangible y se trata de las disparidades en poder militar que existe entre los participantes de una contienda. En la actualidad, un escenario de guerra asimétrica puede ser complementado con el ejercicio del ciberpoder. Sin embargo, en el campo de batalla la dimensión cinética continúa siendo dominante.[175]

En escenarios como en la Guerra Civil Siria la aparición de actores no estatales altera la naturaleza del conflicto, este fenómeno se traslada también al ciberespacio, pues Internet dota de amplios márgenes de acción a grupos terroristas y permite ocultar la fuente de un ataque asimétrico.[176]De acuerdo con Gabi Siboni (2015) el choque de estas fuerzas asimétricas se caracteriza por:

- La mayor vulnerabilidad por parte de los Estados a ser blancos de un ataque
- Las capacidades en el ciberespacio son cada vez más mayores y accesibles para actores no estatales
- La dificultad tanto táctica como tecnológica de los Estados para combatir las organizaciones no estatales a través de ataques cibernéticos.[177]

Desde esta perspectiva el éxito de una operación en el ciberespacio depende de factores como: las capacidades de inteligencia; el empleo de alta tecnología, y la capacidad operacional.[178]

A pesar de todo, la ciberguerra no ha desplazado el uso de la fuerza en los conflictos contemporáneos. Si bien, complementa las operaciones militares tradicionales su impacto aun es limitado, esto se debe a la ausencia, hasta el momento, de una operación militar que combine de forma efectiva el uso de los medios tradicionales e Internet en el marco de un conflicto bélico.[179] Por ello, en el ámbito de la defensa el objetivo principal es evitar la ejecución de ataques

[175] Siboni, Gabi. (Abril 29, 2015). "The Impact of Cyberspace on Asymmetric Conflict in The Middle East". *Georgetown Journal of International Affairs.* [En línea]. Disponible en: <http://journal.georgetown.edu/the-impact-of-cyberspace-on-asymmetric-conflict-in-the-middle-east/>.
[176] *Ídem*.
[177] *Ídem.*
[178] *ídem*
[179] *Ídem.*

convencionales en sincronía con ataques cibernéticos por parte de actores estatales, pero principalmente por parte de actores no estatales.

2.3.2. El surgimiento de ejércitos electrónicos

Los ejércitos electrónicos son un efecto visible de la militarización de la red. El primer ejército (también denominado cibermilicia) de esta naturaleza fue empleado en la guerrilla zapatista en México en el año de 1994.[180] Sin embargo, no se trata de conformaciones pertenecientes a la estructura militar estatal, las cibermilicias a menudo están conformadas por hackers que actúan a favor de una causa. Es así como las cibermilicias comienzan a formar parte de los conflictos bélicos internacionales, pues con el paso del tiempo los ejércitos electrónicos mejoraron su organización y efectividad. Progresivamente, la intervención de esta clase de actores en los conflictos internacionales fue en aumento, como muestra están los enfrentamientos en Pakistán, Serbia y China. El fenómeno de los ejércitos electrónicos consiste no sólo en el surgimiento de una nueva dimensión en la guerra moderna sino de una nueva manifestación de nacionalismo.[181]

Los casos de enfrentamientos con un componente electrónico son numerosos. Empero, en el ámbito militar los eventos más importantes son los ataques a Estonia y el ataque de Israel contra Siria (conocido como operación Orchard), ambas en 2007. Estos eventos son importantes porque el primero demostró la vulnerabilidad de la infraestructura crítica nacional, y el segundo representa una de las más efectivas operaciones militares en dónde se combinó un ataque cibernético y una operación militar convencional para la obtención de un objetivo[182]. (ver tabla 3)

TABLA 3 ALGUNOS CONFLICTOS CIBERNÉTICOS REGIONALES

Año	Conflicto
1998	Simpatizantes zapatistas vs México
	Simpatizantes zapatistas vs DOD, Bolsa de valores de Frankfurt
	Pakistán vs India (después de los ensayos nucleares)
1999	OTAN (Kosovo) vs serbios (y rusos)
	China vs Estados Unidos (bombardeo de la embajada china en Belgrado)

[180] Dudney, Robert S. (Febrero, 2011). "Rise of the Cyber Militias". *Air Force Magazine*, February 2011, p.88. [En línea]. Disponible en: <http://www.airforcemag.com/MagazineArchive/Documents/2011/February%202011/0211c yber.pdf>.
[181] *Íbidem*, p. 88.
[182] *Ídem.*

	China vs Taiwán
	India vs Pakistán (durante el conflicto en Cachemira)
	Hamas vs Israel
2000	Azerbaiyán y Turquía vs Armenia
	Hezbolá contra Israel
2001	China vs Estados Unidos (después de la caída de los aviones EP-3 de la armada de EE. UU)
2005	Indonesia vs Malasia (disputa sobre el Mar de Célebes)
	China y Corea del Sur vs Japón (disputa sobre los crímenes de guerra de Japón)
	Neonazis alemanes vs el mundo
2006	Miembros de la comunidad musulmana vs Dinamarca (durante el furor sobre la historieta de Muhammad)
2007	Rusia vs Estonia
	Israel vs. Siria (Operación Orchard - ataque aéreo de apoyo)
2008	Rusia vs Lituania
	Rusia vs Georgia (durante la invasión de las tropas rusas)
2009	Rusia vs Kazajstán (agencias de noticias)
	Corea del Norte vs Corea del Sur y Estados Unidos
	Rusia vs Kirguizistán
2010	Los opositores estadounidenses de WikiLeaks (y otros) vs los partidarios de WikiLeaks
2011	Origen desconocido vs Países de Europa del Este, ex miembros de la URSS, Asia central, América del Norte y Europa Occidental (virus "Octubre Rojo")
2012	El grupo de hackers "Cutting Swords of Justice" vs la compañía saudí Aramco
2013	Corea del Norte vs Corea del sur (afectó instituciones bancarias)
2017	Origen desconocido vs el mundo (Ataques ransomware WannaCry)

Fuente: Elaboración propia con datos de Dudney (2011); OTAN (2017); Chepkemoi (2017), y Avast (2017)

Igualmente han aparecido milicias cibernéticas en el marco de enfrentamientos bélicos como el caso del Ejército Electrónico Sirio, SEA (por sus siglas en inglés *Syrian Electronic Army*) que se presume tiene vínculos con el gobierno de Bashar Al-Assad. La milicia demuestra su nacionalismo en redes sociales y a través de ataques a medios de comunicación e infraestructura crítica de países rivales.[183]

Las capacidades de estos tipos de actores en el plano internacional aún están por descubrirse. Al respecto existen diversos análisis que sugieren que los ejércitos electrónicos son una nueva modalidad de empoderamiento de los ciudadanos; otros, señalan que es la forma en la que los Estados-nación aprovechan la anonimidad de Internet y la dificultad de atribución para financiar y emplear milicias cibernéticas en contra de países enemigos, pues de esta forma la responsabilidad por el uso de armamento cibernético no regulado por la comunidad internacional queda en mano de actores no estatales.

[183] Al-Rawi, Ahmed K. (2014). "Cyber warriors in the Middle East: The case of the Syrian Electronic Army". *Public Relations Review*, no. 40, pp. 420-428.

2.4. DESARROLLO Y APLICACIÓN DE ARMAMENTO CIBERNÉTICO

Hace algunos años Internet fue proclamada la herramienta más importante para cambiar el mundo,[184] esto teniendo en cuenta sus capacidades a favor de la libertad de expresión, movilización y acción social, y la difusión y defensa de los Derechos Humanos. Sin embargo, es difícil pensar que un espacio como este sea capaz de quedar fuera del alcance de acciones delictivas y ser utilizada también con fines manipulación y campañas de desinformación. La realidad es que actualmente Internet posee las mismas capacidades para ser utilizada tanto a favor de una demanda social como para lanzar un ataque informático en contra de infraestructura militar.[185]

Las estrategias de defensa en el plano internacional se enfrentan a una realidad en la que se crean más de nueve malware por segundo, la situación empeora porque se estima que hoy en día más cien países están desarrollando potencial cibernético-militar. Sin embargo, sólo veinte países cuentan con capacidades avanzadas.[186]

El desarrollo de armamento cibernético con fines ofensivos requiere del análisis de las vulnerabilidades de los sistemas informáticos a atacar, por lo que precisa de un amplio trabajo de inteligencia.[187]Entre las acciones que pueden ser consideradas agresiones en el ciberespacio se encuentran:

- Entrar en el disco duro de un ordenador sin consentimiento del titular
- Interceptar mensajes de correo electrónico
- Suplantar la personalidad en el correo electrónico

[184] Khanna, Ayesha y Parag Khanna. (Julio 12, 2012). "How Technology Promotes World Peace". *The Atlantic*. [En línea]. Disponible en: <http://www.theatlantic.com/international/archive/2012/06/how-technology-promotes-world-peace/258400/>.

[185] Dunn Cavelty, Myriam. (2012). "The Militarisation of Cyberspace: Why Less May Be Better". *NATO CCD COE Publications*. [En línea]. Disponible en: <https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf>.

[186] Singer, Peter W. (2015). "Ciberarmas y carreras de armamentos: un análisis". *La ciberguerra*. Vanguardia dossier, No. 54, pp. 42-47.

[187] Defense Science Board (DSB). (2012). *Task Force on Resilient Military Systems and the Advanced Cyber Threat*, pp. 49-50. [En línea]. Disponible en: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf>

- El Hostigamiento electrónico
- El uso indebido de directorios y listas de usuarios en la red
- La acumulación, registro y/o transferencia de datos sin consentimiento
- La alteración o destrucción de información
- El acceso a cuenta del administrador.[188]

Tales actividades son ejecutadas por el denominado armamento cibernético que consiste en malware de distintos tipos: *sniffer*, *trojan horses*, *worms*, *cookies*, virus, *logic bombs* etc., con los cuales es posible irrumpir, interceptar, modificar y fabricar elementos residentes en sistemas informáticos.[189] Este tipo de armamento representa un problema jurídico ya que desde el Derecho Internacional no existe un marco que tipifique y sancione su uso. (Ver anexo I Algunos tipos de armas cibernéticas)

En resumen, dentro de la esfera militar hoy como en el pasado los medios importan tanto como los fines. En la actualidad, los medios son los que están propiciando una trasformación de la actividad militar, realizar un juicio al respecto es difícil porque aún se desconocen las verdaderas capacidades del uso Internet y del armamento inteligente en un conflicto armado, al momento existen enfrentamientos que ayudan a evaluar en cierto grado su impacto en el plano de las relaciones internacionales, los estudios de seguridad y en el derecho internacional. No obstante, para las agencias de inteligencia y seguridad un futuro en donde se combinen ambos potenciales (Internet, las armas inteligentes y tácticas convencionales) continúa siendo una amenaza potencial, pues entonces se configuraría una guerra multiespectro.

[188] Fernández Rodríguez, José Julio. (2008). Derechos Fundamentales y construcción de la seguridad futura. En Fernández Rodríguez, José Julio; Javier Jordán Enamorado, y Daniel Sansó-Rubert. *Seguridad y defensa hoy: construyendo el futuro*. Madrid: Plaza y Valdés, p. 19.
[189] *Ídem.*

CAPÍTULO 3. LA REVOLUCIÓN TECNOLÓGICO INFORMACIONAL DE LOS ASUNTOS MILITARES Y LAS ARMAS CIBERNÉTICAS EN MEDIO ORIENTE

Medio Oriente es uno de los tópicos que genera más bibliografía en la disciplina de las Relaciones Internacionales, su importancia histórica, cultural, geográfica, política y económica es indudable. Medio Oriente es también una de las regiones que ha sido más azotada por el yugo de la guerra, los conflictos regionales, los que transcienden sus fronteras y los que generan un impacto en las dinámicas regionales han marcado el desarrollo histórico de la interacción internacional.

Por lo anterior, el propósito de este capítulo es analizar el influjo de las nuevas tecnologías, especialmente las bélicas, y el impacto que generan en la seguridad y defensa de la región. Para ello, se traslada el concepto de Revolución Tecnológico Informacional de los Asuntos Militares a escenarios como la Operación Tormenta del Desierto (1991), la invasión a Iraq (2003), la Operación Huerto, u Orchad, (2007, en Siria) y las actividades del autodenominado Estado Islámico en el marco de la Guerra civil siria (2011-2015).

3.1. MEDIO ORIENTE, ANÁLISIS DEL CONCEPTO

Es imposible continuar con este análisis sin definir primero qué es Medio Oriente. La delimitación del concepto ha sido objeto de numerosos estudios como: *The Middle East: A Brief History of the Last 2,000 Years* de Bernard Lewis; *The Shaping of the Modern Middle East* también de Bernard Lewis; *Orientalismo* de Edward Said; *A History of the Modern Middle East* de William L. Cleveland y Martin Bunton; *The Middle East in World Affairs* de George Lenczowski, entre muchos otros.

La definición de "Oriente" como algo ajeno y diferente a Europa data de la época de las cruzadas (entre los siglos XI y XIII), entonces oriente se vinculó con el islam y occidente con el cristianismo.[190]Así, la referencia a términos como "Oriente" y

[190] Özalp, Nuri Osman. (2011). "Where is the Middle East? The Definition and Classification Problem of the Middle East as a Regional Subsystem in International Relations*". TJP Turkish Journal of Politics* Vol. 2 No. 2 Winter 2011, p.5. [En línea]. Disponible en: <http://www.tau.edu.tr/img/files/where_is_the_middle_east2012_onozalp.pdf>

"Occidente" se convirtió más en una forma de pensamiento que una delimitación geográfica.[191]

De acuerdo con Edward Said, la idea de Oriente ha servido a Europa como un punto de referencia mediante el cual se construye a sí mismo en contraposición a lo que Oriente representa desde el punto de vista europeo. De esta forma, explica Said, Oriente es parte integrante de la civilización y de la cultura material europeas.[192] En adición, señala que el vínculo europeo-atlántico con Oriente consiste en una relación de poder y de complicada dominación del primero sobre el segundo, sostenido por una hegemonía cultural y representaciones que colocan a lo occidental como algo superior y lo oriental como el retroceso.[193]

El concepto ha evolucionado a través del tiempo respondiendo a los intereses de los actores interesados en la región. De este modo, Nuri Özalp (2011) describe el empleo de tres tipos de definiciones para referir a la zona geográfica: Oriente próximo, Oriente Medio y el Gran Medio Oriente, las cuales se tratan de perspectivas eurocéntricas, producto del imperialismo occidental del siglo XIX.[194]

Según Bernard Lewis (1968) el primer término para referir a la región fue "Cercano Oriente" que entonces englobaba el área de Europa sudoriental y los Balcanes, y fue empleado en 1890. Más adelante, en 1902, el Almirante Alfred Thayer Mahan se refirió a la zona como "Oriente Medio", de acuerdo con esta perspectiva su delimitación geográfica abarcaba desde el Suez hasta Singapur.[195]

No fue sino hasta la Primera Guerra Mundial, mediante el establecimiento de dos comandos militares británicos, que se establecieron dos espacios de operación, uno en el Golfo árabe pérsico denominado Medio Oriente, y el otro en la costa mediterránea, conocido como Cercano Oriente, a lo largo de este periodo uno y otro

[191] *Íbidem*, p.7
[192] Said, Edward. (2002). *Orientalismo*. Madrid: Debate, p. 20.
[193] *Íbidem*, pp. 25-29.
[194] Özalp, *Óp.cit.* p.7
[195] *Ídem.*

término comenzaron a emplearse sin distinción propiciando la confusión en la delimitación geográfica de dicha región.[196]

La definición oficial, en el plano geográfico, se alcanzó luego de grandes transformaciones en Europa producto de la Primera Guerra Mundial cuando la *Royal Geographical Society* la definió como una región desde el Bósforo hasta las fronteras occidentales de la India.[197]

Sin embargo, Medio Oriente engloba mucho más que sólo una delimitación geográfica, se trata de una noción con alcances históricos, culturales, políticos y económicos[198] y por lo tanto con un papel significativo en desarrollo las relaciones internacionales. Por ello, para los fines de la presente investigación se considera como Medio Oriente a la región conformada por Argelia, Túnez, Libia, Líbano, Israel, Egipto, Siria, los Territorios palestinos, Iraq, Turquía, Irán[199]y la península arábiga, es decir, Arabia Saudita, Kuwait, Bahréin, Qatar y los Emiratos Árabes Unidos, definición que corresponde a la proporcionada por el historiador Carl L. Brown en su obra *International Politics and the Middle East. Old Rules, Dangerous Game* (1984).

3.1.1 El rol de los asuntos militares en la región

Las cuestiones militares en el Medio Oriente no se limitan sólo a los siglos XX y XXI ni a la evolución de las denominadas nuevas tecnologías. El desarrollo e implementación de las prácticas belicistas datan de tiempos remotos, ya desde Imperio Otomano, especialmente durante el siglo XVI bajo la autoridad del sultán Suleimán El Magnífico, el imperio mantuvo supremacía militar y naval en el Mediterráneo[200], todo ello gracias a su gran estrategia belicista. Y es que la cuestión militar representa uno de los pilares de defensa más importantes en una nación, no

[196] Sierra Kobeh, María de Lourdes. (2002). *Introducción al Estudio de Medio Oriente. Del surgimiento del Islam a la repartición imperialista de la zona.* México: Universidad Nacional Autónoma de México, p. 13.
[197] Özalp, *Óp.cit.* p.7
[198] *íbidem*
[199] Irán e Israel no figuran en la definición proporcionada por Carl L. Brown. Sin embargo, dada su importancia en la seguridad de la región se toman en cuenta en el desarrollo de la presente investigación.
[200] Sierra Kobeh, *Óp.cit*. p.98

en vano fue el expansionismo militar otomano el que, de acuerdo con diversos especialistas, representó una de las bases de su esplendor.[201]

Con el paso del tiempo, la injerencia económica europea y el expansionismo tanto europeo como ruso durante el siglo XIX se produciría el debilitamiento y fin del orden otomano. El quebrantamiento de la autoridad del Imperio en todos sus dominios dio paso a la intervención de potencias europeas en búsqueda del establecimiento de zonas de influencia. De esta manera, poco a poco, cayeron bajo dominio extranjero zonas como el Golfo Pérsico, Egipto, Argelia, Túnez, Marruecos, Líbano, Siria, etc. convirtiéndose en una especie de tablero en donde actores como el imperio británico, la Rusia zarista y Francia movieron sus tropas, estableciendo su control en una especie de juego por obtener el balance de poder en la región.[202]

En adelante, tras la Primera Guerra Mundial, la imposición de un orden que sólo respondió a los intereses de quienes ocupaban y no de quienes pertenecían a la región se convirtió en el origen de múltiples enfrentamientos en dónde en las causas, en el desarrollo e incluso en las negociaciones de paz la participación de Estados extra-regionales siempre estará presente.

Medio Oriente es un encuentro de culturas, religiones y grupos étnicos de valiosa herencia histórica, en la región concurren árabes, judíos, kurdos, persas, turcos, entre otros. Es hogar de las tres religiones abrahámicas: el judaísmo, el cristianismo y el islam, además de otras menores en número, pero no menos importantes como las comunidades bahá'ís, drusas, yazidíes y zoroastrianas.[203] Por desgracia, Medio Oriente no ha estado libre de conflicto, los intereses que Europa, Rusia y más adelante Estados Unidos, entre otros actores, preservan en la región es fuente y combustible para sostenimiento de cruentos enfrentamientos. Aunado a ello, las fricciones regionales por el choque de intereses y la búsqueda por obtener la hegemonía regional prolongan la inestabilidad en la zona. Esto ha llevado a que tanto países como actores no estatales con capacidades económicas en la región

[201] *Ídem.*
[202] *Íbidem,* pp. 97-108
[203] The Heritage Foundation. (2017). *Middle East*. 2017 Index of U.S. Military Strength. [En línea]. Disponible en: <http://inde x.heritage.org/military/2017/assessments/operating-environment/middle-east/>

enfoquen sus esfuerzos en el desarrollo y adquisición de tecnología militar, así como en su posterior incorporación en las estrategias militares. Tan sólo 2015 Arabia Saudita figuró como uno lo de los países con mayor inversión en gasto militar con una cifra de 87.2 mil millones de dólares, el incremento más significativo lo experimentó Iraq que de 2006 a 2015 aumentó el gasto cerca del 500%, mientras que el mejor ejército en la región pertenece a Israel.[204]

En el caso de Israel, las autoridades encargadas de la seguridad y defensa han enfocado su trabajo en mantener la superioridad de las defensas antimisiles, la recolección de inteligencia, las armas de precisión y la tecnología cibernética. A comienzos de 2016 las Fuerzas de Defensa de Israel (FID) dieron a conocer un plan de 5 años con un valor de 78.6 mil millones de dólares para mejorar el potencial cibernético de combate a fin de mejorar las capacidades de las FID para actuar en múltiples teatros.[205]

Después de Israel, las fuerzas armadas más tecnológicamente avanzadas y mejor equipadas pertenecen al Consejo de Cooperación del Golfo (CCG), el cual cuenta con equipo altamente sofisticado de origen británico, estadounidense y francés, la mayoría de los miembros del CCG han optado por desarrollar su capacidad aérea.[206]

Todo esto, dentro de un marco histórico en donde las dinámicas regionales se han visto influenciadas por un orden regional fragmentado. Desde las proposiciones nacionalistas de Nasser confrontadas al orden monárquico defendido por Arabia Saudita, hasta los diversos posicionamientos alrededor de los Acuerdos de Camp David (de 1978) han tenido un impacto en la estabilidad regional. Del mismo modo, no hay que olvidar las reacciones generadas tras la Guerra Iraq-Irán (1980-1988), y la posterior invasión a Kuwait (1990-1991). En adición, y de acuerdo con Anoushiravan Ehteshami (2014), la orientación de Siria hacia Irán luego de dicho

[204] *Ídem.*
[205] *Ídem*
[206] *Ídem*

enfrentamiento dividió eficazmente el orden árabe en una estructura multicéntrica carente de núcleo y cada vez más subregionalmente enfocada.[207]

En este escenario las cuestiones de seguridad y defensa representan un elemento bajo constante actualización. Así, la búsqueda por liderazgo militar se convierte en pieza clave para aquellos países que desean resguardar su integridad territorial en el marco de la legitima defensa, pero también para aquellos que buscan imponer sus intereses y el establecimiento de un juego de acuerdo a las normas que le favorezcan, esto claro con el apoyo tanto como económico como militar de países más allá de la región.

3.1.2 Transformaciones en las nociones de seguridad y defensa tras el 9/11

Los acontecimientos del 11 septiembre de 2001 en Estados Unidos significaron una transformación en el orden internacional del siglo XXI, más allá de continuar tomando a Occidente como punto de partida para la explicación de la historia y del acaecer internacional es innegable que el ataque a las Torres Gemelas transformó los paradigmas de seguridad de Estados Unidos y del resto del mundo, cambió las prioridades de defensa y seguridad tanto en América, como en Europa y en Medio Oriente, y dio paso a un discurso en dónde los esfuerzos de seguridad, la articulación de estrategias y el desarrollo de armamento se dirigieron a combatir lo que, en ese entonces, se identificó como la mayor amenaza al orden mundial: el terrorismo yihadista.

Hasta el 11 de septiembre las cuestiones que ocupaban los asuntos de seguridad en Medio Oriente eran: 1) el conflicto israelí-palestino, 2) los enfrentamientos en torno a cuestiones territoriales entre Iraq-Kuwait; Marruecos-Argelia, y Sudán-Egipto, y 3) el apoyo al terrorismo y la imposición de embargos en Libia y Sudán, y la violencia islamista en Argelia.[208]

---

[207] Ehteshami, Anoushiravan. (2014). "Middle East Middle Powers: Regional Role, International Impact". *Uluslararası İlişkiler Dergisi*, Volume 11, No. 42 p. 32. [En línea]. Disponible en: <http://www.uidergisi.com.tr/wp-content/uploads/2016/06/42_1.pdf>

[208] Rakkah, Azzedine. (2005). "El mundo árabe después del 11 de septiembre". *OASIS*, núm. 10, p. 55 [En línea]. Disponible en: <http://www.redalyc.org/pdf/531/53101004.pdf>.

A partir 9/11 los países que conforman la región experimentaron la materialización de la amenaza a su seguridad en forma de: 1) intervenciones uni y multilaterales en nombre de la seguridad mundial y de una democratización forzada; 2) el surgimiento y fortalecimiento de organizaciones terroristas que, poco a poco, se apoderaron de importantes áreas territoriales, y 3) la posibilidad de la desintegración territorial.[209]

El 11 de septiembre también significó una transformación en la industria de la seguridad, a partir del ataque que vulneró la seguridad del país más poderoso del mundo, grandes flujos de capital comenzaron a dirigirse hacia las Empresas Militares Privadas (EMP) y a la par la tecnología *drone* comenzó a ser empleada en escenarios de combate. Por primera vez, desde el término de la Guerra Fría el capital comenzó a orientarse nuevamente hacia grandes contratistas como Boeing Co., Lockheed Martin Corp. y Northrop Grumman Corp.[210]

El gasto en defensa por parte de Estados Unidos se elevó beneficiando a la industria militar e impulsando la proliferación de armamento altamente tecnológico, como es el caso de la contratista General Atomics encargada del desarrollo de Vehículos Aéreos No Tripulados.[211] No obstante, el incremento en el gasto no sólo involucra a Estados Unidos, sino también a otros actores como Rusia, diversos países de Europa y del Medio Oriente (ver gráfica 1). La razón por la que en la gráfica el porcentaje del gasto militar respecto al Producto Interno Bruto (PIB) es más elevado en el caso del "mundo árabe" se debe al gasto militar de países como Omán y Arabia Saudita, en adición bajo el término "mundo árabe" los cálculos del Banco mundial incluyen también a Sudán del Sur.[212]

---

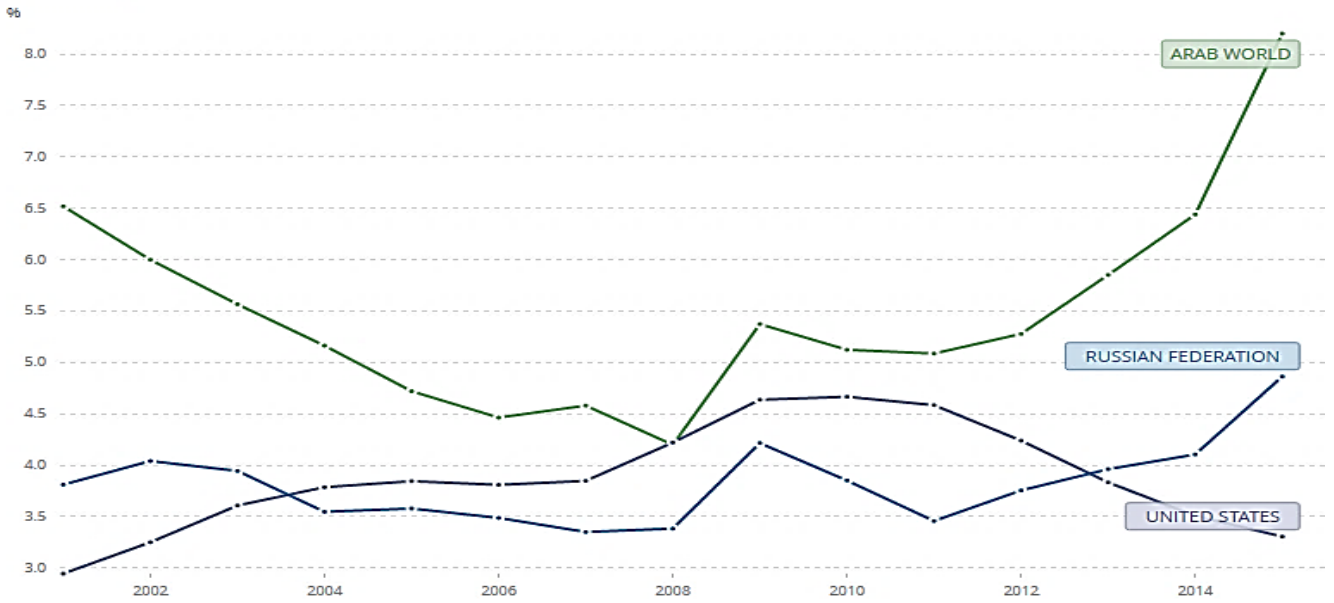
[209] *Íbidem*, p.56

[210] Hennigan, W.J. (Septiembre 9, 2011). "Small military contractors flourished after 9/11 attacks". *Los Angeles Times*. [En línea]. Disponible en: <http://articles.latimes.com/2011/sep/09/business/la-fi-911-aerospace-20110910>.

[211] *Ídem.*

[212] The World Bank Group. (Abril 24, 2017). "Military expenditure (% of GDP)". [En línea]. Disponible en: <http://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?contextual=max&end=2015&locations=RU-1A-US&start=2001&view=chart>.

GRÁFICA 1 GASTO MILITAR EN PORCENTAJE DEL PRODUCTO INTERNO BRUTO, 2001-2005, CORRESPONDIENTES AL MUNDO ÁRABE, ESTADOS UNIDOS Y RUSIA



Fuente: The World Bank Group. (Abril 24, 2017). "Military expenditure (% of GDP)". [En línea]. Disponible en: <http://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?contextual=max&end=2015&locations=RU-1A-US&start=2001&view=chart>.

Las consecuencias del 11 de septiembre en Medio Oriente son difíciles de calcular, dio paso a una transformación en los paradigmas de seguridad regionales e internacionales. Nuevas amenazas resultaron del ataque al World Trade Center y de la posterior guerra contra el terrorismo que transformó el mapa geoestratégico de la región. Desde Libia a Afganistán, se experimentaron los efectos de los nuevos imperativos de seguridad estadounidenses en una zona donde residen un cuarto de los fosfatos mundiales y las mayores reservas de petróleo en el mundo.[213]

3.2. ANTECEDENTES HISTÓRICOS DE LA REVOLUCIÓN TECNOLÓGICO INFORMACIONAL DE LOS ASUNTOS MILITARES

Una vez presentado un panorama histórico y estratégico de la región es posible emprender el análisis de las implicaciones de Revolución Tecnológico-Informacional de los Asuntos Militares (IT-RMA, por sus siglas en inglés) en Medio Oriente. Dado la amplitud del término, que engloba tanto armamento como estrategias militares empleadas en una extensa área geográfica, se toman en cuenta sólo aquellos casos en lo que sofisticación tecnológica representó un rasgo determinante en el combate. En adición, la presente investigación se desarrolla tomando como referencia tres

[213] Sierra Kobeth, *Óp. Cit.,* p. 19.

proposiciones fundamentales de la evolución tecnológica de la práctica belicista, estos son:

- La reducción del espacio y tiempo empleado en ejecutar tales operaciones
- La disminución en el número de bajas en las fuerzas armadas
- La reducción de daños colaterales.

La propia evolución del término IT-RMA está intrínsecamente ligado al pensamiento militar de tres importantes potencias en la región: Estados Unidos, la entonces Unión de Repúblicas Soviéticas Socialistas (URSS) e Israel.[214] De acuerdo con Dima Adamsky y Kjell Inge Bjerga (2010) IR-TMA emergió en el contexto de la Guerra Fría y su desarrollo fue posible gracias a la tecnología desarrollada en "tiempos de paz"[215]. En adición, señalan Adamsky y Inge Bjerga, los efectos de esta transformación pueden ser observados y analizados de forma notable en escenarios como Medio Oriente.[216]

Con base a esto, se parte del análisis de la estrategia militar enmarcada en la Guerra del Golfo (1980-1988) y la posterior anexión de Kuwait por parte de Iraq, dado que la operación Tormenta del Desierto (1991) representó el modelo mediante el cual posteriormente partieron múltiples análisis enfocados a evaluar los alcances de las llamadas "las guerras del futuro".

3.1.1. La tecnología militar en la Guerra del golfo

La influencia de la Guerra del Golfo en la doctrina militar moderna es significativa, pues es frecuentemente empleada para ilustrar la transformación en los paradigmas de seguridad occidentales en donde el uso de armas altamente tecnológicas es capaz de alcanzar en menor tiempo los objetivos de una misión, reduciendo tanto

[214] Adamsky, Dima y Kjell Inge Bjerga. (Agosto, 2010). "Introduction to the Information-Technology Revolution in Military Affairs". *The Journal of Strategic Studies*, Vol. 33, No. 4, pp. 463–468. [En línea]. Disponible en: <htt p://dx.doi.org/10.1080/ 01402390.2010.489700>.

[215] "Tiempos de paz" en forma nominal ya que como Alvin y Heidi Toffler (1994) refieren tras el término de la Segunda Guerra Mundial el mundo experimentó más de 150 y 160 contiendas armadas y conflictos civiles, por lo que de 1945 a 1990 el mundo libró casi el equivalente a la Primera Guerra Mundial en términos de civiles y soldados asesinados. Fuente: Toffler (1994:29-30).

[216] Dima y Bjerga, *Óp. Cit.*

el número de bajas en el ejército como los daños colaterales. Sin embargo, esta última proposición será analizada a lo largo de este capítulo pues mientras que se ha logrado acortar dimensiones como la distancia y el tiempo en lo que respecta a la disminución del daño colateral existe mucho que examinar.

Para abordar las causas y consecuencias de la Guerra del Golfo es necesario ir más allá del contexto y rescatar la historia de Iraq como nación, para lo cual es preciso remontarse a los Acuerdos Sykes Picot de 1916[217]firmados por Gran Bretaña y Francia que en el contexto de la Primera Guerra Mundial determinaron la repartición de los territorios que aún conformaban el decadente Imperio Otomano.[218]

De esta forma, Medio Oriente fue repartido por las potencias europeas en su afán de preservar sus respectivas esferas de influencia en una región de vital importancia geopolítica y energética, tras dichos acuerdos el panorama se estructuró de la siguiente forma: los territorios de Líbano y Siria quedaron bajo dominio francés mientras que Palestina, Transjordania e Iraq pertenecieron al mandato británico,[219]dando paso así a la fabricación del mapa de Medio Oriente y al establecimiento e imposición de Estados-nación que más a delante serán fuente de inestabilidad regional.

Tras la Conferencia de San Remo (del 19 al 26 de abril de 1920) y ya bajo mandato británico fue instaurada una monarquía en territorio iraquí. De esta forma, llegó al poder en 1923 el Rey Faysal I de la dinastía de los hachemíes, quien dirigió una monarquía hereditaria de tipo constitucional parlamentario. Más adelante en 1930, intentando lidiar con el sentimiento antibritánico en Iraq, Gran Bretaña concedió la independencia, la cual fue firmada por el Primer Ministro iraquí Nuri al-Said.[220]No obstante, la monarquía permaneció en el poder hasta 14 de julio de 1958, cuando la revolución, ya incontenible, estalló por enfrentamientos entre los

[217] Aunque desde 1914 Gran Bretaña invadió las provincias otomanas de Mosul, Bagdad y Basora (hoy Iraq) en el marco de la Primera Guerra Mundial. Fuente: Martín Muñoz (2003)
[218] García Sánchez, Pablo. (2016). "La Guerra del Golfo Operaciones Desert Shield y Desert Storm". *Grupo de Estudios de Historia Militar*. [En línea]. Disponible: <http://www.gehm.es/biblio/La_Guerra_del_Golfo_GEHM.pdf.pdf>.
[219] Özalp, *Op. Cit.*
[220] Martín Muñoz, Gema. (2003). *Iraq. Un fracaso de Occidente (1920-2003)* Tusquest Edits: Barcelona. p. 27.

movimientos panarabistas y socialistas, lo cual derivó en el derrocamiento del rey y en la proclamación de la República de Iraq a manos de Abdul Karim Qasim.[221]

Al igual que el modelo egipcio, el golpe de estado llevó al poder a la elite militar, que tras la ejecución del Rey Faysan II y de Nuri al-Said, llevó Karim Qasim al mando de la recién formada república.[222] Inmediatamente después de la creación del nuevo orden Qasim se apresuró a establecer lazos con la entonces Unión de Repúblicas Socialistas Soviéticas (URSS). De 1961 a 1963 el gobierno de Qasim experimentó una serie de revueltas que derivaron en un nuevo golpe de estado impulsado por el Partido Ba'ath, estas revueltas culminaron en la ejecución de Abdul Karim Qasim.[223]

En 1963 los simpatizantes de Ba'ath, con ayuda de Egipto y de la CIA (Agencia Central de Inteligencia de Estados Unidos) ejecutaron un golpe estado que dio como resultado la ejecución de Karim Qasim el 9 de febrero de ese mismo año.[224] Posteriormente, al frente de la república se posicionó Abdul Rahman Arif quien se enfrentó a una creciente influencia del partido Ba'ath que sólo pudo contrarrestar apoyándose en la facción naserista.[225]Sin embargo, el Partido Ba'ath persistió en sus intentos de alcanzar el poder hasta que 17 de julio de 1968, cuando tras un nuevo golpe de estado consiguió el liderazgo político. Es en este momento cuando Ahmed Hassan Al-Bakr fue nombrado presidente, mientras que el cargo de vicepresidente fue ocupado por Sadam Hussein, quien también se encargó de los Servicios de Seguridad e Inteligencia. Durante la década de los 70 y con Ba'ath en el mando la república, Iraq experimentó importantes cambios: la nacionalización del *Petroleum Company*, reformas agrarias y un fuerte desarrollo económico producto de la adopción de tecnología occidental.[226]

[221] García Sánchez, *Op. Cit.*
[222] Martín Muñoz, *Op. Cit.*, pp. 31-37
[223] *íbidem*
[224] García Sánchez, *Op. Cit.*, p. 34
[225] *Ídem*
[226] *Íbidem,* p. 37

El 1 de junio de 1979 Sadam Hussein ocupó el liderazgo de la República de Iraq[227], posicionándose también al frente del partido Ba'ath. Con la Revolución Islámica de Irán liderada por Ruhallah Jomeini las fricciones entre Iraq e Irán se agudizaron, primero por el enfrentamiento iraní contra el régimen "impío" socialista del Ba'ath y después por el posible llamado a la población chiita para que se levantara en armas en contra de Sadam, esto en el contexto de una histórica represión del régimen baazista a cualquier forma de oposición.[228]

El segundo punto de fricción lo constituyó el acuerdo firmado con Irán sobre la región Shatt al- Arab, una región en la que confluyen el Tigris y el Éufrates a lo largo de 200 kilómetros. El enfrentamiento que se remonta a la época de Persia y Mesopotamia fue resuelto de forma temporal mediante el Acuerdo de Argel de 1975. No obstante, en septiembre de1980 Hussein denunció el acuerdo y empleó sus tropas contra Irán.[229]

Durante el desarrollo del enfrentamiento los iraquíes tuvieron éxito en la ofensiva, pues lograron adentrarse en territorio iraní, pero en verano de 1982 el ejército iraní consiguió que las tropas enemigas retrocedieran fuera de sus dominios. Iraq había iniciado la guerra confiado en el apoyo internacional de Estados Unidos y Europa quienes deseaban asegurar su abastecimiento petrolífero en la región, mientras que Irán también tomó ventaja del contexto proporcionado por el enfrentamiento para implementar medidas internas que asegurarían la prevalencia de su naciente orden.[230]

El enfrentamiento que se extendió hasta agosto de 1988 tuvo un alto costo humano, económico y moral para ambos países, se estima que 53 Estados vendieron equipamiento a los dos beligerantes por un valor de 50 000 millones de dólares. Los principales proveedores de Bagdad fueron la URSS y Francia, además de EE. UU, Gran Bretaña, Austria, Bélgica, Brasil, Chile, España, Hungría, Italia, Marruecos, Polonia, Portugal, República Federal Alemana, República Democrática

[227] García Sánchez, *Op. Cit*
[228] Martín Muñoz, *Op. Cit*, pp. 104-105
[229] *Íbidem,* p. 106
[230] *Íbidem,* p. 108.

Alemana, Suiza Checoslovaquia y Yugoslavia. Mientras que Irán recibió apoyo militar de China, Corea del Norte y del Sur, Gran Bretaña, Argelia, Argentina, Brasil, Chile, Libia, Siria, Taiwán y Vietnam.[231]

Se estableció entonces un juego peligroso en donde el mantenimiento del conflicto generaba enormes beneficios a la industria armamentista. Así, por ejemplo, al mismo tiempo en el que vendió armas a Iraq, la URSS también permitió la llegada de equipo militar a Irán a través de Libia. Asimismo, fue también durante esta época que Sadam Hussein logró obtener equipo militar moderno gracias a las ventas de Reino Unido y Francia.[232]

El conflicto finalizó hasta 1988 cuando, luego del atentado en contra de un Airbus civil, Irán decidió aceptar las condiciones establecidas en la resolución 598 del Consejo de Seguridad de Naciones Unidas.[233]

Durante el enfrentamiento también se emplearon armas químicas en contra de población kurda y las fuerzas armadas iraníes por orden de Sadam Hussein, lo cual derivará en posteriores resoluciones del Consejo de Seguridad de Naciones Unidas en contra del régimen de Saddam.[234]

El costo humanitario y moral del enfrentamiento agravó aún más la decadente situación iraquí a la que se sumó una crisis económica. Iraq salió del enfrentamiento con una deuda de 80 000 millones de dólares, los gastos para reconstrucción rondaban los 30 000 millones de dólares y la destrucción ocasionada por el conflicto de casi una década equivalía a 70 000 millones de dólares[235]. Ante esta situación, Hussein estructuró un plan de invasión a Kuwait basado en cuatro argumentos:

1) Producción excesiva de petróleo
2) Negativa de aplazamiento de la deuda de guerra

[231] Íbidem, p. 114
[232] *ídem*
[233] Íbidem, p. 119
[234] *ídem*
[235] Martín Muñoz, *Op. Cit,* p. 120

3) Bombeos ilegales de petróleo desde 1980, en los pozos compartidos de Rumayla por lo que exigía una compensación

4) Discordia entorno a las Islas Warbah-Bubiyán [236]

El 15 de julio de 1990 Hussein movilizó sus tropas a la frontera sur de la provincia de Basora y el 2 de agosto lanzó una ofensiva conformada por 100 000 hombres y 2 000 blindados que entraron a Kuwait, la operación se apoderó de casi todo el territorio y obligó a la familia real a huir a Arabia Saudita.[237] Ante el acontecimiento el 2 de agosto de 1990 el Consejo de Seguridad de la Organización de Naciones Unidas emitió la resolución 660 en dónde condenó la invasión y demandó la retirada de tropas iraquíes de suelo kuwaití. Cuatro días más tarde con la resolución 661 el Consejo estableció el embargo económico contra Iraq que más adelante sirvió como instrumento para negociar la destrucción de armas químicas en manos de Hussein.[238]

Las acciones de Iraq hacia Kuwait encendieron inmediatamente las alarmas para gobierno saudí y para sus aliados en Norteamérica y Europa, por lo que pocos días más tarde se ejecutó la Operación Escudo del Desierto cuyo objetivo fue disuadir a Iraq de continuar su avance a través de Arabia Saudita hacia los Emiratos Árabes Unidos. De esta forma, por medio de los servicios de inteligencia estadounidenses, el gobierno saudí descubrió la posibilidad de que las tropas invasoras de dirigiesen también hacia su territorio por lo que autorizó el despliegue de fuerzas de Estados Unidos en sus dominios. En este sentido, la implementación de la Operación Escudo del Desierto fue un éxito pues logró impedir el avance de tropas iraquíes, el poder disuasorio de la presencia de la 82ª división aseguró la contención de las fuerzas invasoras.[239]

[236] García Sánchez, *Op. Cit.* pp.6-7
[237] *Ibídem*
[238] Asamblea General de Naciones Unidas. (Agosto 2, 1990). Resolución 660 La situación entre Iraq y Kuwait. Consejo de Seguridad de la Organización de Naciones Unidas. [En línea]. Disponible en: <http://www.un.org/es/comun/docs/?symbol= S/RES/660%20(1990)>
[239] Bardají, Rafael L. (1991). "Operaciones En El Golfo: Escudo Del Desierto, Un Análisis Provisional." *Política Exterior*, vol. 5, no. 19. pp.85.87. [En línea]. Disponible en: <www.jstor.org/stable/20643059>.

Durante la Operación Escudo del Desierto se planeó movilizar durante la primera fase a 150 000 soldados, las fuerzas continuarían llegando, entre marines, comandos terrestres y aéreos se alcanzaría la cifra de 230 000 hombres, más 60 000 en los buques. En cuanto al armamento utilizado este corresponde a carros de combate M60 y M1 Abrams, entre otros (ver tabla 4). Con el transcurso del tiempo la presencia militar estadounidense fue en aumento hasta alcanzar 400 000 el número de soldados en Arabia Saudita.[240]

Los recursos económicos que fueron empleados en esta operación rondan los mil millones de dólares por mes de despliegue. No obstante, la operación también reflejó la debilidad económica y logística estadounidense, ya que ante los costos debió solicitar apoyo a otros países en la región para poder mantener las operaciones además de las dificultades de trasladar tanto soldados como armamento hasta golfo.[241]

TABLA 4 VEHÍCULOS Y ARMAMENTO MILITAR EMPLEADOS EN LA OPERACIÓN ESCUDO DEL DESIERTO

DENOMINACIÓN	MODALIDAD	DESCRIPCIÓN	PRODUCTOR
Tanque M60	Tierra	Desde la versión inicial del M60, el vehículo estaba dotado de un sistema ABQ y soportes para la posible instalación de una hoja empujadora. Como equipo normalizado posee luces infrarrojas de conducción y un proyector de luz compuesta sobre el cañón principal. (Mundo Militar: *s.f.*)	General Dynamics
M1 Abrams	Tierra	Cuenta con una pistola M68E1 de 105 milímetros, apareció en agosto de 1985, posee una estación de comando de defensa anti aérea. Las actualizaciones M-1A1, incluyen mayor blindaje y un sistema de protección contra armas nucleares biológicas y químicas. Pesa 63 toneladas y puede alcanzar una velocidad de 45 millas por hora. (Frontline: *s.f.*)	General Dynamics
C 141	Aire (Transporte de tropas y armamento)	Se trata de avión estratégico de transporte militar, introducido para reemplazar modelos más lentos como C-124 Globemaster II, el C-141, es capaz de trasportar vehículos con ruedas, así como 205 pasajeros, o 168 paracaidistas totalmente equipados. Airplanes Of The Past. (*s.f.*).	Lockheed Corporation
C5 Galaxy	Aire (Transporte de	Avión de transporte militar aeronave equipada con cuatro motores turbofan TF39-GE con una	Lockheed Corporation

[240] *Ibídem,* pp. 87 y 88
[241] *Ibídem.,* p.90

	tropas y armamento)	alta relación de derivación. Airplanes Of The Past. (*s.f.*).	

Fuente: Elaboración propia

Por su parte, y tras la anexión oficial de Kuwait (el 8 agosto de 1990) por parte de Iraq, una nueva resolución fue emitida el 29 de noviembre de mismo año por parte del Consejo de Seguridad de Naciones Unidas, esta vez con un carácter más determinante, se trata de la resolución 678, en donde:

> (la ONU) … *Autoriza a los Estados Miembros que cooperan con el gobierno de Kuwait para que, al menos que el Iraq* [sic] *cumpla plenamente para el 15 de Enero de 1991 o antes las resoluciones que anteceden* […] *utilicen todos los medios necesarios para hacer valer y llevar a la práctica la resolución 660 (1990) y todas las resoluciones pertinentes aprobadas ulteriormente y para establecer la paz y seguridad internacionales en la región.*[242]

La coalición internacional conformada por fuerzas armadas de 34 países y liderada por Estados Unidos estructuró la Operación Tormenta del Desierto, cabe destacar que entre sus miembros se encontraban países árabes como Egipto, Siria y Marruecos.[243]

La Operación Tormenta del Desierto, que dio inicio el 17 de enero de 1991 estuvo conformada por cuatro fases:

1) El bombardeo estratégico contra objetivos prioritarios
2) La obtención de superioridad aérea
3) El bombardeo a posiciones iraquíes
4) El empleo de la batalla terrestre y total destrucción de las divisiones de la Guardia Republicana.[244]

Durante el enfrentamiento las fuerzas de la coalición atacaron el Sistema de Integración de Defensa Iraquí (IADS, por sus siglas en inglés), el cual se derrumbó en sólo unas horas y no logró recuperar su funcionalidad, esto en el marco de la

[242] Asamblea General de Naciones Unidas. (Noviembre 29, 1990). Resolución 678 (1990). Consejo de Seguridad de la Organización de Naciones Unidas. [En línea]. Disponible en: <http://www.cinu.org.mx/temas/iraq/doctos/678.pdf>.
[243] García Sánchez, *Op. Cit, p*. 9
[244] *Íbidem*, p. 10.

supresión de las fuerzas armadas enemigas que formó parte de la segunda etapa de la operación. Los IADS iraquíes consistían en sistemas de radares de adquisición y búsqueda de tecnología europea y soviética, además estaba compuesta por una gama de sistemas SAM y AAA todos ligados a una red de comando, control y comunicaciones Kari C3 de origen francés.[245] (Ver tablas 5 y 6)

En respuesta Sadam Hussein lanzó una campaña en contra de Israel y Arabia Saudita. Sin embargo, las operaciones aéreas de la Coalición tuvieron éxito y el 24 de febrero dieron inicio las campañas terrestres, sólo cuatro días más tarde comenzaron las negociaciones de paz. Acto seguido, el Consejo de Seguridad emitió las resoluciones 686, para establecer las condiciones de suspensión de acciones militares, y 687 que contienen: 1) las restricciones hacia Iraq respecto al establecimiento de una zona de seguridad desmilitarizada bajo control internacional en territorio iraquí y kuwaití; 2) la rectificación, por parte de Iraq, de las convenciones y protocolos sobre el uso de armas no convencionales, y 3) la supervisión internacional y la destrucción de estas armas.[246]

[245] Kopp, Carlo. (2005). "Operation Desert Storm The Electronic Battle". *Air Power Australia*. [En línea]. Disponible: <http://w ww.ausairpower.net/Analysis-ODS-EW.html>.
[246] *Íbidem*, pp. 10-12

TABLA 5 ARMAMENTO EMPLEADO EN LA OPERACIÓN TORMENTA DEL DESIERTO (IRAQ)

PARTE DEL ARMAMENTO IRAQUÍ			
DENOMINACIÓN	MODALIDAD	ORIGEN	DESCRIPCIÓN
P15 Flat Face	Espacio-Satelital	Soviético/Almaz-Antey-Zavod imeni Likhachova	Su objetivo es la vigilancia y adquisición de objetivos, consiste en un sistema de radar de alerta temprana capaz de detectar objetivos ubicados a una distancia de hasta 250 kilómetros y a una mínima altitud de 300 metros. (Toperczer: 2012)
Mikoyan-Gurevich MiG-23	Aire	Soviético/Mikoyán	Se trata de un avión caza, cuenta con un poderoso radar, un sistema de búsqueda infrarrojo y con armas guiadas con infrarrojo. Fue diseñada entre 1964-66, como sucesora del MiG-21. (Aftergood: 2010a)
Sukhoi Su-17 (20 y 22)	Aire	Soviético/ Opitnoye Konstructorskoye Biuro-Sukhoi Corporation	Es un cazabombardero derivado del Su-7. Las primeros Su-17 fabricados para su evaluación aparecieron en 1969, la aeronave cuenta con un sistema de control de vuelo SAU-2. (Goebel: 2016).
BMD-1	Tierra-Aire	Soviético/Volgograd Tractor Plant	Vehículo anfibio de combate aéreo, comenzó a desarrollarse en 1965 y entró en servicio 1969. El BMD-1 está ligeramente blindado y tiene un casco de armadura de aluminio soldado. (Genys:2017)
SA-6 Gainful/2K12 Kub	Tierra-Aire	Soviético/ NIIP-Vympel y MMZ	También conocido como 2K12 Kub, su objetivo es destruir aeronaves a velocidades de entre 420 m/s y 600 m/s a altitudes de entre 100-200 metros. Posee un buscador de misiles semi-activo de onda continua (CW, *Continuous Wave*) y un sistema de radar de acoplamiento 1S91. (Kopp: 2012)
SS1 (SCUD)	Tierra-Aire	Soviético/ Opitnoye Konstructorskoye Biuro-RKK Energiya	Se trata de mísiles balísticos tácticos, emplean un giroscopio con el fin de proveer un rudimentario sistema de orientación. Los comandos de orientación se usan sólo durante el vuelo propulsado y los misiles pierden guía una vez que el cohete se queda sin combustible (aprox., después de 80 segundos). (Phillips: 2017)
Aérospatiale SA-316B Alouette III	Aire	Francés/Aerospatiale (hoy Eurocopter)	Es un helicóptero multi-rol de transporte ligero, está diseñado tanto para ejecutar operaciones militares como civiles incluso en las peores condiciones climáticas. Puede transportar 750 kg de carga durante las misiones de rescate en aire o mar, más 175 kg de carga útil adicional. (Kable:2017b)
S-75 Dvina	Tierra-aire	Soviético/ A.A. Raspletin-P.D.Grushin	El un sistema de misiles tierra-aire (SAM) de baja altitud guiadas por comando. Fue empleado por primera vez en 1957, es el misil de defensa aérea más empleado en la historia. Fue diseñado tanto para la defensa de objetivos fijos como para las fuerzas de campo. (Servaes: 2011)
Type 63 multiple rocket launcher	Tierra-aire	China/China state Factory 847	Es un lanzador múltiple de cohetes, dispara cohetes de 107 mm, con un rango máximo de alcance de 8 kilómetros. (Bassiouni: 2013) Su diseño consiste en 12 tubos dispuestos en 4 líneas, pesa 18.84 kg y tiene un alcance de 8 500 metros y un diámetro de 107 mm. (Sherman:1999)
2S3 Akatsiya	Tierra-aire	Soviético/ Uraltransmash	Se trata de un obús autopropulsado de 152-mm Akatsiya, es compatible con todas las municiones de 152 mm desarrolladas para los sistemas de artillería D-20, ML-20 y D-1. Tiene la capacidad de cargar proyectiles nucleares, además de misiles Krasnopol guiados a precisión. (Genys:2017b)

Fuente: Elaboración propia con datos de Military Factory (2017).

TABLA 6 ARMAMENTO EMPLEADO EN LA OPERACIÓN TORMENTA DEL DESIERTO (FUERZAS DE LA COALICIÓN)

PARTE DEL ARMAMENTO DE LAS FUERZAS DE LA COALICIÓN			
DENOMINACIÓN	MODALIDAD	ORIGEN	DESCRIPCIÓN
M1A1 Tanques	Tierra	Estadounidense/ General Dynamics	Es una versión mejorada del carro de combate principal M1 Abrams. Tiene una velocidad máxima de 41.5 Millas por Hora y pesa 67.6 toneladas. (Aftergood: 2000b)
M1M-104 Patriot	Misil Tierra-aire	Estadounidense/ Raytheon	Fue originalmente diseñada en los 70 como arma anti aérea, en el 89 fue modificado para defenderse de misiles balísticos. El sistema consiste en un misil de 17.4 pies de largo alimentado por un motor de cohetes de propulsión sólida, pesa 2 200 libras y tiene un alcance de 43 millas. (Aronson-Rath: 2014b)
Tomahawk Missile	Misil-aire	Estadounidense/ General Dynamics- Raytheon	Posee un margen de error de 10 metros, recurre al empleo de GPS para alcanzar su objetivo, su peso (con propulsor) es de 1 440 kilogramos, tiene un alcance de entre 1300 y 1600 kilómetros y una velocidad máxima de 880 kilómetros por hora. (Pardo: 2017)
Global Positioning System	Sistema espacial	Estadounidense/ Departamento de Defensa de Estados Unidos	Es un sistema de radionavegación espacial con base en Estados Unidos que ayuda a localizar una posición tridimensional (latitud, longitud y altitud) y proporciona el tiempo preciso (en nanosegundos) de cualquier parte de la tierra. (Dunbar: 2014)
AH-64 Apache	Aire	Estadounidense/ Boeing- MD Helicopters.	Es un helicóptero desarrollado por McDonnell Douglas (hoy Boeing), cuenta con un bimotor turbo-eje General Electric T700-GE-701. Emplea supresores infrarrojo que reducen la emisión de calor y tiene una potencia de 1890 Caballos de Fuerza. (Kable: 2017)
B-52 Stratofortress	Aire	Estadounidense/ Boeing	Es un bombardero estratégico de largo alcance, es capaz de volar a velocidades subsónicas, a altitudes de hasta 50 000 pies. Puede realizar operaciones contraofensivas aéreas, también es utilizado para vigilancia de océanos. (United States Air Force: 2015)
E-3 AWACS	Aire	Estadounidense/ Boeing-Northrop Grumman	Es un sofisticado puesto de mando aerotransportado, cuenta con un fuselaje modelo Boeing 707. A dichas aeronaves se les denomina AWACS por sus siglas en inglés *Airborne Warning and Control System*. (Aronson-Rath: 2014c)
F-117 A Stealth	Aire	Estadounidense/ Lockheed	Destaca por el uso de tecnología furtiva y su baja detección por los radares (Sputnik:2015). Cuenta con una planta motriz 2× turbofán General Electric F404-F1D2 y puede alcanzar una velocidad máxima de 993 km/h. (United States Air Force:2012)
E-8C JSTARS	Aire	Estadounidense/ Northrop Grumman	Es un avión militar y apoyo y gestión de batalla, fue empleado por primera vez en la Operación Tormenta del Desierto, cuenta con radares y subsistemas de computadora E-8C que le permiten recolectar y mostrar información sobre el campo de batalla- (Smith: 2017)
Drones (RPVs)	Sistema aéreo	Estadounidense/AeroVironment y General Atomics	Es un tipo de Sistemas de Aeronaves no Tripuladas (UAS, Unmanned Aircraft System), es un sistema operado remotamente por un piloto que puede localizarse en un área geográfica diferente. Algunos modelos de RPV son: RQ-11 Raven y RQ-12A Wasp (fabricados por AeroVironment), y MQ-9 Reaper (fabricado por General Atomics). (Urli:2014)

Fuente: Elaboración propia con datos de Aronson-Rath (2014d).

El 26 de febrero Hussein anunció la retirada de suelo kuwaití y más tarde Tareq Aziz comunicó a Naciones Unidas la aceptación de las resoluciones del Consejo. El 26 de agosto de 1992 a través de la resolución 733 se estableció también la inviolabilidad de la frontera entre Iraq y Kuwait y más adelante la resolución 833 trazó la frontera definitiva desplazándola 600 metros a favor de Kuwait por lo que algunos pozos pasaron a dominio kuwaití y la salida al mar de Iraq quedó reducida.[247]

3.2.2 Los primeros casos de ataques cibernéticos

Luego de la Guerra del Golfo el factor tecnológico comenzó a desarrollarse en la región. Así, de acuerdo con Ariel T. Sobelman (1998), pesé a que Medio Oriente se sumergió en el mundo tecnológico después de otras regiones como América del Norte y Europa ha experimentado de forma progresiva una inclinación hacia el desarrollo de tecnología con el fin de fortalecer sus aplicaciones en el campo militar.[248]

La penetración de Internet en los países de Medio Oriente ha sido importante, para muestra está el caso egipcio. En el año 2000 el número de usuarios de Internet era de 460 000 hacia finales de 2014 la cifra aumentó a 46 millones que corresponde a más de la mitad de la población.[249] La tendencia continua en diversos de países de Medio Oriente y del Norte de África en donde el promedio de la penetración de Internet es de 20% al año [250], a la cabeza se sitúa Qatar con un promedio de 94% (ver gráfica 2). Esto hablando sólo de las tecnologías de la Información y Comunicación (TIC), del otro lado está la investigación científica, especialmente aquella orientada al ámbito militar.

---

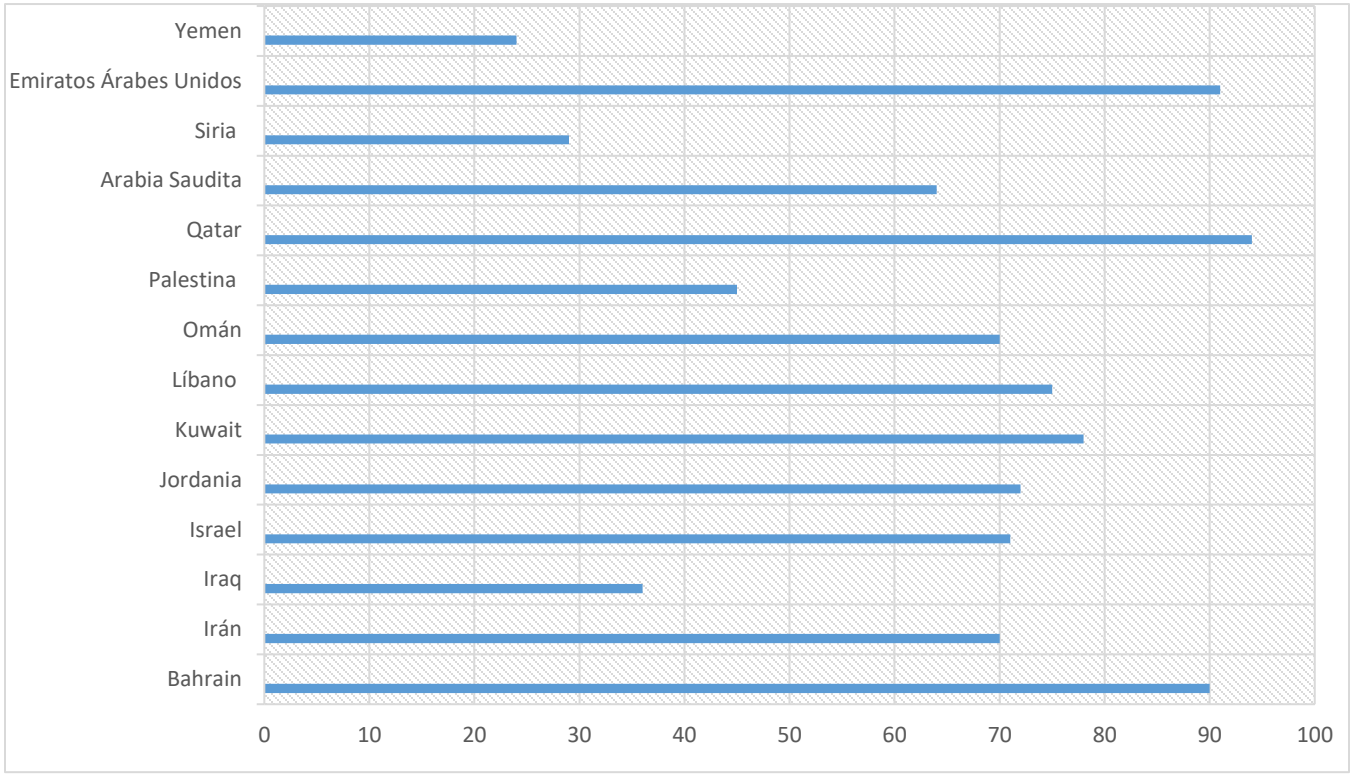
[247] Martín Muñoz, *Op. Cit,* p. 130

[248] Sobelman, Ariel T. (Junio, 1998). "An Information Revolution in the Middle East?". *Strategic Assessment*, Volume 1, No. 2, pp.13-15. [En línea]. Disponible en: <http://www.inss.org.il/uploadImages/systemFiles/An%20Information%20Revolution %20in%20the%20Middle%20East.pdf>.

[249] Savir, Uri. (Julio 5, 2015). "The Middle East's Internet revolution". *Al-Monitor*. [En línea]. Disponible en: <http://www.al-monitor.com/pulse/originals/2015/07/israel-middle-east-internet-revolution-democracy-youth.html>.

[250] Internet World Stats. (2017). Internet Usage in the Middle East. [En línea]. Disponible en: <http://www.internetworldstat s.com/stats5.htm#me>.

GRÁFICA 3 PORCENTAJE DE PENETRACIÓN DE INTERNET EN LA POBLACIÓN DE MEDIO ORIENTE (MARZO 2017)



Fuente: Elaboración propia con datos de Internet World Stats. (2017).

Sin embargo, esta apertura hacia al mundo tecnológico no está de libre de amenazas pues al tiempo en que la red de redes se expande por la región y en el que cada vez más infraestructura crítica regional depende las Tecnologías de la Información y Comunicación (TIC) incrementan también las vulnerabilidades.

Los primeros casos de ataques cibernéticos en el mundo se experimentaron hacia finales del siglo pasado, progresivamente, las capacidades y la sofisticación de los malware empleados para estos fines incrementaron. En esta zona en particular, las fricciones regionales se han trasladado también al espectro cibernético en donde se benefician del anonimato, la dimensión, la rapidez y la viabilidad económica con la que se puede llevar a cabo ataques en contra de medios de comunicación, infraestructura civil, militar y gubernamental. Dichos ataques son efectuados en el marco del choque de fuerzas tanto estatales como no estatales en la región.

Stuxnet representa el caso más emblemático del desarrollo y aplicación de arsenal cibernético en contra de infraestructura crítica nacional con fuertes consecuencias en el espacio tangible. Los primeros indicios de su empleo se registraron verano de 2009, de acuerdo con David E. Sanger reportero de *The New York Times*, el virus fue desarrollado en el marco de la Operación Olympic Games iniciada durante la administración de George W. Bush y acelerada en el periodo de Barack Obama en un intento por sabotear el programa nuclear iraní.[251]

El malware fue detectado en junio de 2010 por una compañía con base en Bielorrusia. Stuxnet está especialmente diseñado para atacar sistemas de control industrial asistidos por computadora (ICS, por sus siglas inglés computer-assisted industrial control system). El malware logró infiltrarse en equipos de cómputo con base operativa *Windows*, los cuales utilizaban un ICS de origen alemán producido por la empresa multinacional *Siemens*.[252]

Existe mucha especulación en torno a la forma en que el virus ingresó en las plantas nucleares iraníes, algunas versiones sugieren el empleo de un agente infiltrado que se encargó de ingresar el malware por medio de una USB. En adición, la sofisticación del virus también sugiere que un Estado estuvo involucrado en su desarrollo y propagación. Sin embargo, es imposible poder determinar con certeza su origen y la forma en que ingresó los ICS iraníes.[253]

Una vez dentro de ICS el malware verificó la presencia de un tipo particular de Controlador Lógico Programable (PLC, por sus siglas en inglés *Programmable Logic Controller*) conectado con un tipo particular de convertidor de frecuencia que funciona a 807-1 210 Hz. Las centrífugas nucleares iraníes normalmente giraban en un rango más lento al nominal que es de 1 064 Hz (la máxima velocidad que puede soportar es de 1 400 Hz), Stuxnet controló los PLC y llevó a las centrifugadoras a

[251] Sanger, David E. (Junio 1, 2012). "Obama Order Sped Up Wave of Cyberattacks Against Iran". *The New York Times.* [En línea]. Disponible en: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>

[252] Kerr, Paul K., John Rollins y Catherine A. Theohary. (Diciembre 9, 2010). "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability". *Congressional Research Service.* [En línea]. Disponible en: <https://fas.org/sgp/crs/natsec/R41524.pdf>

[253] *ídem*

girar a 1 410 Hz por 15 minutos, luego las regresó a 1 064 Hz por un periodo de 27 días, posteriormente las disminuyó a 2 Hz durante 50 minutos para retornar nuevamente a 1 064 Hz, este patrón se repitió de forma indefinida inutilizando cerca de 1 000 centrifugadoras.[254]

Stuxnet, no sólo afectó las instalaciones nucleares de Natanz y los ordenadores relacionados con el nuevo complejo en Bushehr sino que se expandió a otros países, entre los afectados figuran Indonesia, India, Azerbaiyán, Pakistán, Malasia, Uzbekistán, Rusia, Reino Unido, entre otros.[255] Por su complejidad Stuxnet es conocida como el primer ciberarma guiada a precisión, su origen ha sido atribuido a países como Estados Unidos, Israel, Reino Unido, Rusia, China y Francia, en el ámbito de la seguridad su aparición alertó a la comunidad internacional del posible inicio de una carrera armamentística en el ciberespacio.[256]

Otro de los casos más visibles en Medio Oriente fue el ciberataque dirigido a la empresa estatal saudí de petróleo y gas Aramco. El ciberataque tuvo lugar el 15 de agosto de 2012 cuando, aprovechando la celebración de la Lailat al Qadr[257], Aramco fue blanco un ataque cibernético. El resultado fue la inhabilitación de 35 000 computadoras, el virus se expandió a través de un correo misterioso que fue recibido por uno de los técnicos del equipo en informática.[258]

El virus conocido como Shamoon tenía la capacidad de reproducirse a sí mismo afectando a todas computadoras con base operativa *Windows*. A la empresa le tomó al menos dos semanas recuperarse del ataque. Shamoon estaba diseñado para suprimir toda la información en los discos duros de los dispositivos infectados, aunque el malware no poseía la capacidad de tomar control de las instalaciones afecto las operaciones de la empresa y resultó en la perdida de información sobre

[254] Lindsay, Jon R. (Enero 15, 2013). "Stuxnet and the Limits of Cyber Warfare". *Security Studies*, Volume 22, 2013 - Issue 3, p. 390.
[255] Falliere, Nicolas; Liam O Murchu, y Eric Chien. (Febrero 2011). W32.Stuxnet Dossier. *Symantec*. [En línea]. Disponible en: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>
[256] Kerr, *Óp. Cit.,* pp. 8-11.
[257] La *Lailat al Qadr*, se trata de la noche más santa del mes Ramadán. Fuente: Mawlana (2006)
[258] Pagliery, Jose. (Agosto 5, 2015). "The inside story of the biggest hack in history". *CNN*. [En línea]. Disponible en: <http://money.cnn.com/2015/08/05/technology/aramco-hack/>

perforaciones y producción que no pudo recuperarse en adición se expandió a otras empresas como Rasgas, una compañía productora de Gas Licuado con base en Qatar.[259]

El ataque fue reivindicado por un grupo identificado como "Cutting Sword of Justice", el motivo del ataque fue el apoyo proporcionado por la compañía a la familia real Al Saud.[260]El ataque que afectó a una de la empresas productoras de petróleo más importantes del mundo llamó la atención del, entonces, Secretario de Defensa de Estados Unidos Leon Panetta, quién al percatarse del impacto en los mercados financieros que un ataque de esta naturaleza podría ocasionar, precisó que se trataba de un virus especialmente diseñado para hacer daño a dicha compañía y que sólo pocos países contaban con tales capacidades cibernéticas, de esta forma, Panetta planteó presunta participación del gobierno iraní.[261]

De acuerdo con datos de Symantec, Shamoon estaba conformado por tres módulos:

1. Módulo *dropper*. - que constituye el componente principal y la fuente de la infección
2. Módulo *wiper*. - encargado de destruir los datos en el dispositivo infectado
3. Módulo *reporter*. - que enviaba la información de vuelta al atacante.[262]

En adición, se ha planteado la posibilidad de que el virus se introdujera de forma directa a una computadora dentro de la compañía. [263] Shamoon sacó a la luz dos puntos importantes en cuanto a las consecuencias de un ciberataque a infraestructuras críticas. El primero es el posible control de funciones importantes como los procesos de extracción del petróleo, que pudieran poner en riesgo la seguridad de una nación y, el segundo punto, corresponde al impacto de la

[259] Bronk, Christopher y Eneken Tikk-Ringas. (2013). "The Cyber Attack on Saudi Aramco". *Survival Global Politics and Strategy*, vol. 55 no. 2, p.81.
[260][260] Pagliery, *Óp. Cit.*
[261] Bronk, *Óp. Cit., p.82*
[262] Carr, Jeffrey. (Agosto 22, 2012). "Was Iran Responsible for Saudi Aramco's Network Attack?". *Digital Dao*. [En línea]. Disponible en: <http://jeffreycarr.blogspot.mx/2012/08/was-iran-responsible-for-saudi-aramcos.html>
[263] Pagliery, *Óp. Cit.*

inhabilitación de empresas clave para la economía nacional y su efecto en los mercados financieros mundiales.

En 2014 salió a la luz un nuevo ataque cibernético: el virus cleaver, que perjudicó por alrededor de dos años infraestructura crítica, corporaciones en el ámbito de la defensa y estructuras gubernamentales en Medio Oriente y más allá. Entre los países afectados figuran Canadá, China, Reino Unido, Francia, Alemania, India, Israel, Kuwait, México, Pakistán. Qatar, Arabia Saudita, Corea del Sur, Turquía, Emiratos Árabes Unidos y Estados Unidos. El ataque también conocido como Operación Cleaver ejecutó durante varios años actividades de vigilancia e infiltración. El responsable de la operación es, presuntamente, el gobierno iraní.[264]Entre los objetivos de Cleaver figuran:

- Entidades militares
- Infraestructura energética y de servicios
- Aeropuertos
- Telecomunicaciones
- La base de la industrial de la defensa
- Infraestructura gubernamental.[265]
- Infraestructura de petróleo y gas
- Sistemas de transporte
- Hospitales
- El sector aeroespacial
- Compañías químicas

El malware tenía la capacidad de apoderarse de Sistemas de Control Industrial (ICS, por sus siglas en inglés Industrial Control Systems) y de Sistemas de Supervisión, Control y Adquisición de Datos (SCADA, por sus siglas en inglés Supervisory Control And Data Acquisition), Claver se propagó en dispositivos con base operativa *Windows* y *Linux*, la mayoría de los cuales se ubicaban en países de Medio Oriente.[266]

Los casos hasta este momento se dirigen en contra de infraestructura crítica nacional. En la mayoría de los casos el lapso entre su descubrimiento y el inicio de operaciones es de por lo menos tres años, la mayoría de los malware permanecen inactivos por un periodo antes de su activación en los sistemas y son ayudados por

[264] Cylance. (Diciembre 2, 2014). Operation Cleaver. [En línea]. Disponible en: <https://www.cylance.com/content/dam/cylance/pages/operationcleaver/Cylance_Operation_Cleaver_Report.pdf>
[265] *Ídem*.
[266] *Ídem*.

otros software maliciosos que les ayuda a mantener la apariencia de normalidad en los sistemas atacados. Se ha examinado que en la mayor parte de los casos los sistemas victimas notan de ataque cuando ya es tarde: se ha sustraído información relevante o inhabilitado centrifugas nucleares. Una tendencia en este tipo de eventos es que a menudo las entidades atacadas no revelan que han sido víctimas de ataques, pues hacerlo vulneraria aún más su seguridad, como es el caso de Stuxnet en donde no existe más información sobre los sistemas fuera de Irán donde se propago el virus.

Del otro lado se encuentran las operaciones de ciberespionaje que, aunque no representan una amenaza de las mismas dimensiones como lo es el apoderamiento de las funciones de una planta nuclear, la información que se puede obtener a través de su empleo vulnera de forma significativa la seguridad de las naciones (como se analiza más adelante en el caso de Siria e Israel). En este sentido, Medio Oriente posee gran parte de los *Hot Spots* cibernéticos a los que refiere Richard Stiennon en su obra *Surviving Cyberwar*, por lo que tanto el desarrollo de arsenal cibernético como la aparición de ejércitos electrónicos incrementa con el paso del tiempo, demostrando la trasformación en la conducción de conflictos y en la percepción de amenazas a nivel regional.

Entre los casos más sobresalientes de espionaje cibernético se encuentran:

- Operación Duqu: fue descubierta en 2011, su arquitectura le relaciona con Stuxnet y su intención era crear una base de datos de inteligencia mundial, según investigaciones tanto Duqu como Stuxnet fueron creados en 2007.[267]Los equipos infectados se encuentran en todas partes del mundo de los que robó certificados digitales, lo cuales permitirían a otro malware ingresar en el futuro sin ser detectado.[268]

[267] Gutierrez del Moral, Leonardo. (2014). *Curso de Ciberseguridad y Hacking Ético*. España: Lantia Publishing 2013, p. 48.
[268] Walchko, Kevin J. (2016). "Cyber Espionage Tools". *Planet Express*. [En línea]. Disponible en. <https://walchko.github.io/posts/2015/12/cyber-espionage-tools/>

- Operación Olympic Games: en el marco de la operación en contra del programa nuclear iraní por parte, presuntamente, de Estados Unidos e Israel, se desarrolló otra arma cibernética dedicada al robo de información. Se trata de virus Flame, descubierto en 2012. El virus infectó numerosos ordenadores en Irán y según autoridades iraníes está relacionada también con el virus Duqu. De acuerdo con las investigaciones Flame era capaz de registrar trazos del teclado, activar micrófonos para grabar conversaciones y tomar capturas de pantalla. Según datos de la firma de antivirus Kaspersky Lab, se encontraron rastros del virus por todo Medio Oriente, el país más infectado fue Irán, seguido de Israel, los Territorios Palestinos, Sudán, Siria y Líbano, también se registraron casos en Estados Unidos y Europa.[269]
- La Operation Newscaster: fue descubierta en 2014, se trata del empleo del virus conocido como *Parastoo*, las operaciones de ciberespionaje político y militar fueron ejecutadas en contra de Estados Unidos. Israel, Reino Unido, Arabia Saudita, Iraq y Afganistán. El responsable es, presuntamente, la República Islámica de Irán, la operación utilizó "ingeniería humana" pues un grupo en cargado de la misión creó un portal de noticias falso, además de perfiles falsos con el fin de crear lazos con personajes políticos y militares de los que se sustrajo información confidencial. El virus fue enviado a través de correos electrónicos, enviados a cerca de 2 000 personas y en donde se transmitía el virus. La operación estuvo activa cerca de tres años antes de detectada, se especula que se trató contraofensiva iraní al ataque de Stuxnet, sin embargo, como sucede en el ámbito de la seguridad informática encontrar un culpable es casi imposible.[270]

[269] Nakashima, Ellen. (Mayo 29, 2012). "Iran acknowledges that Flame virus has infected computers nationwide". *The Washington Post*. [En línea]. Disponible en: <https://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U_story.html?utm_term=.e9ef9806a61b>

[270] Pizzi, Michael. (Mayo 29, 2014). "Iran hackers set up fake news site, personas to steal U.S. secrets". *Al Jazeera America.* [En línea]. Disponible en: <http://america.aljazeera.com/articles/2014/5/29/iran-newscaster-hackers.html>

En el marco de las fricciones regionales se ha desarrollado y utilizado armamento cibernético en Medio Oriente, el avance tecnológico ha permitido que tanto actores estatales como no estatales apliquen esta clase de armamento en contra de infraestructura critica nacional o para sustraer información de carácter confidencial. La evolución y la sofisticación de este tipo de armas eleva las alertas de seguridad, pues si la atribución de responsabilidad es una tarea imposible, la regulación y control del ciberarsenal posee mayor complejidad.

3.3. LAS POTENCIAS TECNOLÓGICO-MILITARES EN LA REGIÓN

Son múltiples los países en Medio Oriente que han desarrollado proyectos de infraestructura tecnológica atendiendo a la creciente correlación entre la era de la información y la seguridad nacional. De este modo, Egipto fue uno de los primeros países en orientar esfuerzos al desarrollo de capacidades militares en materia de Comando, Control, Comunicaciones, Computación e Inteligencia (C4I) e incluso para el establecimiento de comandos cibernéticos especiales. [271]

Bajo esta misma línea también se encuentra el desarrollo de armamento con sistemas autónomos de funcionamiento, esta clase de armas transforman los datos del entorno en planes y acciones intencionales, por lo que involucra diversas aplicaciones tecnológicas como sensores, software de control y ejecución, hardware, tecnologías de comunicación e interfaces hombre-máquina que permiten al sistema interactuar con otros agentes.[272]A esta rama pertenecen los vehículos conocidos como drones, especialmente los UCAVs (*Unmanned Combat Air Vehicles*). De acuerdo con estudios del think tank *New America*, los principales países exportadores de este tipo de tecnología son Estados Unidos e Israel. En EE. UU la empresa encargada de su fabricación es General Atomics, mientras que los

[271] Sobelman, *Óp. Cit.*

[272] Boulanin, Vincent. (Diciembre, 2016). *Mapping the Development of Autonomy in Weapon Systems, A primer on autonomy*. Stockholm International Peace Research Institute. Working Paper, pp. 11-16. [En línea]. Disponible: <https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf>.

principales importadores de drones MQ-9 Reaper son países miembros de la Organización del Tratado del Atlántico Norte (OTAN).[273]

El caso de Israel es muy importante, ya que es el mayor exportador de drones con capacidad de combate en el mundo. El modelo IAI Heron, fabricado por *Israel Aerospace Industries*, está diseñado para competir con su contraparte estadounidense, el MQ-9 Raper. Hasta el momento, no se conoce con certeza los países a los que Israel ha exportado este tipo de tecnología, pues el país se ha rehusado a compartir dicha información. Sin embargo, entre algunas naciones que la conforman la lista figuran EE. UU, Reino Unido, Canadá, Francia, Australia, Alemania, España, Brasil, India, China, Países Bajos, Azerbaiyán y Nigeria.[274]

En adición, los primeros países en emplear drones en combate (sin capacidad de ataque) fueron Estados Unidos y Reino Unido en escenarios como Afganistán (en 2001 y 2008), e Israel en Gaza (en 2004). Sin embargo, el uso de este tipo de vehículos aéreos se ha expandido a otras regiones, para el año 2016 países como Arabia Saudita, Iraq, Turquía, Pakistán y Nigeria ya habían empleado este tipo de vehículos zonas de combate (ver tabla 7).[275]

TABLA 7 EMPLEO DE UAVS (UNANIMATED AIR VEHICLES) EN MEDIO ORIENTE (2001-2016)

PAÍS	FECHA	PAÍS EN EL QUE SE USO	MODELO	DRONES EN ARSENAL
Estados Unidos	7-octubre-2001	Afganistán	Predator	RQ-11 Raven, AeroVironment Wasp III, AeroVironment RQ-20 Puma, RQ-16, T-Hawk, MQ-1C Grey Eagles, MQ-9 Reapers, RQ-7 Shadow, RQ-4 Global Hawk
Israel	24-octubre-2004	Gaza	Desconocido	Orbitor (series), Aerostar, Hermes (series), Heron (series), Searcher (Series)
Reino Unido	1-mayo-2008	Afganistán	MQ-9 Reaper	ScanEagle (United States), MQ-9 Reaper (United States), Hermes 450 (Israel)
Pakistan	7-septiembre-2015	Su propio territorio	Burraq	Burraq, Shahpar, Arrow

[273] Bergen, Peter; David Sterman; Alyssa Sims; Albert Ford, y Christopher Mellon. (2016). *In Depth World of Drones.* New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/1-introduction-how-we-became-world-drones/>.

[274] *Ídem.*

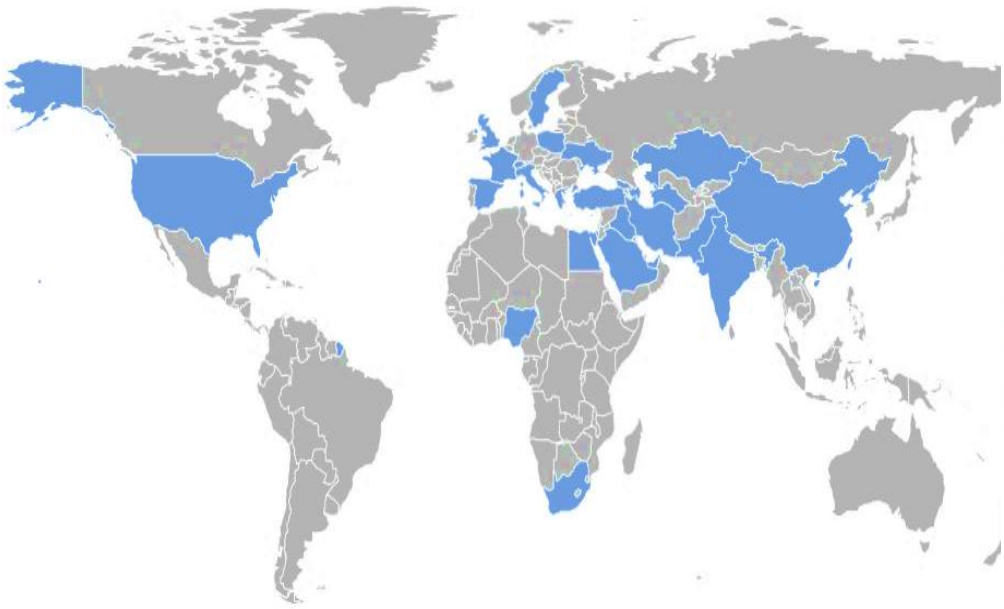
[275] Bergen, Peter (et.al). (2016). *In Depth World of Drones. Who Has What: Countries with Drones Used in Combat*. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/2-who-has-what-countries-drone s-used-combat/>.

Nigeria	3-febrero-2016	Su propio territorio	CH-3	Aerostar (Israel), CH-3 (China) GULMA (Domestic)
Irán	4-febrero-2016	Siria	Shahed 129	Ababil (five variants), Mohajer (four variants), Karrar, Yasir, H-110 Sarir, Hazem, Hamaseh, Shahed 129, Ra'ad-85
Azerbaiyán	5-abril- 2016	Nagorno-Karabakh	IAI Harop	
Iraq	25-mayo- 2016	Su propio territorio	CH-4	ScanEagle (United States), CH-4B (China)
Turquía	9-diciembre-2016	Su propio territorio	Bayraktar	TAI ANKA, Bayraktar, Bayraktar TB-2, Heron (Israel), Aerostar (Israel), Gnat (United States)

Fuente: Bergen, Peter (et.al). (2016). *In Depth World of Drones. Who Has What: Countries with Drones Used in Combat*. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/2-who-has-what-countries-drone s-used-combat/>.

Actualmente el número de países que se ha equipado con drones con capacidades de combate ha incrementado. La tendencia comenzó con Estados Unidos, Israel y Reino Unido hasta 2008, a partir de 2011 la lista incluyó a países como Irán, Emiratos Árabes Unidos, Iraq, Egipto, Arabia Saudita y Turquía, además de otros países más allá de Medio Oriente (ver mapa 1). [276]

MAPA 1 PAÍSES QUE POSEEN DRONES CON CAPACIDADES DE COMBATE (2016)



Países	Año	Países	Año
EE.UU	2001	Georgia	2015
Israel	2004	Kazajstán	2016
R.U.	2008	India	2016
Irán	2010	Grecia	2016
E.A.U.	2011	Suecia	2016
Corea del Norte	2012	Suiza	2016
China	2013	Ucrania	2016
Sudáfrica	2013	Turquía	2016
Italia	2015	Azerbaiyán	2016
Nigeria	2015	France	2016
Spain	2015	Turkmenistán	2016
Pakistan	2015	Arabia Saudita	2016
Iraq	2015	Polonia	2017
Egypt	2015	Taiwán	2017
Georgia	2015		

Fuente: Bergen, Peter (et.al). (2016). *In Depth World of Drones. Who Has What: Countries Developing Armed Drones*. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/4-who-has-what-countries-developing-armed-drones/>

[276] Bergen, Peter (et.al). (2016). *In Depth World of Drones. Who Has What: Countries Developing Armed Drones. New America*. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/4-who-has-what-countries-devel oping-armed-drones/>.

Al mismo tiempo, actores no estatales en la región también han adquirido drones tanto con fines de vigilancia como con capacidades de ataque. En enero de 2017 el Estado Islámico anunció el establecimiento de una unidad oficial de drones conocida como *Unmanned Aircraft of the Mujahideen* que se encarga de organizar el uso de aviones no tripulados en escenarios de combate. Sin embargo, a diferencia de otras organizaciones como Hezbollah y Hamas, el Estado Islámico aún no cuenta con aeronaves no tripuladas de grado militar, es decir, con capacidad de ataque. Los drones utilizados por el Estado Islámico se han equipado con armamento de forma improvisada. No obstante, han causado bajas, por ejemplo, entre las fuerzas kurdas en octubre de 2016. [277]

En adición, en escenarios como Yemen, el movimiento Houthi atacó un buque de guerra de Arabia Saudita en el Mar Rojo mediante el uso de una nave marítima armada no tripulada. Asimismo, miembros de la rebelión Houthi también han empleado vehículos aéreos comerciales de operación remota en el marco de enfrentamientos contra la Coalición árabe.[278] Por su parte, la organización Hezbollah, es conocida por ser el primer actor no estatal en poseer este tipo de tecnología, Hezbollah ha sobrevolado espacio aéreo israelí con drones Mirsad 1 de vigilancia militar. En agosto de 2016 la organización envió pequeños helicópteros armados con municiones para lanzar un ataque a las posiciones rebeldes en Alepo (Siria).[279]

Finalmente, la organización Hamas cuenta con drones tanto de vigilancia como de combate que han sobrevolado espacio aéreo israelí y que, se presume, fueron provistos por Irán. De esta forma, drones tipo Ababil (tecnología iraní) han sido empleados en Gaza en 2014.[280] Otros actores no estatales que poseen tecnología

[277] Bergen, Peter (et.al). (2016). In Depth World of Drones. *Non-State Actors with Drone Capabilities.* New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/5-non-stateactors-drone-capabilities/>.
[278] *Ídem.*
[279] *Ídem.*
[280] HispanTv. (Diciembre 21, 2016). "HAMAS alerta a Israel que seguirá fabricando drones más avanzados". [En línea]. Disponible: <http://www.hispantv.com/noticias/palestina/327899/hamas-fabrica-drones-israel-asesinato-experto>.

drone son grupos rebeldes en Libia, kurdos peshmerga, Jabhat al-Nusra, Faylaq Al-Sham y Saraya al-Khorani.[281]

Respecto a otros tipos de armamento altamente tecnológico, diversos países de Medio Oriente han desarrollado su propia industria armamentista, entre los cuales se encuentran:

Israel

Israel ha desarrollado los tanques Merkava empleados por la Fuerzas de Defensa desde 1979, los cuales representan uno de los vehículos militares más sofisticados.[282]Israel se ha convertido en uno de los países que más invierte en investigación científica, lo cual se traduce en armas de alta tecnología como los robots de combate de la compañía *G-Nius*, esta clase de armamento ha sido empleado en zonas como Franja de Gaza.[283]

Otra compañía que ha prosperado en los últimos años es IWI (Israel Weapon Industries) que provee al ejército con ametralladoras Uzi, rifles de asalto Tavor y ametralladoras Negev, el 90% de su producción se exporta.[284]Por último, es preciso mencionar a la Fuerza Aérea Israelí, que en los últimos años ha desarrollado un mejor sistema de defensa aéreo, la Honda de David es capaz de interceptar misiles de corto alcance, provenientes de Irán o Siria. Este nuevo sistema refuerza a los ya conocidos Cúpula de Hierro, "Arrow 2" y "Arrow 3". La Honda de David no es móvil, como la Cúpula de Hierro, sin embargo, tiene la capacidad de proteger en su totalidad al Estado de Israel.[285]

Turquía

Después de la década de los 80 las fuerzas armadas turcas establecieron centros tecnológicos, de Investigación y Desarrollo (I+D). Entonces, surgieron empresas

[281] *Ídem.*
[282] Cohen, Amir. (Mayo 13, 2015). "Las cinco armas de guerra más mortíferas de Israel". *RT*. [En línea]. Disponible: <https://actualidad.rt.com/actualidad/174692-armas-guerra-mortiferas-israel>.
[283] Becker, Markus. (Agosto 27, 2014). "Israel's War Business". *Spiegel*. [En línea]. Disponible: <http://www.spiegel.de/international/world/defense-industry-the-business-of-war-in-israel-a-988245.html>.
[284] *Ídem.*
[285] LATAMISRAEL. (Mayo 18, 2017). "Nuevo sistema de defensa aéreo protege a todo Israel contra misiles de alto rango." [En línea]. Disponible en: <http://latamisrael.com/nuevo-sistema-defensa-aereo-protege-israel-misiles-alto-rango/>.

como ASELSAN, HAVELSAN, ROKETSAN y TAI (Industria Aeroespacial Turca), el resultado fue el desarrollo de las capacidades aéreas, navales y terrestres, así como el avance en equipos de artillería, misiles y sistemas C4I.[286]

De esta forma, los equipos de comunicación y los sistemas de guerra electrónica para el ejército turco son producidos por ASELSAN, cuyo mayor accionista es OYAK (fondo de pensiones las Fuerzas Armadas de Turquía). La corporación también se encarga de la producción de Sistemas de Navegación Inercial y Control de Fuego para un proyecto perteneciente a TÜSAS (Industria Aeroespacial) dedicada a la producción de aviones F-16, y que también produce componentes para el programa de misiles Stinger.[287]

Progresivamente, el gobierno se ha orientado por el desarrollo de la industria militar nacional con el fin de reducir su dependencia de la OTAN, por lo que se han firmado acuerdos de cooperación con países como Benín, Chad, Congo, Malí, Senegal, Gabón, Rumania, Gambia, Somalia e Indonesia, además ha firmado acuerdos de cooperación militar más concretos con Níger, Nigeria, Djibouti, Costa de Marfil, Montenegro, Qatar y Suecia, según datos de mayo de 2017.[288]El gobierno turco invierte en este sector 3.5 mil millones con una producción anual de entre 2 y 3 mil millones, mientras que los gastos militares ascendieron a 14 900 millones en 2016.[289]

Emiratos Árabes Unidos

Es uno de los países de la región con mayor inversión en la industria militar, según cifras de 2016 rondaba los 23.5 mil millones de dólares y se prevé que seguirá hasta alcanzar los 31.8 mil millones en 2021.[290] El porcentaje de inversión en defensa respecto al Producto Interno Bruto es elevado, pues busca responder a tres

[286] Herdem. (Septiembre 9, 2015). "Turkish Defence Industry: A Step Towards a Nation-Oriented Production". [En línea]. Disponible en: <http://herdem.av.tr/turkish-defence-industry-step-nationoriented-pro duction/>.
[287] Global Security. (Noviembre 5, 2016). "Turkey Domestic Arms Industry". [En línea]. Disponible en: <http://www.globalsecurity.org/military/world/europe/tu-industry.htm>.
[288] Tastekin, Fehim. (Mayo 19, 2017). "How lucrative is Turkey's defense industry?". *Al-Monitor.* [En línea]. Disponible en: <http://www.al-monitor.com/pulse/originals/2017/05/turkey-how-lucrative-defense-industry.html>
[289] *Ídem.*
[290] Global Security. (Diciembre 15, 2016). "Emirati Military Spending". [En línea]. Disponible en: <http://www.globalsecurity.org/military/world/gulf/uae-budget.htm>.

importantes factores para seguridad de los emiratos, lo cuales son: 1) el incremento del extremismo islamista en la región, 2) las persistentes tensiones con Irán, y 3) la participación de los emiratos en la coalición liderada por Arabia Saudita en Yemen.[291]

Los Emiratos Árabes Unidos (EAU), son el segundo comprador de equipo militar más grande de Estados Unidos, su Programa de Ventas Militares Extranjeras (*Foreign Military Sales*, FMS) es una de las más grandes en Medio Oriente y el mundo.[292] Tanto los EUA como Arabia Saudita buscan fabricar armas modernas para hacer frente a la amenazas de la región, principalmente del lado del golfo, en sentido el desarrollo de Irán en equipo militar como misiles balísticos y sistemas no tripulados, incentiva que tanto EAU como Arabia Saudita se esfuercen igualarlo y superarlo.[293]

Específicamente se ha fabricado vehículos blindados por parte de la compañía *NIMR Automotive*, en 2014 los emiratos fusionaron más de una docena de compañías creando un conglomerado llamado *Emirates Defense Industries Company* (una de las cuales es *NIMR*). Mientras que el plano de la defensa aérea y tras la negativa de Estados Unidos y Europa para venderles aeronaves F-35 (capaces de evadir radares) de Lockheed Martin y demás armamento de tecnología sensible, los EAU optaron por recurrir a Rusia, específicamente a la corporación Rostec para desarrollar aviones de combate ligeros.[294]

Egipto

Después de la firma del Tratado de Paz con Israel en 1979, el sector militar en Egipto se convirtió en una institución cada vez más profesional, a partir de ese mismo año la República Árabe de Egipto recibió créditos anuales por parte de Estados Unidos por 1 300 millones de dólares para la adquisición de defensa, por

[291] The International Trade Administration. (Diciembre 8, 2016). "United Arab Emirates - Defense". *Export.gov* [En línea]. Disponible en: <https://www.export.gov/article?id=United-Arab-Emirates-Defense>.
[292] *Ídem.*
[293] Saab, Bilal Y. (Mayo, 2014). *The Gulf Rising*. Washington: The Atlantic Council of the United State, pp.1-13
[294] Fox Business. (Mayo 12, 2017). "Gulf Arab States Push to Develop Their Own Defense Industries". [En línea]. Disponible en: <http://www.foxbusiness.com/features/2017/04/26/ted-nugent-on-cruzs-wall-proposal-idea-is-absolutely-bulletproof.html>.

lo que las fuerzas armadas comenzaron a dotarse de equipo militar occidental, dejando a un lado los insumos soviéticos.[295]

Del mismo modo, la cooperación con Washington incrementó en el ámbito de la educación y capacitación, en donde la milicia egipcia adquirió conocimientos tácticos occidentales que cobraron fuerza especialmente en la década de los 90.[296]La Organización Árabe Industrial (AOI, por sus siglas en inglés) es el complejo industrial militar egipcio creado en 1973 por el entonces presidente Anwar el-Sadat, hacia 1980 la AOI tenía una producción anual de 100 millones de dólares y además de abastecer a las fuerzas armadas nacionales, realizaba exportaciones a Iraq y otros países árabes.

Paralelamente a la AOI, existen las Industrias de Producción Militar (MPI, por sus siglas en inglés) que consta de 15 fábricas principalmente ubicadas en El Cairo, cuya producción se orienta a satisfacer la demanda interna.[297]Actualmente, Egipto posee un número importante de plataformas de armas modernas colocándose como el segundo país en la región con ese inventario (sin considerar a Turquía), el ejército egipcio cuenta con tanques M-60 y M-1, cuya moderna tecnología se combina con el viejo sistema de blindaje soviético.[298]

Egipto, Israel y Siria cuentan con un gran número de misiles aire-tierra. Sin embargo, sólo la Fuerza Aérea Israelí posee tres equipos exclusivos: 1) sistemas modernos de mediano y largo alcance, 2) avanzados sistemas de radares, y 3) facilidades de comando y control.[299]

En adición, se presume que Egipto y Siria poseen ojivas químicas para sus misiles SCUD, ambos países también poseen la capacidad de producir drones y UCAVs, Egipto en particular cuenta con un número desconocido de SCUD-B

[295] Kechichian, Joseph y Jeanne Nazimek. (Septiembre 1997). "Challenges to the Military in Egypt". *Madre East Policy*. [En línea]. Disponible en: <http://www.mepc.org/challenges-military-egypt>
[296] *ídem*
[297] Stork, Joe. (1987). "Arms Industries of the Middle East". Middle East Research and Information Project. [En línea]. Disponible en: <http://www.merip.org/mer/mer144/arms-industries-middle-east>
[298] Cordesman, Anthony H. (Febrero 10, 2011). "The Egyptian Military and the Arab-Israeli Military Balance". *Center for Strategic and International Studies.* [En línea]. Disponible en: <https://www.csis.org/analysis/egyptian-military-and-arab-israeli-military-balance>
[299] *Ídem*

(también conocido como misiles R-17 con un rango de alcance de 300 kilómetros) y al menos entre 9-12 lanzadores TEL (vehículos militares para transportar misiles, capaces de llevar en posición de tiro y de lanzar uno o dos misiles), además de SCUDS C (una versión mejorada del R-17, con un rango de alcance de 600 kilómetros) presuntamente adquiridos de Corea del Norte. Egipto es uno de los países con mayor dependencia a la asistencia militar estadounidense que cualquier otro país en la región, en 2008 la ayuda militar ascendía a 1.29 mil millones, y todo muestra que la tendencia se mantendrá.[300]

Irán

Estados Unidos fue de los mayores proveedores de armas de Irán. En especial el subministro comenzó a crecer a partir de 1953, después que el Primer Ministro democráticamente electo, Mohammad Mosaddegh, fue derrocado mediante un golpe de estado y suplantado por la dictadura monárquica del Sha Mohammad Reza Pahlavi.[301]En 1963 sólo cuatro industrias estatales constituían la base militar iraní, juntas conformaban la Organización de Industrias Militares (MIO, por sus siglas en inglés), la Industria de Aviación Iraní se concentraba en vehículos aéreos de combate, de la misma forma la Industria de Helicópteros, mientras que la Industria Electrónica de Irán lo hacía en los sistemas de defensa.[302]

Sin embargo, de acuerdo con datos de 1973, Irán era el mayor comprador militar estadounidense, hacia 1974 las ventas militares sumaban alrededor de 4 mil millones de dólares, entonces Irán se convirtió en la potencia militar dominante, hasta 1979.[303]Tras la Revolución Islámica en Irán, China y la Unión Soviética reemplazaron a Estados Unidos como proveedores, empero, entre 1984 y 1986 Estados Unidos e Israel vendieron armas de forma ilegal a Irán, pese al embargo en su contra (en el marco de la negociación estadounidense para la liberación de

[300] *Ídem*

[301] Keng Kuek Ser, Kuang. (Junio 1, 2016). "Where did Iran get its military arms over the last 70 years?". *Public Radio International.* [En línea]. Disponible: <https://www.pri.org/stories/2016-06-01/where-did-iran-get-its-military-arms-over-last-70-years>

[302] Global Security. (Junio 16, 2012). "Defense Industry". [En línea]. Disponible: <http://www.globalsecurity.org/military/world/iran/industry.htm>

[303] Keng Kuek Ser, *Óp. Cit*.

rehenes en Líbano, por lo cual recurrió a la venta clandestina de armas, el caso es conocido como Irán-contra o *Irangate*).[304]

Como resultado de las restricciones en las ventas de armas en su contra, se impulsó el desarrollo de la industria militar interna, a partir de entonces, Irán comenzó a producir sus propios tanques, vehículos blindados, misiles, aviones de combate y submarinos, de esta forma de 2008 a 2015 China y Rusia mantuvieron un volumen menor de comercio de armas con Irán.[305]

Por otra parte, está el desarrollo del programa de misiles balísticos, el cual fue especialmente impulsado después de dos hechos determinantes en la región: la Guerra Iraq-Irán y la Guerra del Golfo. Ambos eventos demostraron la superioridad en armamento aéreo por parte de Iraq y Estados Unidos. A partir de entonces, y de acuerdo con Uzi Rubin, la república islámica incrementó sus esfuerzos en el desarrollo y despliegue de misiles diseñados para lograr el control de los espacios marítimos, terrestres y aéreos adyacentes a sus fronteras, especialmente en el Golfo Pérsico. De esta manera, según datos de 2006, Irán cuenta con armamento aéreo de origen chino y ruso, un ejemplo de esto es el misil anti-buque Raad de base tierra, que tiene un alcance de 350 km.[306] En adición, están Fatah, un cohete de precisión con un alcance de 200 km y una ojiva de varios cientos de kilogramos, y el lanzacohetes tipo Katyusha conocidos como Fadjr.[307]

Además de la conocida familia de misiles balísticos *Shahab*[308] que tras la guerra con Iraq comenzaron a desarrollarse con mayor prioridad, los primeros misiles balísticos fueron adquiridos en Libia y empleados en la Guerra de las Ciudades[309]. En adelante el mayor proveedor de misiles Scud B y Scud C fue Corea del Norte

[304] *ídem*
[305] *Ídem*
[306] Rubin, Uzi. (2006). "The Global Reach of Iran's Ballistic Missiles". *Institute for National Security Studies*. [En línea]. Disponible en: <http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/(FILE)1188302 022 .pdf>.
[307] *Ídem*
[308] *Shahab*, es un nombre genérico en Irán para la línea de misiles balísiticos de diversas gamas y cargas, comparte modelo en tecnología de propulsión y diseño con los famosos misiles soviéticos scud, también conocidos como R11. Fuente: Rubin (2016).
[309] En 1988, fue un punto muerto en la guerra con Iraq, en donde ambos países concentraron sus fuerzas en la guerra aérea, durante dichos enfremientos Tehran y Bagdad recibieron numerosos ataques aéreos. Fuente: Cordesman (2003).

con un alcance de 300 y 580 km, respectivamente, progresivamente el alcance de los misiles aumentó hasta llegar a misil denominado *Cossar* que se presume tiene un alcance de entre 2000 y 5000 km.[310]Según informes de 2009, el programa de Misiles Balísticos Intercontinentales (*Intercontinental Ballistic Missiles*, ICBM) iraní se encontraba a seis u ocho años de producir un misil capaz de lanzar una ojiva nuclear de 1000 gramos a un alcance de 2000 kilómetros, el mismo informe estimó que Irán recibió ayuda de China, Rusia y Corea del Norte.[311]

La firma del acuerdo nuclear en 2015 creó una nueva oportunidad de comercio armamentista con China y Rusia, en adición también en 2015, Rusia levantó el embargo que impedía la venta de un poderoso sistema de defensa aérea antimisiles.[312]El crecimiento en la capacidad de producción interna de Irán le ha permitido enviar armamento (semipesado y blindado) y tanques T-72S a fuerzas paramilitares en Iraq, en suma, a su llegada a la presidencia Hassan Rouhani plasmó en el plan de gobierno la necesidad de la República Islámica de Irán de contar con autosuficiencia en la industria de defensa, la industria se ha desarrollado de forma significativa, ayudada por la cooperación en materia de transferencia tecnológica con China y Rusia, y en pasadas exhibiciones ha demostrado contar con Vehículos Aéreos No Tripulados, diversos tipos de morteros y misiles.[313]

Estados Unidos

Como actor con presencia militar significativa en Medio Oriente, es preciso analizar también la industria y tecnología militar estadounidense, dado que las tres compañías de defensa más grandes del mundo son estadounidenses. En 2001 su ingreso combinado sumó un total 100 000 millones de dólares, y juntas alcanzan un total de 400 000 personas a su cargo, se trata de Lockheed Martin, Northrop

[310] Rubin, *Óp.Cit.*

[311] Bruno, Greg (Julio 23, 2012). "Iran's Ballistic Missile Program". *Council on Foreign Relations*, pp. 8. [En línea]. Disponible en: <https://www.cfr.org/backgrounder/irans-ballistic-missile-program>.

[312] Keng Kuek Ser, *Óp. Cit*.

[313] Qaidaari, Abbas. (Marzo 24, 2016). "Is Iran becoming a major regional arms producer?". *Al-Monitor*. [En línea]. Disponible en: <http://www.al-monitor.com/pulse/en/originals/2016/03/iran-weapons-arms-experts-iraq-syria-lebanon.html>.

Grumman y Boeing, cuyos ingresos combinados representan el 1% de PIB de Estados Unidos.[314]

Lockheed Martin Corporation, con base en Maryland, es la contratista de defensa más grande del mundo, también es la mayor fabricante aviones militares, los cuatro principales sectores en los que concentra su actividad son: 1) Sistemas de Integración, conformado por subsistema de procesamiento de datos y guerra electrónica; 2) Aeronáutica, aeronaves de combate y de transporte, y 3) Servicios tecnológicos, administración y servicios logísticos. Entre el equipo fabricado por Lockheed Martin figuran los aviones de combate Falcon F-16 y el Hércules C-130, no obstante, la mayoría de sus ingresos se deben a la venta de Sistemas de Integración y Sistemas Espaciales, su principal comprador es el gobierno estadounidense.[315]

En Medio Oriente, Arabia Saudita figura entre la lista de clientes, las Fuerzas Armadas saudíes poseen aeronaves de combate como F-15, que son empleados en Yemen, además el gobierno saudí también ha iniciado negociaciones con General Atomics para la adquisición de drones Predator (con capacidad de combate).[316]

Northrop Grumman Corporation, con base en California, se convertirá en la segunda mayor contratista militar del mundo. Actualmente es la mayor constructora naval a nivel internacional y es conocida por manufacturar la aeronave más costosa jamás construida el B-2 *Spirit Stealth Bomber*. Northrop Grumman trabaja en seis principales sectores: 1) Sistemas electrónicos, que consististe en aviación de combate y vigilancia; 2) Tecnología de la información, en forma de sistemas computacionales; 3) Sistemas Integrados, referente a combate aéreo, guerra electrónica y gestión del campo de batalla; 4) Sistemas de Navegación, tanto militares y comerciales; 5) Submarinos y portaaviones de propulsión nuclear, y 6)

[314] Stanford University. (*s.f.*). "The U.S. Defense Industry and Arms Sales". [En línea]. Disponible en: <https://web.stanford.edu/class/e297a/U.S.%20Defense%20Industry%20and%20Arms%20Sales.htm>.
[315] *Ídem.*
[316] Mazzetti, Mark y Helene Cooper. (Abril 18, 2015). "Sale of U.S. Arms Fuels the Wars of Arab States". *The New York Times*. [En línea]. Disponible: <https://www.nytimes.com/2015/04/19/world/middleeast/sale-of-us-arms-fuels-the-wars-of-arab-states.html>

Componentes tecnológicos, como componentes electrónicos y ópticos. En entre el equipo militar que produce se encuentran las aeronaves B-2 *Spirit Stealth Bomber* y el F-14 *Tomcat*, no obstante, la mayor parte de sus ingresos se deben a los Sistemas Electrónicos y Tecnología de la Información.[317]

La compañía tiene contratos en Medio Oriente con Arabia Saudita y los Emiratos Árabes Unidos, en el caso de Arabia Saudita la relación comercial se remonta a cuatro décadas atrás, provee servicios de seguridad, ciberseguridad y comunicaciones, posee una presencia importante en la capacitación y entrenamiento de la milicia saudí, y trabaja con la empresa estatal Aramco en el desarrollo de protección estratégica avanzada; respecto a la relación con los Emiratos Árabes Unidos, la compañía es subcontratista de la Fuerza Aérea de los emiratos, encargada de la producción de aeronaves F-16 Block 60 Desert Falcon, también provee servicios de ciberseguridad, sistemas C4ISR, servicios logísticos y desarrolla sistemas autónomos.[318]

Boeing Company, con base en Illinois, es la tercera mayor contratista militar del mundo, es la mayor fabricante de satélites y jets comerciales del mundo, sus cinco principales unidades de producción son: 1) Aviones comerciales; 2) Sistemas de defensa integrados, 3) la Corporación Boeing Capital, de servicios financieros; 4) *Connexion* de Boeing, entretenimiento abordo, y 5) Gestión de tráfico aéreo, sistemas de control de tráfico aéreo.[319]

Sin embargo, la mayoría de sus ingresos provienen de las dos primeras unidades, entre el equipo militar producido por Boeing está la aeronave C-17 Globemaster.[320]En Medio Oriente, la compañía tiene presencia desde 1982 y posee lazos comerciales con Arabia Saudita, los Emiratos Árabes Unidos, Qatar, Kuwait y Egipto.[321]En 2016, el gobierno estadounidense aprobó la venta de jets de combate

[317] Stanford University, *Óp. Cit.*
[318] Media Net. (2017). "Profile a major organization: Nothrop Grumman Middle East". [En línea]. Disponible en: <http://dhow.com/organization-profile/38863828/northrop-grumman-middle-east/>.
[319] Stanford University, *Óp. Cit.*
[320] *Ídem*.
[321] Boeing. (2017). "Boeing Defense, Space & Security in the Middle East". [En línea]. Disponible en: <http://www.boeing-me.com/en/boeing-in-the-middle-east/about-boeing-in-the-middle-east/defense-space-and-security.page>.

a Kuwait y Qatar, específicamente de los jet F-15; los Boeing F/A-18E y F/A-18F Super Hornet, y el F/A-28 Tiger Hornet, la intercambio comercial con ambos países sumó un total de 7 mil millones de dólares, la aprobación se realizó en el marco de un intento por parte de Washington para consolidar su relación con los países del golfo, esto a pesar de las opiniones en contra por parte del gobierno israelí, específicamente respecto a la venta a Qatar. Tanto Qatar como Kuwait forman parte de la alianza de 34 naciones anunciada por Arabia Saudita para combatir a las fuerzas del Estado Islámico y Al Qaeda en Iraq, Siria, Libia, Egipto y Afganistán.[322]

Rusia

A pesar de que ha tenido una presencia militar histórica en la región, en los últimos años lazos en materia cooperación militar y transferencia tecnológica han incrementado. Las relaciones comerciales con Egipto, por ejemplo, no son nuevas, sin embargo, a partir de 2013 (ante la suspensión de ayuda militar por parte de Estados Unidos) las ventas en el sector militar se elevaron, lo cual se reflejó en la entrega de 50 aviones de combate Mig-29M (un avión-caza de cuarta generación) y 46 helicópteros de combate Ka-50.[323]

Los Emiratos Árabes Unidos por su parte, han adquirido equipamiento militar ruso, particularmente Sistemas de Defensa Aérea, mientras que Bahréin adquirió misiles antitanque 250 9M133 Kornet y AT-14. Empero, no hay duda de que la participación en Siria ha representado un punto en inflexión para la presencia de la industria militar rusa en Medio Oriente, antes del estallido de la guerra civil en Siria, se acordó la compra de un sistema de defensa aérea y de cazas rusos.[324]

Sin embargo, tras el inicio del conflicto la entrega de cazas se pospuso, quedando sólo el intercambio de municiones y repuestos. En el caso de Irán, Rusia suministró Sistemas de Defensa Aérea S-30 en 2016, [325]en adición entre 1992 y 2000 Rusia

[322] Shalal, Andrea. (Septiembre 28, 2016). "U.S. approves Boeing, Lockheed fighter jet sales to Gulf: sources". *Reuters* [En línea]. Disponible en: <http://www.reuters.com/article/us-boeing-fighters-gulf-idUSKCN11Y2TX>
[323] Salacanin, Stasa. (Marzo 13, 2017). "Weapons sales: The key to Russia's Middle East agenda". *The New Arab*. [En línea]. Disponible en: <https://www.alaraby.co.uk/english/indepth/2017/3/13/weapons-sales-the-key-to-russias-middle-east-agenda>
[324] *Ídem*.
[325] *Ídem*.

vendió a Irán 3 submarinos, cerca 200 tanques T-72 y aviones de combate Su-24 and 8 MiG-29.[326] Además Irán ha adquirido licencias para la producción de vehículos aéreos de combate T-72C y BMP-2 y ha recibido capacitación militar para el empleo de sistemas avanzados de armas. La cooperación militar Irán-Rusia es muy significativa, pues un número importante de oficiales militares iraníes asisten a academias rusas, con esta alianza ambos actores buscan contrarrestar la presencia militar dominante de Estados Unidos y Turquía en la región del Caspio. Los lazos de cooperación también involucran áreas de energía nuclear civil y exploración de petróleo y gas, lo cual genera fricciones con Estados Unidos e Israel, pues se presume que Moscú ayuda a Irán en el desarrollo de misiles balísticos.[327]

El avance de la tecnología militar rusa y su creciente participación en escenarios como Medio Oriente constituyen una señal de su resurgimiento como actor relevante en la dinámica internacional, pues tanto para Estados Unidos como para Israel la cooperación nuclear con Irán y las avanzadas capacidades en guerra electrónica son fuente preocupación, la actuación rusa no limita al sector industrial, su apoyo a las fuerzas kurdas en Siria generó tensiones con Turquía.[328]

3.3.1 Agencias de Inteligencia

El estudio de las actividades de inteligencia es un campo relativamente nuevo y difícil de explorar dada su naturaleza. Su enfoque e importancia en la seguridad nacional e internacional dificulta la disponibilidad de fuentes de información al respecto. Sin embargo, es uno de los sectores que más cambios ha experimentado a raíz de la innovación científica, además de poseer un importante rol en el desarrollo histórico de la región, pues dadas las tensiones y distensiones en la zona la industria de la inteligencia en Medio Oriente es una de las más desarrolladas en el mundo, dirigida no sólo a investigar las actividades de los Estados enemigos sino también las de los aliados. En adición, al ser una de las regiones que sufre mayor

[326] Rubín Center. (Marzo 3, 2011). "Russia's Military Involvement in the Middle East". *MERIA Journal*, Volumen 5, Número 1. [En línea]. Disponible en: <http://www.rubincenter.org/2001/03/antonenko-2001-03-03/>
[327] *Ídem*
[328] Sengupta, Kim. (Enero 29, 2016). "War in Syria: Russia's 'rustbucket' military delivers a hi-tech shock to West and Israel". *Independent*. [En línea]. Disponible en: <http://www.independent.co.uk/news/world/middle-east/war-in-syria-russia-s-rustbucket-military-delivers-a-hi-tech-shock-to-west-and-israel-a6842711.html>

número de ataques terroristas los servicios de inteligencia resultan ser uno de los sectores más activos, actuando tanto hacia el interior como hacia fuera de los Estados. [329]

La presencia de actividades de inteligencia en la zona se remonta a los antiguos imperios. Desde Egipto a Mesopotamia la recolección, análisis y difusión de información ha sido una función activa tanto en tiempos de paz como en tiempos de guerra. Durante el orden otomano, la inteligencia se convirtió en un pilar para mantenimiento del imperio, derivando incluso en alianzas con la Monarquía austrohúngara. Sin embargo, no fue sino hasta el inicio de la Primera Guerra Mundial que los aparatos de inteligencia regionales comenzaron a expandirse, al tiempo en el que la inteligencia de países como Francia, Gran Bretaña, Italia, entre otros, proliferaron también en la zona. Tras el desmantelamiento del imperio, el nuevo orden geográfico regional dio origen al surgimiento de movimientos de resistencia y organizaciones terroristas, por lo que el fin de la Primera Guerra Mundial representó un parteaguas en los servicios y actividades de inteligencia en Medio Oriente.[330]

El reordenamiento interno político y administrativo que sufrieron Estados nacientes como Iraq, Irán y Turquía condujeron al establecimiento de nuevos organismos de seguridad, también aumentó la presencia de países como Reino Unido y Francia. Así, ante la presencia de organizaciones extranjeras en la zona, la inestabilidad heredada de los Guerras Mundiales y los esfuerzos por el establecimiento de un frágil orden comenzaron a expandirse y renovarse las agencias de inteligencia en la región.[331]

Con el paso del tiempo, y hasta ya entrado el siglo XXI, se desarrollaron también órganos especializados en ciberseguridad, incorporándose a la comunidad de inteligencia de diversos países (ver tabla 8).

[329] Kahana, Ephraim y Muhammad Suwaed. (2009). Historical Dictionary of Middle Eastern Intelligence. Estados Unidos: The Scarecrow Press, Inc.
[330] *Ídem.*
[331] *ídem*

TABLA 8 AGENCIAS DE INTELIGENCIA QUE OPERAN EN MEDIO ORIENTE

PAÍS	NOMBRE	FECHA CREACIÓN	DESCRIPCIÓN
ARABIA SAUDITA	Maslahat Al-Istikhbarat Al-Aammah (*General Intelligence Department)*	**1955**	El *General Intelligence Directorate*, depende directamente del Rey, es responsable de la recolección y análisis de inteligencia. En adición, lleva a cabo funciones de coordinación de tareas y reportes de todas las agencias de inteligencia incluido el Ministerio de Defensa y de Aviación y la Guardia Nacional. (Global Security, 2016) **Ciberseguridad:** No existe información disponible al respecto, pues los portales electrónicos relacionados con el Departamento General de Inteligencia no están funcionamiento desde 2010. Sin embargo, existe información que refiere a la colaboración con corporaciones como Northrop Grumman, especialmente orientada a la mejora de capacidades de defensa. Northrop Grumman también trabaja con la Guardia Nacional y con ARAMCO (empresa estatal de petróleo y gas). (Northrop Grumman Corporation: 2017).
EGIPTO	Military Intelligence and Reconnaissance Administration Idarat El Mukhabarat El Ḥarbiya Wel Istitla	**1952**	Las agencias de inteligencia nacional de Egipto comprenden: 1) El Servicio General de Inteligencia (Al-Mukhabarat AlAmma); 2) La Administración de Inteligencia y Reconocimiento Militar (AlMukhabarat Al-Harbeya); 3) El Servicio de Seguridad Nacional (Mabaheth Alamn Alwatany), y 4) La Autoridad de Control Administrativo (Ar-Raqabaal-Idareya). **Ciberseguridad:** Existen reportes que sugieren la existencia de un Departamento de Investigación Técnica (TRD, *Technical Research Department*), que forma parte de los Servicios de Inteligencia General de Egipto. Al parecer, el TRD se encarga de ejecutar operaciones de vigilancia a través de tecnología adquirida de compañías como Nokia Siemens Networks (NSN) y Hacking Team. Posee un centro de monitoreo de comunicaciones, un sistema de gestión de intercepciones y un spyware altamente intrusivo. (Privacy International: 2016)
ESTADOS UNIDOS	United States Intelligence Community	**1981**	La Comunidad de Inteligencia de Estados Unidos comprende, además del Director de Inteligencia Nacional, 16 organizaciones (Stone:2013). la estructura de la organización incluye a los Gestores Nacionales de Inteligencia (*National intelligence managers* NIMs) que son: 1) La Agencia Central de Inteligencia (CIA), 2) la Agencia de Inteligencia de Defensa (DIA), 3) la Subdivisión de Seguridad Nacional (FBI), 4) la Agencia Nacional de Inteligencia Geoespacial (NGA), 5) la Oficina Nacional de Reconocimiento (NRO), 6) la Agencia Nacional de Seguridad (NSA) Estas seis agencias se encargan de integrar a la Comunidad de Inteligencia y realizan actividades enfocadas en determinadas zonas geográficas y temas. (Stone:2013) **Ciberseguridad:** 23 de junio de 2009 se creó el Comando Cibernético de Estados Unidos (USCYBERCOM, por sus siglas en inglés), ubicado en Fort Meade. El comando se encarga de planear, coordinar, integrar y realizar actividades para dirigir las operaciones y la defensa de determinadas redes de información del Departamento de Defensa, también se encarga de preparar y dirigir un amplio espectro de operaciones militares en el ciberespacio con el fin de permitir la libertad de acción en todos los dominios. (Strobel:2015)
IRÁN	Organización de Inteligencia y Seguridad Nacional (Sazeman-i Ettelaat va Amniyat-i Keshvar, SAVAK)	**1957**	La comunidad de inteligencia de la República Islámica de Irán está conformada por: 1) el Consejo Supremo de Seguridad Nacional, 2) el Cuerpo de Guardia Revolucionaria Islámica, también conocida como Pasdaran, 3) el Ministerio de Inteligencia y Seguridad Nacional, 4) las Fuerzas Quds, que forma parte de los Pasdaran, que conforman una Unidad de Fuerzas Especiales. (Banerjea:2015). **Ciberseguridad:** En 2010 Irán creó el Comando de Defensa Cibernética (Gharargah-e Defa-e Saiber) bajo la Organización de Defensa Pasiva Artesh (que son las Fuerzas Armadas). En 2012, el segundo líder supremo iraní, Alí Jamenei, decretó un Consejo Supremo del Ciberespacio (Shora-ye Ali-ye Fazo-ye Majazl) con el fin de coordinar las agencias gubernamentales iraníes con responsabilidades relacionadas con la seguridad cibernética. (Wege:2015)
ISRAEL	Israeli Intelligence Community	**1948**	La comunidad de inteligencia de Israel está dividida en cuatro componentes: 1) La Dirección de Inteligencia Militar, AMAN, es una rama dentro de las Fuerzas de Defensa de Israel (IDF, *Israel Defense Forces*), 2) la Agencia de Seguridad de Israel,

			SHABRAK 3) el Instituto Central de Inteligencia y Seguridad, Mossad, 4) el Centro de Investigación Política del Ministerio de Relaciones Exteriores. **Ciberseguridad:** En 2013, las IDF consolidaron todos los aspectos de su conocimiento situacional del plano cibernético en una organización que está vinculada con: 1) el sistema Tehila (de carácter civil, es la infraestructura gubernamental de comunicaciones vía Internet); 2) el proyecto de gobierno electrónico, y 3) el recientemente establecido National Cyber Bureau. (Raska:2015).
RUSIA	Comisión Extraordinaria Chrezvycháinaya Komíssiya	**Diciembre 1917**	Tras el fracaso del Golpe de Estado de agosto de 1991 la KGB fue seccionada en varios servicios, los cuales reportaban directamente al presidente. Los servicios más importantes creados a partir de la KBG son: 1) el Servicio de Inteligencia Exterior de Rusia (SVR), 2) el Servicio Federal de Seguridad, FSBRF, 3) la Agencia Federal de Comunicación e Información Gubernamental (FAPSI), 4) Servicio Federal de Control Técnico y de Exportación sustituyó al Servicio Técnico Estatal (GTK), y 5) el Servicio Federal de Protección (OFS) y la Dirección Principal de Programas Especiales del presidente (GUSP) (Pringle:2010) **Ciberseguridad:** Rusia cuenta con un Centro de Respuesta Inmediata a Ataques Cibernéticos, encargado de coordinar las acciones de las compañías y las agencias gubernamentales en el campo de la detección, prevención y supresión de actividades ilegales relacionadas con los recursos en red de los cuerpos gubernamentales conocido como Russian Gov CERT. Además, existe otro centro de respuesta conocido como RU-CERT orientado a la seguridad informática no relacionada con organismos gubernamentales ofrece asesorías a persona dentro y fuera del país para identificación, prevención y represión de ataques informáticos. (ITU:2015)
SIRIA	Dirección General de Inteligencia Idarat al-Mukhabarat al-Amma	**1971**	Las agencias militares y de inteligencia en Siria ha tenido un papel determinante en la política interna y en la política exterior de la república árabe. Se estima que el país cuenta con 15 servicios de inteligencia y seguridad, sin embargo, dada la naturaleza de las organizaciones no existe información detallada al respecto. De forma general la comunidad de inteligencia está conformada por cuatro principales organizaciones: 1) el Departamento de Inteligencia Militar, 2) la Dirección de Seguridad Política, 3) la Dirección General de Inteligencia, 4) la Dirección de Inteligencia de la Fuerza Aérea. Todas estas organizaciones operan bajo la supervisión del Consejo Nacional de Seguridad, cuyo director reporta directamente al presidente. (Hendi:2017). Históricamente, las agencias de inteligencia sirias han sido influenciadas por el modelo del mandato francés, que creó el Estado sirio moderno. (Kahana y Suwaed: 2009) **Ciberseguridad:** El gobierno sirio cuenta con una Ley de comunicación en red y control de la delincuencia informática (promulgada en 2012), sin embargo, no posee con ningún instrumento legal especialmente dirigido a la ciberseguridad. La república árabe cuenta con una Agencia Nacional de Servicios de Red, creada en 2009, encargada de la regulación del uso de nombres de dominio en Internet y redes computacionales en Siria. (NANS: *s.f.*) También se ha reconocido como la autoridad responsable en el ámbito de la ciberdefensa. (ITU:2014)
TURQUÍA	Servicio de Seguridad Nacional Milli Emniyet Hizmeti, MEH (MAH)	**6 de enero de 1926**	El Servicio de Seguridad Nacional fue establecido en la República de Turquía por Mustafá Kemal Atatürk. Así, se creó el 6 de junio de 1926 el Milli Emniyet Hizmeti Riyaseti liderada por Mariscal Fevzi Cakmak (MIT:2016) Posteriormente, la Agencia Nacional de Inteligencia (*Milli İstihbarat Teşkilatı*, MIT) fue establecida en reemplazo del Servicio de Seguridad Nacional bajo la Ley 644, que entró en vigor el 22 de julio de 1964, tras el golpe de Estado del 12 de septiembre. Actualmente el MIT está conformado por: 1) la Dirección de Análisis Estratégico, 2) la Dirección de Contrainteligencia, 3) la Dirección de operaciones externas, 4) la Dirección de Inteligencia y Seguridad, 5) la Dirección de Inteligencia electrónica y técnica, 6) la Dirección Señales de Inteligencia. (MIT:2016) **Ciberseguridad:** Hasta octubre de 2012 la autoridad responsable de la seguridad cibernética fue la agencia TUBITAK, a partir del 20 de octubre de 2012, la autoridad se trasladó a el Ministerio de Transporte, Asuntos Marítimos y Comunicaciones. El mismo año también se estableció una Junta Nacional de Seguridad Cibernética, de la que forman parte el Ministerios de Asuntos Interiores, el Ministerios de Asuntos Interiores, el Ministerio de Defensa, y diversas subsecretarias como la Agencia Nacional de Inteligencia, la Comisión de Comunicaciones y Telecomunicaciones,

			entre otras. Además, se crearon dos Centros de Respuesta a Ataques Cibernéticos una bajo responsabilidad gubernamental (TR-BOME) y la otra perteneciente a TUBITAK (ULAK-CSIRT). (Şentürk, Çil y Sağıroğlu:2012)

Fuente: Elaboración propia

Durante el transcurso de la Guerra Fría, Medio Oriente se convirtió en el escenario de choque de dos ideologías, de esta forma servicios de inteligencia de ambos bandos (tanto de Estados Unidos como de la Unión de Repúblicas Soviéticas Socialistas) comenzaron a ejercer influencia en la zona, ya sea a través de financiamiento o entrenamiento de grupos disidentes para combatir a las fuerzas rivales. Así, por ejemplo, la URSS proporcionó entrenamiento a fuerzas disidentes en Iraq, Siria, la ex República Democrática Popular de Yemen y Libia, como respuesta se crearon organizaciones rivales o con el fin de verificar la autonomía de los servicios de inteligencia nacionales, lo que propició el faccionismo. En algunos casos, como en Siria e Iraq los puestos de coordinación y supervisión de inteligencia se otorgaron a parientes cercanos, como Hafez Al Assad lo hizo entregando la jefatura a su hermano Rifat Al Assad. Por su parte, la inteligencia estadounidense que comenzó a ocupar un lugar significativo en la región durante la Guerra Fría trabajó en cooperación con el Mossad israelí frente a la amenaza del terrorismo en la escena internacional.[332]

Con la posibilidad del desarrollo de capacidades nucleares por parte de Irán y Siria, y ante los efectos del 9/11 la actividad de inteligencia estadounidense en Medio Oriente no sólo se intensificó, sino que recibió la cooperación de países como Libia y Sudán. En adición, la revolución informática ha trasformado la estructura, las funciones y el financiamiento de las organizaciones inteligencia que operan en Medio Oriente, la proliferación de alta tecnología y de medios de comunicación ha incentivado operaciones de inteligencia, contrainteligencia y desinformación además de dar paso al empleo de la guerra cibernética.[333]

[332] *ídem*
[333] *Ídem.*

3.3.2. Centros de Respuesta a Ataques cibernéticos

Los Centros de Respuesta a Ataques Cibernéticos, también conocidos como Centros de Respuesta a Incidentes de Seguridad Computacionales (CSIRT, por sus siglas en inglés *Computer Security Incident Response Teams*) consisten en un grupo de técnicos especialmente entrenados para resolver y gestionar incidentes informáticos de alto impacto, su objetivo es dar efectiva y rápida respuesta a los incidentes que puedan ocurrir, un CSIRT debe proteger infraestructura crítica y procurar la continuidad de los servicios principales de dicha estructura.[334]

La velocidad en la respuesta constituye el eje central del trabajo de los CSIRT, ya que una repuesta rápida, precisa y eficaz puede minimizar el daño general a las finanzas, al hardware y al software de la infraestructura atacada, otro de los elementos que ayudan al correcto funcionamiento de los CSIRT es el reforzamiento de software y de la infraestructura para disminuir el número de incidentes.[335]

Actualmente, los CSIRT constituyen un pilar importante para la ciberseguridad internacional. En adición se ha conformado un grupo de expertos del sector gubernamental orientados al desarrollo en el campo de la información y comunicación en el contexto de la seguridad internacional, conocido como UNGGE (por sus siglas en inglés *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*) que encabeza los esfuerzos de la comunidad internacional en la negociación de normas de ciberseguridad globales bajo el auspicio de la Organización de Naciones Unidas.[336]En suma, se ha alentado la cooperación internacional en materia de intercambio de datos, donde las CSIRT ocupan también un lugar primordial, todo

[334] Carozo Blumsztein, Eduardo. (Marzo 5, 2013). "Centro de Respuesta a Incidentes Informáticos… ¿Para qué?". *Seguridad*. [En línea]. Disponible en: <https://revista.seguridad.unam.mx/node/2168>

[335] Rouse, Margaret. (Agosto, 2012). "Computer Security Incident Response Team (CSIRT)". *TechTarget*. [En línea]. Disponible en: <http://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT>

[336] Morgus, Robert; Isabel Skierka; Mirko Hohmann, y Tim Maurer. (Noviembre 19, 2015). "National CSIRTs and Their Role in Computer Security Incident Response". *GPPi & New America*. [En línea]. Disponible en: <http://www.gppi.net/publications/data-technology-politics/article/national-csirts-and-their-role-in-computer-security-incident-response/>

ello para responder a las amenazas cibernéticas crecientes y persistentes en un mundo interconectado.

Los ataques cibernéticos son una amenaza de carácter mundial, sin embargo, Medio Oriente es una región especialmente afectada por este tipo de prácticas. En suma, dado que tanto las principales potencias militares como actores no estatales han desarrollado capacidades significativas en el ámbito de la ciberguerra, se hace cada vez más urgente la estructuración de tácticas capaces de responder a esta relativamente nueva amenaza. Respecto a la presencia de Centros de Respuesta a Ataques Cibernéticos en Medio Oriente, es posible afirmar que la mayoría de los países cuenta con CSIRT (ver tabla 9), los cuales comenzaron a desarrollarse a partir de 2005. Estos CSIRT se encargan de promover la cultura de la seguridad cibernética en el sector industrial, responden a las necesidades de la población civil y orientan a cualquier interesado en desarrollar medidas para la protección de infraestructura y sistemas computacionales, por lo que el funcionamiento de estos CSIRT depende en buena medida de la cooperación entre el sector privado y estatal.[337]

En el caso de Israel no existe información abundante referente a su Centro de Respuesta a Ataques Cibernéticos. Sin embargo, Tel Aviv cuenta con una Oficina Cibernética Nacional, y actualmente es uno de los Estados más avanzados en el plano de la ciberseguridad. Al respecto refiere Dudu Mimran, directora del departamento de tecnología de la Universidad de Ben-Gurion: “El ambiente desafiante que Israel enfrenta en el mundo físico en Medio Oriente tiene proyecciones también en el mundo cibernético”.[338]

En este sentido, las amenazas no sólo se dirigen a Israel, pues países como Arabia Saudita, Irán, Iraq, Siria, entre otros, también han sido vulnerados en su seguridad cibernética, por ello el desarrollo de CSIRTs constituye una pieza clave para la seguridad, no sólo en el plano civil sino en el militar.

[337] Suciu, Peter. (Septiembre 1, 2015). “Why Israel dominates in cyber security”. *Fortune*. [En línea]. Disponible en: <http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/>
[338] *Ídem.*

Otro país con importantes avances en la materia es la República de Turquía, pues ha desarrollado una estrategia de ciberseguridad nacional que no sólo contempla la creación de un CSIRT, sino el establecimiento de otros centros de respuesta especializados en cada ámbito (en la estructura gubernamental y la infraestructura crítica) además de contemplar la coordinación entre todas estas entidades para mantener la ciberseguridad de la nación.[339]

En el plano regional la Organización de Cooperación Islámica (OIC, por sus siglas en inglés *Organisation of Islamic Cooperation*), creada en 1969 y con sede en Arabia Saudita, propuso en junio de 2005 la creación de CSIRTs entre los miembros que la componen (aquellas naciones de confesión musulmana) en el marco de la Reunión Anual de los Gobernadores del Banco Islámico de Desarrollo. Como resultado se estructuró un grupo de trabajo orientado a cooperar con los países miembros y se creó OIC-CERT, lo cual representó un avance muy significativo en la materia, pues sólo un año después, en julio de 2006, se llevó acabo la primera reunión del grupo de trabajo en Kuala Lumpur, Malasia.[340]

Pese a todos los esfuerzos en torno a la ciberseguridad, aún existen naciones que requieren desarrollar o mejorar tanto prácticas como normas internas en la materia, tal es el caso de Libia, Líbano, Siria, Palestina, Iraq, Kuwait y Bahréin. Kuwait, por ejemplo, no cuenta con un organismo dedicado a la ciberseguridad, ni con una estrategia nacional.[341] Mientras que en Iraq la ley sobre cibercrimen fue revocada y no existe ninguna agencia nacional dedicada a la seguridad cibernética, según datos de 2013.[342]

---

[339] Emre Karabulut, Yunus (*et.al*) (Diciembre, 2015). "Characteristics of Cyber Incident Response Teams in the World and Recommendations for Turkey". *Balkan Journal of Electrical & Computer Engineering*. [En línea]. Disponible en: <https://www.re searchgate.net/publication/289118287_Characteristics_of_Cyber_Incident_Response_Teams_in_the_World_and_Recommendations_for_Turkey>.

[340] OIC-CERT. (2017). History. [En línea]. Disponible en: <https://www.oiccert.org/en/history.html#.WSsS1WiGPIU>.

[341] ITU. (Diciembre 2013). "Cyberwellness Profile State of Kuwait ". [En línea]. Disponible en: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Kuwait.pdf>.

[342] ITU. (Diciembre 2013). "Cyberwellness Profile Republic of Iraq". [En línea]. Disponible en: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Iraq.pdf>.

TABLA 9 CENTROS DE RESPUESTA A ATAQUES CIBERNÉTICOS EN MEDIO ORIENTE

PAÍS	AÑO DE CREACIÓN	DENOMINACIÓN	DESCRIPCIÓN
Túnez	2007	Tunisian Computer Emergency Response Team (tunCERT)	Proporciona asistencia y apoyo al *Centre d'assistance et de Soutien en Matière de Sécurité Informatique* (Equipo de Respuesta a Emergencias Cibernéticas) creada en 1999. También ofrece asistencia gratuita tanto a ciudadanos como a profesionales en materia de seguridad cibernética.
Egipto	2009	Egyptian Computer Emergency Readiness Team (EG-CERT)	Fue creada por la Autoridad Reguladora Nacional de Telecomunicaciones (NTRA, por sus siglas en inglés, *National Telecom Regulatory Authority*) proporciona respuesta a incidentes de seguridad cibernética, actúa en colaboración con el gobierno, entidades financieras y cualquier otra infraestructura crítica.
Turquía	2013	National Cyber Incident Intervention (USOM)	Fue creada por la Institución de Ciberseguridad de Turquía (*Cyber Security Institution of Turkey*), posterior a su fundación el gobierno turco también consideró el establecimiento de centros de respuesta sectoriales e institucionales, los cuales se ocuparían de proteger ministerios e instituciones gubernamentales, mientras que los sectoriales protegerían a la industria a la infraestructura crítica.
Irán	2005	Team Coordination Center Computer Emergency Response (MAHER)	Se trata de un equipo de asistencia y coordinación calificada de respuesta a incidentes cibernéticos, trabaja en colaboración con el Ministerio de Tecnologías de la Información y Comunicación, y con las organizaciones de seguridad nacional para mantener la integridad del ciberespacio. Entre sus cargos y responsabilidades está la cooperación regional e internacional en la materia.
Israel	No disponible	Israel's Computer Emergency Response Team (IL-CERT)	No existe información clara al respecto, la página web oficial refiere que es un centro de carácter civil dedicado a detectar incidentes relacionados con la seguridad de la información y ciber-eventos; que no está afiliado al gobierno, y que es una organización sin fines de lucro. Sin embargo, otras fuentes sostienen que forma parte de la Oficina Cibernética Nacional de Israel (INCB, por sus siglas en inglés *Israel National Cyber Bureau*).
Arabia Saudita	2006	Computer Emergency Response Team (CERT-SA)	Tiene como objetivo aumentar y cultivar el conocimiento, gestión, prevención, coordinación y respuesta de incidencias de ciberseguridad a nivel nacional. Es miembro del OIC-CERT, que se deriva de la Organización de Cooperación Islámica y se compone de los CERTs de los países que la conforman como: Azerbaiyán, Bangladesh, Brunei, Costa de Marfil, Egipto, Irán, Jordania, Kazajistán, Libia, Malasia, Marruecos, Nigeria, Omán, Paquistán, Sudán, Siria, Túnez, Turquía, Emiratos Árabes Unidos, Reino Unido, Estados Unidos y Yemen. Además, se dedica a proporcionar recomendaciones a corto plazo para tratar problemas de ciberseguridad, y brindar orientación para la protección y recuperación de sistemas computacionales.
Qatar	2005	Qatar Computer Emergency Response Team	Es una organización patrocinada por el gobierno, bajo el auspicio del Consejo Supremo de Tecnología de la Información y Comunicación (ictQATAR, por sus siglas en

		(Q-CERT)	inglés *Supreme Council of Information and Communication Technology*). Se trata de una organización diseñada para localizar y responder de forma proactiva y reactiva a los riesgos que pueda surgir del uso de las tecnologías.
Emiratos Árabes Unidos	2008	Computer Emergency Response Team (aeCERT)	El equipo se estableció para mejorar normas y prácticas de seguridad de la información y proteger la infraestructura de las tecnologías de información de los Emiratos Árabes Unidos. En adición, se encarga de mejorar las leyes de seguridad cibernética, así como la cooperación con CSIRTs nacionales e internacionales.

Fuente: Elaboración propia con datos de Software Engineering Institute (2017); Emre Karabulut *et.al* (2015), y Cyber Security Intelligence (*s.f.*)

3.4. EJÉRCITOS ELECTRÓNICOS Y COMANDOS ESPECIALES

Si existe una evidencia del cambio en la naturaleza de la guerra en el marco de la era informatizada esa es el surgimiento de ejércitos electrónicos, también conocidos como armadas cibernéticas, que consisten en un grupo de expertos en informática que actúan en el ámbito militar con el fin de prevenir, contener y contrarrestar un ataque cibernético, su trabajo también implica el empleo de armas cibernéticas con el fin de dirigir operaciones militares contra el adversario.

Estos nuevos actores operan en la red beneficiados por el anonimato y las dificultades alrededor del proceso de atribución de responsabilidades característica de la red de redes, por ello tanto Estados como actores no estatales han recurrido al empleo de este tipo de elementos, mientras que otros han surgido genuinamente en la red, es decir no poseen ningún vínculo con el espacio tangible por lo que su actuación se realiza básicamente en el espacio cibernético.

Al respecto, existen dos tipos actores con capacidades de combate en el espacio digital:

1.- Ejércitos cibernéticos: que se subdividen en dos categorías, los que forman parte de la estructura de un estado (o su presume que lo hacen) y aquellos conformados por hackers patrióticos que se autodenominan ejércitos electrónicos como es el caso del Ejército Electrónico Sirio (SEA, por sus siglas en inglés S*yrian Electronic Army*).

2.- Los Comandos especiales, forman parte de la estructura militar, consisten en un reducido grupo de fuerzas especiales dedicadas a combatir las amenazas cibernéticas como es el caso del Ciber-Comando estadounidense creado en 2009.

Debido a que la participación militar en el ciberespacio constituye una actividad no regulada, al igual que el uso de ciberarmamento, es difícil que un Estado declare abiertamente que cuenta con una unidad militar especializada en ciberguerra, que ejecuta acciones mediante el empleo de armas cibernéticas y que se encuentra activa, pues ello significaría aceptar que se actúa fuera del margen de la ley. Por ello, es complicado determinar si se trata de una organización externa que recibe financiamiento por parte de un Estado, si forma parte de la arquitectura militar y actúa de forma encubierta en el espectro cibernético, o si se trata solamente de un grupo de hackers patrióticos.

Existen casos en los que diversas naciones se acusan unas a otras de lanzar ataques cibernéticos e incluso de poseer una unidad militar especial, por ejemplo, la República Popular China ha sido constantemente acusada de ejecutar labores de ciberespionaje contra industrias e incluso contra embajadas de todo el mundo, se le ha acusado también de poseer un equipo especializado en ciberguerra denominado "Unidad 61398" que presuntamente forma parte del Ejército Popular de Liberación.[343]

Particularmente en Medio Oriente, Israel es conocido por poseer una de las organizaciones militares más avanzadas en el ámbito tecnológico denominada "Unidad 8200". La Unidad 8200 es considerada una de las mejores agencias militares de inteligencia en todo el mundo y forma parte oficialmente de las Fuerzas Armadas de Israel.[344]El papel de la unidad en la seguridad nacional es significativa, pues se estima que provee el 90% del material de inteligencia, en adición se ha

[343] Mandiat. (*s.f.*). APT1: Exposing One of China's Cyber Espionage Units. [En línea]. Disponible en: <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>

[344] Enlace Judío. (Agosto 28, 2013). "La mejor escuela sobre el planeta es la unidad 8200 del Ejército de Israel". [En línea]. Disponible en: <http://www.enlacejudio.com/2013/08/28/la-mejor-escuela-sobre-el-planeta-es-la-unidad-8200-del-ejercito-de-israel/>

sugerido la existencia de un subsector conocido como Unidad 81 dedicada al desarrollo de tecnología para labores de inteligencia.[345]

Por otra parte, está el Ejército Electrónico Iraní, que consiste en un grupo de hackers patrióticos que actúan a favor del presidente en turno[346]. Asimismo, los Cuerpos de la Guardia Revolucionaria Islámica (IRGC, por sus siglas en inglés *Islamic Revolutionary Guard Corps*) han declarado tener uno de los ejércitos cibernéticos más grandes del mundo,[347]además se estima que en noviembre de 2010 el Consejo Cibernético Basij (BCC, por sus siglas en inglés *Basij Cyber Council*) capacitó a cerca de 1 500 guerreros cibernéticos. El potencial iraní es tan grande que expertos como Ian Bremmer consideran que en el futuro las capacidades cibernéticas de Irán serán igual de preocupantes que el programa nuclear.[348]

En el caso Siria, surge el Ejército Electrónico Sirio (SEA, por sus siglas en inglés *Syrian Electronic Army*) que está conformado por hackers patrióticos a favor de Bashar Al-Assad. Las actividades del SEA van desde hackeos a páginas web de medios de comunicación como Al Jazeera, BBC News, Orient TV y Al Arabia hasta ataques cibernéticos intrusivos e incluso actividades de ciberespionaje. Según diversas investigaciones la SEA posee vínculos con el gobierno de Bashar Al Assad desde que éste participó en la *Syrian Computer Society* (SCS).[349]

Adicionalmente, el grupo creó un portal en línea en donde mostraba documentos confidenciales de servidores gubernamentales en Turquía, Qatar y Arabia Saudita.

---

[345] Behar, Richard. (Marzo 25, 2017). "Así funciona la fábrica secreta de startups de Israel". *Forbes*. [En línea]. Disponible en: <http://forbes.es/actualizacion/7575/asi-funciona-la-fabrica-secreta-de-startups-de-israel>

[346] Naar, Ismaeel. (Enero 23, 2017). "Why does the GCC need its own electronic army?". *Al Arabiya English*. [En línea]. Disponible en: <http://english.alarabiya.net/en/media/digital/2017/01/23/Why-does-the-GCC-need-its-own-cyber-army-.html>

[347] Waqas, Amir. (Octubre 18. 2013). "Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World". *Hack Read*. [En línea]. Disponible en: <https://www.hackread.com/iran-biggest-cyber-army-israel/>

[348] Bertrand, Natasha. (Marzo 27, 2015). "Iran is building a non-nuclear threat faster than experts 'would have ever imagined'". *Bussines Insider*. [En línea]. Disponible en: <http://www.businessinsider.com/irans-cyber-army-2015-3>

[349] Grohe, Edwin. (2015). "The Cyber Dimensions of the Syrian Civil War". *The Johns Hopkins University Applied Physics Laboratory*. [En línea]. Disponible en: <http://www.jhuapl.edu/ourwork/nsa/papers/TheCyberDimensionsoftheSyrianCivilWar.pdf>.

La plataforma proporcionaba evidencia que demostraba el respaldo de dichos países a la oposición en Siria, incluidas organizaciones terroristas. Con el fin de obtener los documentos, el SEA hackeó agencias gubernamentales turcas, incluyendo la oficina del Primer Ministro y del Presidente, así como el Comando de la Fuerza Aérea entre marzo de 2009 y noviembre de 2012.[350]

Yemen también cuenta con ejército en línea, se trata de la Ciberarmada Yemení (YCA, por sus siglas en inglés *Yemen Cyber Army*), un grupo de hackers favorable a la facción chií, que, en el marco de la Guerra Civil Yemení, se posiciona como un grupo a favor del ex presidente Ali Abdullah Saleh. Al igual que el SEA, el YCA obtuvo documentos confidenciales de los Ministerios de Exterior, de Interior y de Defensa del gobierno saudí, los cuales fueron incorporados a la página de filtraciones *WikiLeaks*. El ataque cibernético le dio el control de 3 000 ordenadores y servidores, así como el acceso a cuentas de correo electrónicos de funcionarios del gobierno de Arabia Saudita.[351]Se ha sugerido que el YCA recibe apoyo del gobierno iraní y, que incluso, podría ser el responsable del ataque a la empresa estatal de petróleo y gas Aramco en 2012.[352]

Egipto, por su parte, cuenta también con una armada electrónica, conformada por un grupo de hackers inspirado en el SEA. La *Egyptian Cyber Army* (ECA) ha emprendido acciones en el ciberespacio para contrarrestar la propaganda del Estado Islámico en línea. De acuerdo con declaraciones en línea, la armada está conformada por civiles, algunos de los cuales posee experiencia militar y policial, y todos sus integrantes son simpatizantes del gobierno de Abdelfatah Al-Sisi. Entre

[350] MEMRI. (Febrero 11, 2015).“Turkish Media Reports: Syrian Electronic Army (SEA) Leaks Official Confidential Turkish Documents From 2012, Exposing Turkish, Saudi, And Qatari Support for Terrorist Groups”. *Special Dispatch No.5964*. [En línea]. Disponible en: <https://www.memri.org/reports/turkish-media-reports-syrian-electronic-army-sea-leaks-official-confidential-turkish>.

[351] Fars News Agency. (Mayo 21, 2015). “Saudileaks 2: Yemen Cyber Army Releases Hacked Contents”. [En línea]. Disponible en: <http://en.farsnews.com/newstext.aspx?nn=13940231001097>.

[352] The Cyber & Jihad Lab. (Julio 21, 2015). “Experts Suggest Yemen Cyber Army Could Actually Be Iranian”. En línea]. Disponible en: <http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/experts-suggest-yemen-cyber-army-could-actually-be-iranian/>.

sus objetivos también está defender al gobierno egipcio de la Hermandad Musulmana o cualquier otra oposición.[353]

Los casos de armadas cibernéticas en Medio Oriente son numerosos, en la mayoría de los casos se trata de hackers patrióticos que actúan de forma independiente, aunque existen acusaciones que les vinculan con sus respectivos gobiernos e incluso con otras armadas (como es el caso del ejército electrónico yemení). El robo de información confidencial, los ataques a infraestructura crítica y las operaciones de ciberespionaje los colocan como una amenaza latente para la seguridad de los Estados en la región. Además de los casos ya analizados, han surgido otras armadas cibernéticas cuya presencia en el ciberespacio se activa de forma periódica y, al contrario de los casos antes expuestos, no han ejecutado un ataque a gran escala en contra de sistemas o infraestructura crítica a algún país en la región, tal es el caso del *Algerian Cyber Army*, *Palestine Cyber Army*, *Afghan Cyber Army* y *Turkey Cyber Army*.

Además, existen actores extra-regionales con presencia en línea como Estados Unidos, que a través de su Comando Cibernético ha emprendido acciones para contrarrestar la actividad del Estado Islámico en web.

Las actividades del USCYBERCOM en Medio Oriente se dedican a combatir al Estado Islámico en varios frentes, entre los que figuran: 1) las operaciones de reclutamiento y propaganda, 2) atacar las vías de comunicación dentro de la organización terrorista, y 3) impedir las transacciones financieras. El anuncio de la operación se realizó de manera cuidadosa pues, aunque las medidas cibernéticas refuerzan el combate a Daesh, el gobierno estadounidense hizo referencia por primera vez al empleo de ciberarsenal.[354]

[353] Franceschi-Bicchierai, Lorenzo. (Noviembre 23, 2014). "Egyptian Cyber Army: The hacker group attacking ISIS propaganda online". *Mashable*. [En línea]. Disponible en: <http://mashable.com/2017/05/23/aerones-drone-jump/#VY9LW.beNmqI>.

[354] Sanger, David E. (Abril 24, 2016). "U.S. Cyberattacks Target ISIS in a New Line of Combat". *The New York Times*. [En línea]. Disponible en: <https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0>.

3.5. OPERACIONES CONJUNTAS

Ante el desarrollo tanto de capacidades como de armamento cibernético el peor de los escenarios posibles en un contexto de guerra es el empleo conjunto de tácticas militares convencionales y de potencial cibernético. El surgimiento de una guerra “multi-espectro” que se libre tanto en el espacio tangible como en el virtual configura una de las más grandes preocupaciones para los expertos en seguridad. Aunque, no se trata de una nueva posibilidad, ya que la táctica ha sido empleada con grados de afectación limitados. En su momento, su ejecución se enfocó en la inhabilitación de sistemas de defensa aérea durante la fase inicial de una operación militar. El primer caso se remonta a la Guerra del Golfo donde los radares de defensa fueron afectados con el fin de iniciar la campaña aérea.

No obstante, como se ha analizado, el rango de afectación de un ciberataque va más allá de los sistemas de defensa aérea, pues el potencial del arsenal cibernético es mucho más amplio. Así, por ejemplo, en el caso de la invasión a Iraq (en 2003) se planteó la posibilidad de atacar el sistema financiero momentos previos a la incursión militar.

Ante este escenario, es necesario analizar dos operaciones en donde las tácticas militares tradicionales y el empleo de prácticas de ciberguerra crearon una sinergia, y evaluar los efectos generados por la ejecución de esta nueva práctica en la doctrina militar. Los casos referidos corresponden a la invasión a Iraq en 2003 y la Operación Orchard de 2007, los cuales constituyen dos prototipos de la evolución de la guerra moderna.

3.5.1. La invasión a Iraq (2003): Operación Libertad para Iraq

La invasión a Iraq es considerada la continuación de los asuntos inconclusos heredados de la Guerra del Golfo (1980-1988) y la anexión de Kuwait (1990-1991) que junto a otros factores como la posible posesión de armas de destrucción masiva y la recién iniciada lucha contra el terrorismo abrieron la oportunidad a la invasión estadounidense.

Después de la derrota en 1991 a manos de la coalición la victoria militar pareció insuficiente. Los estrategas militares estadounidenses deseaban también eliminar a

Sadam Hussein del mando iraquí, por lo que la Organización de Naciones Unidas (ONU) recibió constante presión por parte de Washington para comprobar que el régimen iraquí no contaba con armas de destrucción masiva. En Iraq, Hussein enfrentó su propia oposición, la situación posbélica fue complicada, sectores importantes de la población como el sector chií y la minoría kurda comenzaron una serie de sublevaciones que desafiaron la autoridad del partido Ba'ath,[355]la respuesta fue una herramienta frecuentemente aplicada por la administración iraquí: la represión.

La brutalidad con la que el régimen actuó en ciudades como Basra, Najaf y Karbala en contra de la comunidad chiita, y en las provincias del norte contra la población kurda, donde dirigió bombardeos indiscriminados que acabaron con hospitales y ciudades enteras, evidenciaron la sistemática violación de Derechos Humanos por parte de Sadam.[356]

En adelante, Iraq continuó en la mira del gobierno estadounidense al existir sospechas de que el arsenal químico no había sido totalmente destruido. El enfrentamiento se caracterizó por solicitudes a la ONU por parte de Estados Unidos de enviar inspectores a Iraq, así como de imponer sanciones al régimen de Hussein, al tiempo en que el aumentaron las campañas aéreas estadounidenses y británicas en las zonas de exclusión aérea.[357]

El camino de vuelta a Bagdad inició a la llegada de George W. Bush a la presidencia de Estados Unidos en 2001, cuando el entonces Secretario de Estado, Colin Powell solicitó la aplicación de sanciones más severas y concretas contra Iraq. Sin embargo, un punto decisivo en el plan fue, sin duda, los ataques del 11 de septiembre de 2001 contra el World Trade Center y el Pentágono.[358]

---

[355] Clark, Wesley K. (2004). ¿Qué ha fallado en Irak? La guerra, el terrorismo y el imperio americano. Barcelona: Crítica, p.4

[356] García Encina, Carlota y Alicia Sorroza Blanco. "Orígenes de la crísis". En Rafael L. Bardají. (Ed.) (2003). *Irak: Reflexiones sobre una guerra*, p.13 [En línea]. Disponible en: <http://www.realinstitu toelcano.org/wps/portal /rielcano_es/publicacion?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/publicaciones/irak_+reflexiones+sobre+una+guerra>.

[357] Clark, *Óp. Cit*., pp. 4-5.

[358] *Ídem*, p. 7

Fue entonces cuando, tras iniciar la campaña contra Afganistán en 2001 en busca del líder de Al Qaeda y una vez declarada la guerra global contra el terrorismo, se emplearon argumentos como la posesión de armas de destrucción masiva e incluso vínculos entre Sadam Hussein y la organización terrorista para justificar las operaciones militares en suelo iraquí que dieron inicio el 20 de marzo de 2003.[359]

No obstante, la planeación militar había comenzado desde enero de 2002 en el marco de una serie de reuniones celebradas entre el general Tommy Franks y el Secretario de Defensa Donald Rumsfeld. Los planes del Centro de Mando de Estados Unidos, OPLAN 1003 contenían el modelo utilizado en la Guerra del Golfo. Sin embargo, el Secretario de Defensa abogó por modificaciones relacionadas con: 1) el empleo de grupos reducidos y, 2) la ejecución de una campaña de ritmo rápido, el plan fue modificado más de una decena de veces antes conseguir una versión final.[360]

Las técnicas empleadas en la Operación Tormenta del Desierto otorgaron la victoria a la coalición, sin embargo, ninguna guerra se parece a otra y en esta ocasión el plan sustrajo las lecciones aprendidas en 1991 e incluyó medidas para responder a un posible contrataque con misiles SCUD dirigidos a Israel, como ya lo había hecho Hussein durante la liberación de Kuwait, e incluso para responder al uso de armamento químico como ocurrió en el enfrentamiento con Irán.[361]

El resultado fue un plan integral conformado por tres componentes:

1. Una fuerte ofensiva aérea dirigida contra objetivos gubernamentales, destinada a destruir el sistema integrado de defensa iraquí (sistemas de mando y control, y radares aéreos)
2. Unas fuerzas operacionales especiales encargadas de destruir las plataformas de lanzamiento de misiles SCUD en el oeste de Iraq, así como todas las instalaciones navales en las proximidades de Umm Qasr

[359] Bassil, Youssef. (2012). "The 2003 Iraq War: Operations, Causes, and Consequences". *Journal Of Humanities And Social Science*, Volumen 4, Issue 5, p. 29. [En línea]. Disponible en: <www.lacsc.org/papers/papera1.pdf>
[360] Clark, *Óp. Cit*., p 9.
[361] *Ídem*, p. 11

3. Fuerzas en tierra que avanzarían hacia Bagdad rápidamente para aniquilar el resto de las tropas iraquíes.[362]

Adicionalmente, se emplearían campañas de desinformación con el fin de engañar a las fuerzas iraquíes, impidiéndoles reaccionar de forma efectiva. La tecnología moderna, también jugó un importante papel, ya que desde la Guerra del Golfo había supuesto una disminución en el número de bajas y en los daños colaterales, mediante la explotación de ventajas asimétricas.[363]

Por su parte, Iraq mostraba una debilidad significativa, de acuerdo con el General Wesley K Clark (2004), a pesar de que la defensa iraquí contaba con veintiséis divisiones, constituidas por 2 000 tanques, 2 500 piezas de artillería, 300 cazas y aviones de ataque, 150 helicópteros armados, 400 000 hombres y cerca de 40 000 fedayines, los equipos eran anticuados, el sistema integrado de defensa era vulnerable por su ubicación, y tanto los misiles como los vehículos aéreos mostraban un alcance limitado.[364]

Mientras que las fuerzas estadounidenses contaban con bombarderos B-2 Spirit, cada uno de ellos capaces de transportar 16 Joint Direct Attack Munitions (JDAM), conocidas también como “bombas inteligentes”, además de los ya empleados en la Operación Tormenta del Desierto, cazas indetectables F117 Nighthawk.[365]

Los equipos bélicos electrónicos también habían sido reforzados y al EA- 6B Prowler le fueron añadidas cubiertas de interferencia para su protección, mientras que el F-16D contaba con misiles anti radiación capaz de detectar los radares enemigos.[366]

Los procesos de mando y control se vieron reforzados con el desarrollo y empleo de Aviones Aéreos No Tripulados (UAV, *Unmanted Air Vehicles*) que, al estar dotados de cámaras, otorgaron grandes beneficios al momento de explorar el campo de batalla, a ello se sumó la mejora en los sistemas JSTARS (Joint

[362] *Íbidem*
[363] *Ídem*, p. 12
[364] *Ídem*, p. 13-14
[365] Ídem, pp 20-21
[366] *Íbidem*

Survillance and Target Adquisiton Radar System) Sistema Conjunto de Radar de Vigilancia y Ataque Objetivo, el resultado de toda esta incorporación tecnológica fue una disminución de soldados en la batalla.[367]

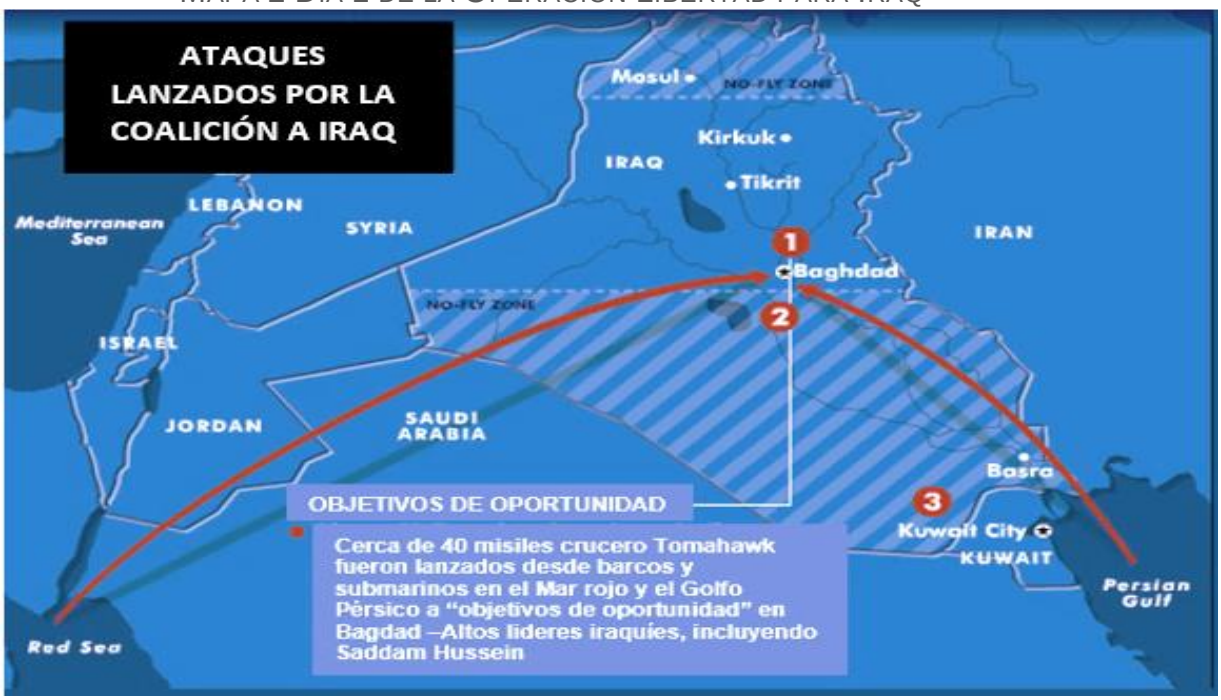
Sin embargo, no fue sólo el armamento lo que derrotó a las fuerzas iraquíes sino la conformación de una alianza internacional que en un primer momento estuvo conformada por Estados Unidos, Reino Unido y Australia.[368]Más adelante, en la Operación Libertad para Iraq se sumaron tropas de 37 países, más otros 20 aportando apoyo indirecto.[369]

Antes de iniciar la operación había que resolver una cuestión muy importante, que consistía en el apoyo de dos importantes actores regionales: Turquía y Arabia Saudita. El apoyo de Turquía permitiría el despliegue de tropas por el este del Iraq facilitando la conquista de los pozos petrolíferos de Kirkuk, y de esta forma la Coalición lograría atacar desde el norte de Bagdad y Tikrit. Sin embargo, ya iniciada la operación el entonces presidente Recep Tayyip Erdoğan no aprobó la utilización del espacio aéreo turco, ni el despliegue de tropas norteamericanas en su territorio.[370]

Del lado saudí, el uso de sus puertos facilitaría el rendimiento diario de las tropas y de las provisiones. Del mismo modo, el uso del espacio aéreo permitiría llevar a cabo operaciones especiales y aéreas al oeste de Iraq. No obstante, el gobierno saudí no permitió el uso de puertos ni el despliegue de tropas a través de su territorio, aunque sí permitió el uso del espacio aéreo y el establecimiento de un cuartel general.[371] (ver mapa 2)

[367] *Ídem, pp 19-21*
[368] Bassil, *Óp.Cit.*, p.34
[369] Carney, Stephen A. (2011). *Allied Participation in Operation Iraqi Freedom*. Washington: Center of Military History, p. 1.
[370] Clark, *Óp. Cit., pp.21-22*
[371] *Ídem.*

MAPA 2 DÍA 1 DE LA OPERACIÓN LIBERTAD PARA IRAQ



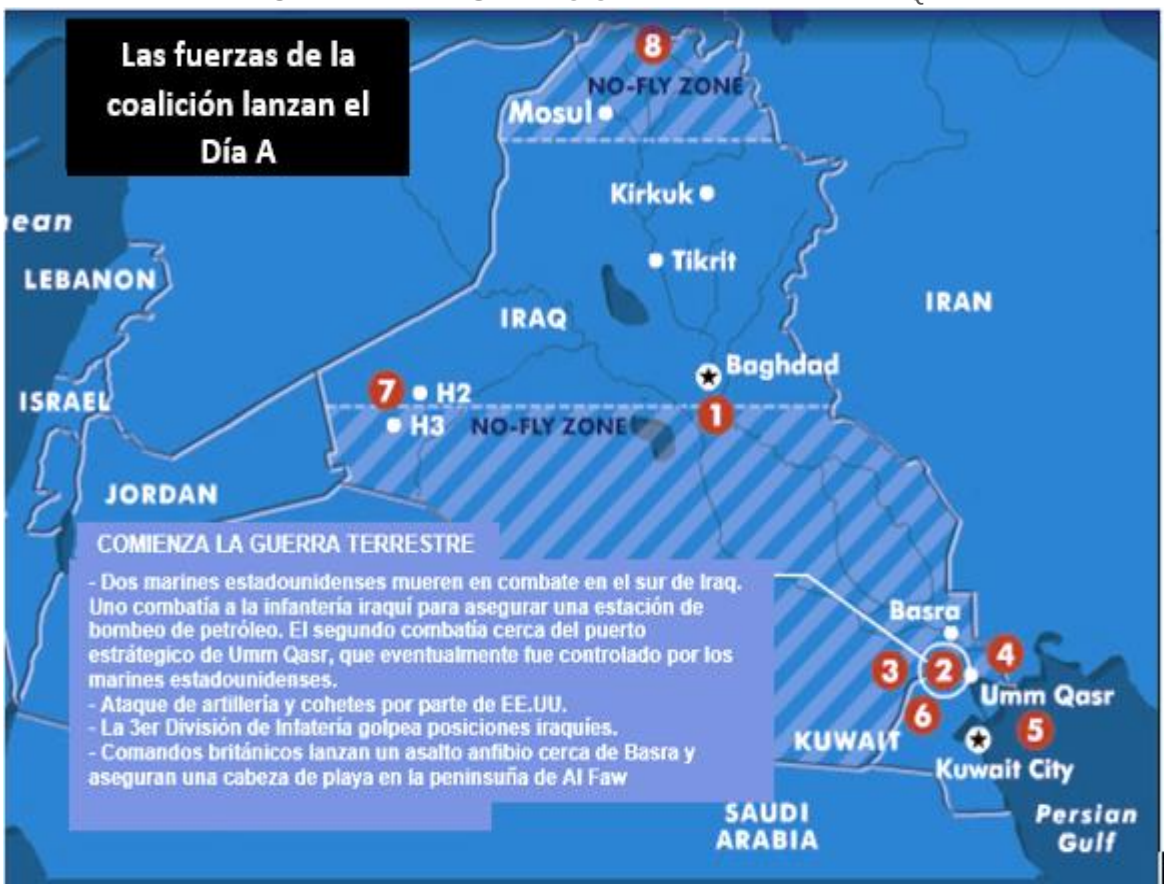
Fuente: USA TODAY. (2002). "Operation Iraqi Freedom". [En línea]. Disponible en: <https://usatoday30.usatoday.com/news/world/iraq/bigmap.htm>

La Operación Libertad para Iraq comenzó el 20 de marzo de 2003 cuando las fuerzas de la coalición, una vez finalizado el ultimátum de 48 horas otorgado por George W. Bush a Sadam Hussein y a sus hijos Uday y Qusay para abandonar Iraq, comenzaron un bombardeo aéreo contra Bagdad empleando aviones F117 y cuarenta misiles de crucero Tomahawk.[372](Ver tabla 10)

Las fuerzas aliadas se concentraron en bombardear la capital y otras ciudades, además de los sistemas de defensa del país. Sólo 18 horas después del inicio de la campaña aérea las fuerzas terrestres se movilizaron, lo que significó un cambio muy importante respecto a la Operación Tormenta del Desierto. (Ver mapa 3)

[372] Clark, Wesley K. (2004). *¿Qué ha fallado en Irak? La guerra, el terrorismo y el imperio americano*. Barcelona: Crítica, p.1

MAPA 3 DÍA 2 DE LA OPERACIÓN LIBERTAD PARA IRAQ



Fuente: USA TODAY. (2002). "Operation Iraqi Freedom". [En línea]. Disponible en: <https://usatoday30.usatoday.com/news/world/iraq/bigmap.htm>

Mientras tanto, en el sur fuerzas británicas y estadounidenses se enfrentaron a tres divisiones del Ejército Regular iraquí. En los siguientes días se libraron múltiples batallas en las ciudades de Umm Qasr y Nasiriyah. En Basra la resistencia iraquí combatió por dos semanas, mientras que las fuerzas de Hussein en Basora fueron apoyadas por artillería del volumen de un batallón y ninguna ayuda aérea, poco a poco, las fuerzas iraquíes cedieron ante el peso numérico y armamentista de la alianza. La infantería mecanizada estadounidense consiguió dirigirse a Bagdad acompañado por tanques blindados, artillería pesada y la supremacía aérea. Sin embargo, dada la negativa turca las fuerzas estadounidenses debieron moverse a través de Kuwait.[373]

[373] Bassil, Óp.Cit., pp.34-36

Tras 19 días, la coalición logró empujar al sur y al este a las unidades iraquíes que combatían en Bagdad, Tikrit, Baquba y Kut. A pesar del empleo de misiles balísticos por parte de la Guardia Republicana no se consiguió obtener ninguna ventaja, pues fueron interceptados por misiles Patriot por parte de la coalición. Finalmente, el régimen de Sadam cayó en los días siguientes, los hijos de Hussein Uday y Qusay fueron capturados y asesinados el 22 de julio de 2003. Mientras que Hussein fue detenido en un sótano en Tikrit por soldados estadounidenses el 14 de diciembre 2003, condenado por un Tribunal Especial Iraquí y finalmente colgado el 30 de diciembre de ese mismo año.[374]

[374] *Ídem.*

TABLA 10 ARMAMENTO EMPLEADO EN LA INVASIÓN A IRAQ (2003)

DENOMINACIÓN	MODALIDAD	ORIGEN	DESCRIPCIÓN
Talon Sword robots	Tierra-Funciones de reconocimiento	EE. UU - R.U/ Foster-Miller, Inc.-Qinetiq	Se trata de un robot militar ligero no tripulado. Su objetivo es proteger a los combatientes y a los primeros socorristas contra amenazas explosivas. Puede transportar una carga útil de 45kg y tiene una capacidad de arrastre de hasta 77.11kg con pinza, una capacidad de remolque de 340 kg. (Kable:2017c)
Misiles AGM-86	Misil Tierra-Aire	EE. UU/Boeing	Es un misil de crucero diseñado para incrementar la efectividad de los bombarderos B-52H Stratofortress de la Fuerza Aérea de los Estados Unidos. Tiene una longitud de 20 pies y 9 pulgadas, pesa 3 150 libras, tiene un alcance de 1 500 millas y una velocidad de 550 millas por hora. (Smith: 2017)
Misiles AGM-158 JASSM	Misil Tierra-Aire	EE. UU/ Lockheed Martin	Misil del crucero, forma parte de los misiles JASSM (Joint Air-to-Surface Standoff Missile), este tipo de misil están guiados por una combinación de posicionamiento GPS / INS (Inertial Navegation System) y por un infrarrojo de imagen (IIR, radiación infrarroja) para el objetivo final. (Defense Industry Daily: 2017)
Misiles AGM-84 ER Harpoon	Aire	EE. UU/ Boeing	Es un misil anti-bunque al servicio de las Fuerzas Armadas de Estados Unidos, el proyecto inició formalmente en 1968. El término AGM refiere a que este tipo de misil es lanzado desde el aire (es posible lanzarlo desde buques de superficie RGM-84 y submarinos UGM-84). Tiene un alcance de 90 km, su producción comenzó en 1975. (Parsch:2008).
Misiles AGM-65 Maverick	Misil Tierra-Aire	EE. UU/ Raytheon	Es un misil táctico aire-superficie empleado en misiones de apoyo cercano, interdicción y supresión de defensas enemigas. Tiene un diámetro de 305 mm, una envergadura de 720 mm y una longitud de 2.49 metros, mientras que el peso varía de entre 286-301 kg. (Figueroa: 2002)
AGM-114 Hellfire	Misil Aire-Tierra	EE. UU/ Lockheed Martin	Es un misil subsónico aire-tierra, guiado por láser con una gran capacidad antitanque. El misil también puede utilizarse como un arma aire-aire contra helicópteros y aviones de ala fija de lento movimiento. Este modelo es un misil aire-tierra (AGM, por sus siglas en inglés Air to Ground) 114 posee un importante grado de precisión contra, tanques, estructuras, búnkeres y helicópteros. (Smith:2017)
MQ-1B Predator	Aire-Drone	EE. UU/ General Atomics	Se trata de un sistema de aeronaves no tripuladas de larga duración y altitud media, empleado en misiones de vigilancia y reconocimiento. Inicialmente empleaba el sistema operativo Windows XP, pero luego de un ataque informático en octubre de 2011 fue sustituido por otro con base en GNU/Linux. (Leyden:2012)
MQ-9A Reaper	Aire-Drone	EE. UU/General Atomics	Se trata de aviones pilotados remotamente diseñados para misiones de Inteligencia, Vigilancia y Reconocimiento (ISR, por sus siglas en inglés *Intelligence, Surveillance and Reconnaissance*). Debido a su variedad de sensores de vigilancia se ha convertido en una unidad en un elemento cada vez más vital, también sirve de apoyo a las unidades Predator. (Hillier:2007)
Bombardero B-52	Aeronave	EE. UU/Boeing	Es bombardero estratégico subsónico, tiene 48.5 metros de largo y una envergadura de 56.4 metros. Es capaz de volar a 1 046 km/h a una altura de hasta 15 200 metros. Su capacidad de carga es de 22 670 kilos conformados por armas convencionales y 32 misiles de crucero, además puede recargar combustible en el aire. (Morgan: 2015)
CBU-94	Bomba (letal)	EE. UU/Sin información disponible	Se conoce también como bomba blanda es un arma no letal que se utiliza para apagar los suministros de energía del enemigo. Emplea filamentos de carbono tratados químicamente que se lanzan sobre componentes electrónicos provocando cortos circuitos y descargas electrónicas dentro de diversos tipos de infraestructura. (Jeler y Roman: 2016

Fuente: Elaboración propia con datos de Sánchez Méndez (2003), McElroy (2007) y Yenne (2017).

Durante la Operación Libertad para Iraq los imperativos de la Revolución Tecnológico Informacional de los Asuntos Militares estuvieron presentes. No se trató de un plan creado en sólo unos meses, puesto que desde la Operación Tormenta del Desierto se consideró su posible re-aplicación en suelo iraquí. Sin embargo, el plan sufrió varias modificaciones respondiendo a las capacidades militares de la Guardia Iraquí y la posible cooperación de los países clave en la región.

La intervención de la Coalición en Iraq es vista desde el plano militar como un éxito otorgado por el uso estratégico de las fuerzas militares y la supremacía tecnológica armamentística. Reafirmó la proposición de una trasformación en la naturaleza de la guerra, pues, de acuerdo con el General Wesley K. Clark: "la guerra de 2003 en Irak fue el primer ensayo a gran escala de guerra moderna en plena acción".[375]

Sin embargo, el grado en objetivos propuestos por la Revolución Tecnológico Informacional de los Asuntos Militares se alcanzó es difícil de calcular pues, aunque la creación de una coalición y el empleo de armamento altamente tecnológico se tradujeron en menor presencia militar estadounidense en Iraq (en comparación con la Guerra del Golfo), la reducción del daño colateral estuvo muy lejos de alcanzarse. De acuerdo con la organización *Iraq Body Count,* de 2003 a noviembre de 2011 entre 103 013 y 112 571 iraquíes murieron en enfrentamientos militares y al menos 250 000 resultaron heridos. Del lado estadounidense, se reportaron 4 485 bajas y 32 219 heridos. En adición, como resultado del conflicto desde 2003 dos millones de iraquíes huyeron en dirección a Siria y Jordania. Mientras que la organización *National Priorities Project* estimó que la guerra costó al gobierno estadounidense 800 000 millones de dólares.[376]

Determinar el costo humano del enfrentamiento es imposible, además los datos varían dependiendo de la fuente. Por ejemplo, según un informe del Comando Central estadounidense dado a conocer después de 2010, se calcula que sólo entre

[375] Clark, *Óp.Cit*., p. XXI
[376] Bassil, *Óp. Cit.,* p. 29

enero 2004 y agosto de 2008, 76 939 fuerzas de seguridad y civiles iraquíes murieron, mientras que 121 649 fueron heridos.[377]

Ya sea tomando en cuenta los datos del *Iraq Body Count* o del Comando Central estadounidense, la Invasión a Iraq de 2003 ha sido más devastadora que la Guerra de Golfo. Lo que demuestra que el uso de armamento altamente tecnológico con mayor grado de precisión no es capaz de eliminar, y en este caso, de disminuir los daños colaterales.

Otro elemento presente durante la fase de planeación de la Operación Libertad para Iraq fue la posibilidad del uso de un ataque cibernético para dañar la economía del líder iraquí. La operación consistiría en atacar cibernéticamente el sistema financiero con el fin de congelar millones de dólares de las cuentas bancarias de Sadam Hussein antes de la invasión. De esta forma se perjudicaría el desempeño militar, pues no habría recursos para pagar a las tropas. Sin embargo, el plan fue descartado, ya que se temió que el ataque pudiera afectar también los sistemas financieros de Europa o Estados Unidos.[378]

No obstante, en el plano militar sí se llevaron a cabo ataques cibernéticos en contra de comunicaciones gubernamentales y militares iraquíes durante las primeras horas de la operación. De este modo se inutilizaron las torres de comunicación móvil, y se realizaron interferencias electrónicas y ataques digitales en contra de redes telefónicas.[379]

En cuanto a la evolución del armamento durante la intervención se emplearon robots militares y drones. Existen reportes de *WikiLeaks* que revelan una mayor inversión y uso de robots militares en Iraq, según los documentos filtrados cerca de 400 robots se trasladaron a suelo iraquí, sus capacidades iban desde el reconocimiento hasta las capacidades de combate. En cuanto al número de drones,

---

[377] Crawford, Neta C. (Marzo, 2013). *Civilian Death and Injury in the Iraq War, 2003-2013*. Waston Institute, p 7. [En línea]. Disponible: <http://watson.brown.educostsofwar/files/cow/imce/papers/2013/Civilian%20Death%20and%20Injury%20in%20the%20Iraq%20War%2C%202003-2013.pdf>

[378] Markoff, John y Thom Shanker. (Agosto 1, 2009). "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk". *The New York Times*. [En línea]. Disponible: <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html>

[379] *Ídem*.

fueron cerca de 144, según la misma fuente, bajo ambas modalidades (reconocimiento y combate).[380]

De esta manera, analizando las proporciones de la Revolución Tecnológico Informacional de los Asuntos Militares durante la intervención en Iraq, se tiene que:

1. En cuanto a la reducción del tiempo necesario para ejecutar una operación militar la implementación de la Operación Libertad para Iraq consiguió su objetivo inmediato, que fue la captura de Sadam Hussein en un lapso corto de tiempo. Sin embargo, las críticas de la acción militar en Iraq se dirigen a la ausencia de un plan posterior a la intervención que permitiera la estructuración de un gobierno genuinamente iraquí. Aunado a ello, la presencia militar en la zona derivó en la creación de grupos de resistencia conformados por los ex miembros de la Guardia Republicana[381] que se enfrentaron a las fuerzas de la coalición impulsando la desestabilización social y política.
2. Respecto a la disminución en el número de bajas, el empleo de armamento altamente tecnológico proporcionó ventajas a las fuerzas armadas. Así, por ejemplo, el empleo de UCAV Predator (*Unmanned Combat Air Vehicles*), permitió que se llevaran a cabo operaciones de combate sin la presencia física de las fuerzas armadas en el campo de batalla. En adición, el uso de robots Talon permitió ejecutar labores de reconocimiento y disminuyó los riesgos presentados por el empleo de dispositivos explosivos improvisados por parte de la insurgencia. Además, la conformación de una alianza internacional se tradujo en presencia militar tecnológicamente equipada y con sistemas de inteligencia y comunicación avanzados.
3. En cuanto a la disminución del daño colateral, pese al empleo de armamento inteligente, desde el comienzo de la Operación Libertad para

[380] Assange, Julian y staff. (Noviembre 8, 2007). "US Military Equipment in Iraq (2007)". *WikiLeaks*. [En línea]. Disponible: <https://wikileaks.org/wiki/US_Military_Equipment_in_Iraq_(2007)#Cryptographic_and_communications_security_equipment>

[381] Mesa Delmonte, Luis y Rodobaldo Isasi Herrera. (2004). *Estados Unidos e Iraq, Prólogo para un golpe preventivo*. México: CIESAS, p. 188

> Iraq los bombardeos de la coalición internacional derivaron en la muerte de civiles en lugares como al-Hilla, al-Najaf y al-Nasiriyya.[382]

A lo anterior hay que sumar el comportamiento de las tropas en territorio iraquí que resultó en abusos como los cometidos en la cárcel de Abu Ghraib. Finalmente, la ausencia de un plan de posguerra que propiciara la reconstrucción efectiva de Iraq sumado a la retirada de tropas estadounidenses terminó favoreciendo a los grupos islamistas radicales como Al Qaeda en Iraq.

3.5.2. El bombardeo a Al-Kibar: la Operación Huerta

Un caso quizá menos conocido en donde el armamento cibernético y la tecnología militar se conjugaron para detener el desarrollo de capacidades nucleares en Medio Oriente es la Operación Orchard (u Operación Huerta) ejecutada en Siria por parte de Israel en septiembre de 2007.

Esta operación militar giró en torno a los servicios de inteligencia israelíes (Mossad), la Agencia Nacional de Seguridad de Estados Unidos (NSA, por sus siglas en inglés) y el gobierno sirio, entonces liderado por Bashar Al Assad. El uso de armamento cibernético previo y durante la intervención aérea proporcionó los datos y las capacidades necesarias para aniquilar las instalaciones nucleares en Al Kibar, al norte de Siria.

Todo comenzó en el año 2000 a la llegada del presidente Bashar Al-Assad al gobierno de la República Árabe Siria, pues desde comienzo de su administración la figura de Bashar fue objeto de observación de la agencia de inteligencia israelí, Mossad, quien deseaba descifrar el perfil del nuevo líder.[383]

En 2004, los servicios de inteligencia estadounidense identificaron un aumento inusual de llamadas telefónicas entre Corea del Norte y Siria, por lo que la NSA realizó un informe que compartió con la unidad 8200 del Mossad. En 2006, los

[382] Human Rights Watch. (Diciembre 12, 2003). “Off Target, The Conduct of the War and Civilian Casualties in Iraq”. [En línea]. Disponible en: <https://www.hrw.org/report/2003/12/11/target/conduct-war-and-civilian-casualties-iraq>

[383] Follath, Erich y Holger Stark. (Febrero 11, 2009). ”How Israel Destroyed Syria's Al Kibar Nuclear Reactor”. *SPIEGEL*. [En línea]. Disponible: <http://www.spiegel.de/international/world/0,1518>

servicios de inteligencia israelí ejecutaron operaciones de espionaje en contra de un alto funcionario sirio de visita en Londres, tras el empleo de un virus informático de tipo troyano se consiguió evidencia que sugirió la cooperación entre Corea del Norte y Siria para el desarrollo de un complejo nuclear en Al Kibar.[384]

Luego de confirmar la información, de parte de un desertor del programa iraní, el entonces Primer Ministro Ehud Olmert dio inicio a la Operación Orchard el 6 de septiembre de 2007, cuando diez aeronaves F-15 y F16 partieron de la base aérea de Ramat David con dirección a desierto Deir ez-Zor.[385]

La primera fase de esta operación se dirigió atacar los sistemas de comunicaciones sirios por dos medios:

1. El sabotaje al sistema de defensa antiaéreo Pantsyr-S1 (tecnología rusa) mediante el empleo de un programa que atacó e invadió la red de comunicaciones aéreas sirias y tomó el lugar del administrador del sistema.[386]
2. El bombardeo con armas de precisión a las instalaciones de radares, en donde se presume se emplearon misiles AGM-65 Maverick y bombas de 500 kg guiadas por láser. [387]

Posteriormente se aniquilaron las instalaciones nucleares, empleando el mismo tipo de arsenal inteligente. La operación, aunque presentada en los medios de comunicación tanto israelíes como sirios, no fue oficialmente aclarada ni por Bashar Al Assad ni por Ehud Olmert, pues en primer lugar Siria forma parte del Acuerdo de No Proliferación de Armas Nucleares y al emitir alguna declaración evidenciaría la violación del tratado, además de desvelar la cooperación con Corea del Norte e Irán. Mientras que el gobierno israelí tendría que enfrentarse a dos importantes argumentos: 1) la forma en la obtuvo el material que evidenciaba el desarrollo de

[384] *ídem*
[385] *ídem*
[386] Kaplan, Caren. (Noviembre 5, 2014). "Air power's visual legacy: Operation Orchard and aerial reconnaissance imagery as ruses de guerre". *Critical Military Studies*, Vol. 1, No. 1, p. 63. [En línea]. Disponible: <http://www.tandfonline.com/doi/pdf/10.1080/23337486.2014.974949?needAccess=true>.
[387] Schreier, Fred. (2015). *On* Cyberwarfare. DCAF Horizon 2015 Working Paper No. 7, p.111. [En línea]. Disponible: <www.dcaf.ch/content/download/.../OnCyberwarfare-Schreier.pdf>

las instalaciones y 2) el uso unilateral de la fuerza, con lo cual violó el espacio aéreo sirio y empleó armamento cibernético en contra del sistema de defensa antiaéreo.

La Operación Orchard es relevante en el ámbito de la ciberdefensa, pues constituye un modelo de guerra "multi-espectro", en donde el empleo de armamento cibernético conjugado con intervención militar convencional potenció el impacto de las actividades militares que actuaron de forma simultánea en dos espacios (cibernético y tangible) hacia un sólo objetivo.

3.6. ACTORES NO ESTATALES EN LÍNEA

El surgimiento de Ejércitos Electrónicos es un ejemplo de cómo la habilidad en el uso de herramientas tecnológicas otorga ventaja asimétrica a actores no estatales.

En Medio Oriente la actividad de los hackers se ha dirigido en contra de instituciones bancarias[388] y compañías petroleras. El daño que un ataque exitoso a estos sectores podría generar en los mercados mundiales ha propiciado el incremento de presupuesto destinado a la implementación de medidas de ciberseguridad.[389]

La mayoría de los ataques cibernéticos en Medio Oriente se ejecutan bajo la ideología hacktivista, es decir, con el fin de promover un objetivo político. Según cifras de 2013, cerca del 45% de los ataques en la región fueron perpetrados por grupos clasificados bajo esta categoría, 40% se clasificaron como cibercrimen y el resto se colocó bajo la categoría de guerra cibernética, que incluye actividades de ciberspionaje. En general, las operaciones hacktivistas tienen como objetivo la irrupción de un servicio. De esta forma, grupos como "Cutting Sword of Justice" han

[388] Wagstaff, Jeremy y Raju Gopalakrishna. (Mayo 23, 2016). "Hackers probe defenses of Middle East banks: FireEye". *Reuters*. [En línea]. Disponible en: <http://www.reuters.com/article/us-cyber-heist-mideast-idUSKCN0YE19Q>.

[389] Amine Belarbi, Mohamed. (2015). "Cybersecurity in the Middle East: You're Not As Safe As You Think". *Gulfelitemag*. [En línea]. Disponible en: <http://gulfelitemag.com/cybersecurity-in-the-middle-east-youre-not-as-safe-as-you-think/>.

declarado la intención de atacar a los países que apoyen los crímenes y atrocidades cometidos en Siria, Bahréin, Líbano y Egipto.[390]

Otra clase de actores son las corporaciones, encargadas de proveer servicios de seguridad y comunicación, a menudo empleadas por los Estados para llevar a cabo operaciones de guerra cibernética.[391]

Así, el incremento de ataques cibernéticos contra infraestructura crítica ha atraído a corporaciones como Lockheed Martin e IBM que, en el caso específico del gobierno saudí, están creando soluciones de seguridad para hacer frente a las amenazas digitales. Los participantes en este sector son corporaciones como Cisco Systems Inc., IBM Corporation, Intel Security Group, Dell Secure Works Inc., Symantec Corporation, y Verizon Communications Inc. Mientras que en el ámbito militar figuran BAE Systems Plc, General Dynamics Corporation, Finmeccanica S.P.A., Lockheed Martin Corporation, Northrop Grumman Corporation, Raytheon Company, y Thales Group.[392]

Finalmente, aparecen las organizaciones delictivas y los grupos terroristas que se trasladan a la web para: 1) realizar operaciones financieras a través del mercado negro (donde comúnmente emplean la *deep web*) asistidas por los bitcoins, 2) utilizar la red como medio de comunicación, en especial los canales de comunicación cifrada para la transmisión de mensajes dentro de la estructura, 3) como medio de propaganda y reclutamiento, y 4) para la destrucción, mediante ataques cibernéticos, de bienes públicos.[393]

En la web, y de forma especial, en la *deep web* operan grupos dedicados al fraude, robo de identidad, comercio ilícito, el lavado de dinero, espionaje industrial y hasta mercenarios, dada la transnacionalidad de dichas amenazas los expertos

---

[390] Hamid, Triska. (Junio 6, 2013). "Hacktivism the motivator of cyber attacks in Middle East". *The National*. [En línea]. Disponible en: <http://www.thenational.ae/business/industry-insights/technology/hacktivism-the-motivator-of-cyber-attacks-in-middle-east>.

[391] Sigholm, Johan. (Abril, 2013). "Non-State Actors in Cyberspace Operations." *Journal of Military Studies*, p. 21. [En línea]. Disponible: <https://journal.fi/jms/article/view/7609>.

[392] Sharma, Sanjana. (2017). "Cyber Security for the Defence Industry". *Cyber Security Review*. [En línea]. Disponible: <http://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defence-industry/>.

[393] Sigholm, *Óp. Cit.*, p. 18.

en seguridad promueven la cooperación internacional en materia de intercambio de información con el fin de combatir todo tipo de crimen cibernético.[394]

Particularmente, en el caso del terrorismo el uso de la red como medio de radicalización, ha sido empleado por Al Qaeda desde finales de la década de los 90, cuando comenzó a explotar la capacidad otorgada por la evolución de las comunicaciones para adoptar nuevos canales de interconexión dentro de la organización terrorista. Más adelante, se desarrollaron también páginas web bajo ideología yihadista que incluso contaban con foros de debate, y el lanzamiento de una revista conocida como Inspire.[395] Esto sólo por parte de Al Qaeda, del otro lado se encuentra Daesh, que en los últimos años ha atraído la atención de los expertos en seguridad por el extenso empleo de los medios digitales. No obstante, para analizar la actividad en línea del Daesh es preciso conocer sus objetivos e historia.

3.7. Génesis del Daesh

El origen de Daesh, también conocido como Estado Islámico, se ubica en la actividad de Ahmad Fadl Al Nazar Al Khalayleh mejor conocido como Abu Musab Al Zarqawi, un jordano encarcelado en su país bajo acusaciones de formar parte del grupo terrorista Bayal Al Imam. Una vez en libertad Zarqawi se trasladó a Afganistán en busca de apoyo financiero por parte del entonces líder de Al Qaeda, Osama Bin Laden, quien le otorgó un préstamo de 200 000 dólares[396] para establecer un campo de entrenamiento en la ciudad de Herat, al oeste de Afganistán.[397]

Sin embargo, Al Qaeda y Abu Musab Al Zarqawi poseían diferencias ideológicas importantes en torno a la concepción de la yihad. El objetivo personal de Al Zarqawi era emular la figura histórica de Nur Al Din Zangi, un caudillo árabe que en la época

[394] Williams, Phil. (*s.f.*). "Organized Crime and Cybercrime: Synergies, Trends, and Responses". [En línea]. Disponible: <http://www.crime-research.org/library/Cybercrime.htm>.

[395] Estarellas y López, Juan C. (Febrero, 2011). "Los medios de comunicación de Al-Qaeda y su evolución estratégica". *Documento de opinión. Instituto Español de Estudios Estratégicos*, Número 15, p.13. [En línea]. Disponible en: <ww w.ieee.es/Galerias/fichero/.../DIEEEO16_2011MediosComunicacionAl-Qaeda.pdf>.

[396] Jordán, Javier. El Daesh. *Cuadernos de Estrategia 173 La Internacional Yihadista*. (2015) Instituto Español de Estudios Estratégicos, p. 111. [En línea]. Disponible: <http://www.ieee.es/Galerias/fichero/cuadernos/CE_173.pdf>.

[397] Bunzel, Cole. (Marzo, 2015). *From Paper State to Caliphate: The Ideology of the Islamic State*. The Brookings Project on U.S. Relations with the Islamic World Analysis Paper, No. 19, p. 3 [En línea]. Disponible: <https://www.brookings.edu/wp-content/uploads/2016/06/The-ideology-of-the-Islamic-State.pdf>.

de las cruzadas luchó por la unificación de los territorios ubicados entre Mosul y Damasco.[398](ver Anexo II. Bases Ideológicas del Estado Islámico)

En 1999 tras un fallido atentado descubierto por los servicios de inteligencia jordanos Al Zarqawi se refugió en el Kurdistán iraquí en donde estableció vínculos con Ansar Al Islam. En Iraq, Zarqawi encontró un nuevo espacio de operaciones y llevó a cabo varios ataques entre los que se encuentra el atentado con coche bomba contra la embajada jordana en Bagdad acaecido el 7 de agosto de 2013.[399]

En septiembre de 2004, Al Zarqawi juró lealtad a Osama Bin Laden y con ello se convirtió en líder de Al Qaeda en Iraq (AQI). Sin embargo, las rivalidades persistieron y el año siguiente Ayman Zawahiri y Atiya Abd Rahman enviaron una carta a Al Zarqawi en donde expresaron su inconformidad por los métodos mediáticos utilizados por AQI, pues ya habían comenzado a publicarse los videos de decapitaciones. Posteriormente, cuando la posibilidad de un acuerdo entre la minoría sunní en Iraq y las fuerzas estadounidenses comenzaba a convertirse en una realidad dio inicio el período de declive de la organización.[400]

En enero de 2006 AQI organizó una reunión denominada “Consejo Shura de los Muyahidín” mediante la cual reunió a cinco grupos insurgentes que en su mayoría provenían de Iraq (a excepción del Ejército Islámico de Iraq quién no formó parte de dicha convocatoria) con el fin de unir fuerzas bajo su mando. En junio de 2006, Al Zarqawi fue abatido por fuerzas militares estadounidenses, cinco días después Abu Hamza Al Muhajir, conocido también como Abu Ayyub Al Masri tomó el mando de AQI y cuatro meses más tarde se anunció la creación del Estado Islámico de Iraq[401], también conocido como ISI, liderado ya por Abu Omar Al Baghdadí.[402]

Progresivamente, las actividades del ISI se tornaron más violentas, y comenzaron a asesinar a musulmanes iraquíes que no aceptaban su autoridad, lo cual exacerbó las diferencias entre ISI y Al Qaeda central. De forma paralela, el

[398] Jordán, *Óp. Cit*., p. 112.
[399] Íbidem, p. 113
[400] Jordán, *Óp. Cit* p. 115
[401] Que comprendía los territorios de Bagdad, Anbar, Diyala, Kirkuk, Salah al-Din, Nínive y partes de las provincias de Babil y Wasit. Fuente: Bunzel: 2015.
[402]Jordán, *Óp. Cit*., pp. 114-115

número de combatientes aumentó, en su mayoría individuos provenientes de Arabia Saudita, Libia y Siria. Sus ingresos económicos también incrementaron, hacia 2006 se calculó que la organización percibió un ingreso anual de 70 millones de dólares derivado de diversas actividades delictivas como extorsiones, secuestros, robo de petróleo, etc.[403]

La brutalidad de las acciones de ISI se agravó con el paso del tiempo, especialmente en contra de tribus suníes y chiíes (pues emprendió acciones con el fin de alimentar las rivalidades y generar más violencia), miembros de la comunidad cristiana y yazidíes. Aunque en un comienzo recibió apoyo por parte de la comunidad sunní la incapacidad de ISI para responder de forma efectiva a las demandas de seguridad de dicha minoría llevó a que ésta formara un grupo de resistencia denominada Al Anbar (el despertar sunní) que terminó colaborando con tropas norteamericanas en las operaciones de combate a Estado Islámico (EI).[404]

Para 2008, el cuartel general del ISI se trasladó a Mosul, en esta etapa la organización adoptó un nuevo modelo operativo. Sin embargo, el 18 de abril de 2010 las fuerzas estadounidenses abatieron a Omar Al Baghdadi y Ayyub Al Masri cerca de Tikrit, al norte de Bagdad. Durante ese año las operaciones de combate al ISI consiguieron eliminar a 34 de los 42 miembros de la élite de alto nivel. Hacia 2012 la organización experimentó una etapa de recuperación que le permitió reclutar nuevos miembros (provenientes incluso de Al Anbar). En 2013 el asalto a prisiones, como Abu Ghraib donde 500 presos fueron liberados, nutrió las filas de Estado Islámico. [405]

En 2011, ante el inicio del conflicto sirio Abu Bark Al Bagdadi, nuevo dirigente de ISI, envió a Abu Muhamad Al Joulani a Siria con el fin de establecer un mando regional en la zona. De esta forma, Al Joulani estableció contactos con grupos yihadistas sirios y creó Jabhat Al Nusra. En 2013, Bark Al Bagdadi anunció la incorporación de Al Nusra a su organización y así surgió el Estado Islámico de Iraq y el Levante (conocido también como ISIS o ISIL). No obstante, Al Nursa juró lealtad

[403] Ídem
[404] *Ídem*
[405] *Ídem*

a Al Qaeda y de esta manera estableció su influencia en Siria mientras que ISIL lo hizo en Iraq. [406]

El enfrentamiento entre ambos grupos aumentó en suelo sirio, por lo que Ayman al-Zawahiri decidió arbitrar el enfrentamiento, inclinándose, por supuesto, a favor de Al Nusra y ordenó a ISIS volver a Iraq. Es entonces cuando Al Bagdadi rompe relaciones con Ayman al-Zawahiri, y argumentó que su obediencia se dirigía a Bin Laden. En este punto, surge Da´ish (por sus siglas en árabe *Dawlat Islami Irak wa Sham*) retomando la idea de ISIS o ISIL (Estado Islámico de Iraq y Damasco/Levante) y desafiando las órdenes de Al Zawahiri y su dominio en Siria.[407]

La creación de Daesh y su autoproclamación como Califa y "líder de todos los musulmanes" dio inicio a una nueva etapa en el historial terrorista de Al Bagdadi. En febrero 2014 la organización rompió lazos con Al Qaeda, en ese mismo año se apoderó de Raqqa donde estableció la capital del califato.[408]

En un esfuerzo por sintetizar el origen de Daesh, es posible afirmar que es producto de la invasión soviética en Afganistán que resultó en la islamización de la resistencia, impulsado por Estados Unidos y Arabia Saudí a travez de Osama Bin Laden, y de la invasión a Iraq (en 2003) y la inestabilidad política y social derivada de tal evento. Con la disolución tanto de la policía como del ejército iraquí, además del aislamiento político de la población suniita, se propició que mandos del ejército iraquí, del servicio secreto, el partido Baaz y la policía pasaran a forman parte de la organización terrorista.[409]

La fuerza se Daesh reside en buena medida en la cantidad de combatientes que conforman sus filas. En 2014 se estimó que cerca de 14 mil voluntarios extranjeros formaban parte de la organización.[410]

---

[406] *ídem*

[407] Ebrahimneyad, Mohammad. (*s.f.*). "El Estado 'Islámico' de Iraq y Siria EI, ISIS o Daesh". Islam Oriente. Fundación Cultural Oriente. [En línea]. Disponible en: <http://islamoriente.com/node/140802>.

[408] *Ídem*

[409] Salinas, Juan José. (Julio 28, 2016). "ISIS – DAESH – ESTADO ISLÁMICO. El origen de la pesadilla". *Pájaro Rojo*. [En línea]. Disponible en: <http://pajarorojo.com.ar/?p=26290>.

[410] Jordán, *Óp. Cit,* pp. 122

La estructura de Daesh es piramidal y posee conexiones baathistas derivadas del reclutamiento de ex prisioneros, especialmente de los compañeros de Al Bagdadi en la prisión de Camp Bucca durante su estancia en 2004. Las decisiones importantes son tomadas por un Consejo de Sharia que se encarga de cuestiones como la sucesión del poder, la legislación, la justicia, la ideología etc. Los territorios bajo su dominio han sido divididos en "provincias", las cuales cuentan con gobernadores, funcionarios y delegados.[411]

3.7.1. Actividad en línea: propaganda y reclutamiento en la red

En la actualidad, la actividad en línea de la organización terrorista constituye un frente más en el combate a Daesh. Desde 2011, las operaciones de propaganda y reclutamiento han conseguido atraer a 30 000 combatientes extranjeros provenientes de alrededor de 100 países a escenarios como Iraq y Siria.[412]La organización ha sabido apropiarse de los nuevos medios de comunicación global y ha sacado ventaja al empleo de comunicación cifrada y de la *deep web* para llevar a cabo campañas de radicalización en línea. El Estado Islámico emplea múltiples aplicaciones tecnológica, entre comunicación cifrada, Apps y plataformas como:

- Mappr y Photo GPS Extract, para evadir la localización geográfica
- Tor y Tails, como sistema operativo
- Criptocat, Wickr, PQChat, SwissCom y Telegram, para servicios de mensajería instantánea
- Protonmail, Hushmail y Tutanota Service, para la correspondencia electrónica

[411] Quivooijpp, Romain. (Junio, 2015). *The Islamic State*. Policy Report. S. Rajaratnam School of International Studies, pp. 7-8. [En línea]. Disponible en: <https://www.rsis.edu.sg/rsis-publication/cens/the-islamic-state/>
[412] Press TV. (Septiembre 27, 2015). "Some 30,000 foreign fighters have joined the ranks of Daesh: report". *The Syrian Observatory for Human Rights*. [En línea]. Disponible en: <http://www.syriahr.com/en/?p=33494>

- MegaService, Spider Oak, SugarSyc y Copycom, para compartir archivos[413][414]

La estrategia de comunicación del Estado Islámico en la web se basa en la explotación intensiva y simultanea de plataformas sociales, tan sólo en 2014 se detectaron en *Twitter* 46 000 cuentas a favor de Daesh. Los contenidos en línea incluyen noticias y actualizaciones, además de revistas en PDF y videos de propaganda en varios idiomas y de alta calidad.[415]

En un principio la organización tuvo presencia en redes socio-digitales como *Twitter* y *Facebook*, pero conforme la cooperación entre el sector privado y las autoridades estatales permitieron la mitigación de su presencia en línea, Daesh se trasladó a la *deep web*.

El material con el que actualmente cuenta el Estado Islámico va desde documentales, videos de combate, grabaciones con fines de propaganda, cantos que glorifican la yihad, revistas electrónicas y los lamentablemente conocidos videos de ejecuciones tanto individuales como colectivas. La narrativa empleada por Daesh es variada y depende del objetivo del material.

Así, recurriendo a la etnografía digital y mediante un ejercicio de observación de material audiovisual en línea, se analizaron tres clases de videos del Daesh y su narrativa:

1. **Videos de reclutamiento y propaganda. -** En donde las referencias religiosas son abundantes, tanto de forma visual como auditiva. Se cita en múltiples ocasiones a Alá y a diversos suras del Corán. En esta clase de videos se emplea una narrativa libertadora, en el sentido en el que coloca a

[413] Zetter, Kim. (Noviembre 19, 2015). "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits". *Wired*. [En línea]. Disponible en: <https://www.wired.com/20 15/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/>. (Consulta 01/03/2017)
[414] PANDEY, Ashish. (Julio 18, 2016). "Web of terror: ISIS lists dos and don'ts of social media for jihadis". *India Today*. [En línea]. Disponible en: <http://indiatoday.intoda y.in/story/web-of-terror-isis-lists-dos-and-donts-of-social-media-for-jihadis/1/7142 60.html>. (Consulta 01/03/2017).
[415] Quivooijpp, Romain. (Junio, 2015). *The Islamic State*. Policy Report. S. Rajaratnam School of International Studies, pp. 7-8 [En línea]. Disponible en: <https://www.rsis.edu.sg/rsis-publication/cens/the-islamic-state/> .

la yihad como una forma de acceder al paraíso. Resalta la lucha de quienes forman parte del Daesh y muestra a la organización como un lugar en donde no existe la discriminación y en el que sólo hay hermandad y camaradería. Los videos también muestran el potencial militar de la organización, y los combatientes interpretan su éxito en la conquista de territorios como una señal divina.

2. **Videos de ejecuciones individuales. -** En esta clase de material aparecen menos miembros de la organización. Generalmente, se presenta un combatiente de Daesh con el rostro cubierto. La actitud es agresiva, el lenguaje es directo y a diferencia de los videos de reclutamiento como "There Is No Life Without Jihad" quien se dirige a la audiencia sigue un dialogo previamente preparado. La narrativa de este material presenta a las acciones de combate a Daesh como una agresión en contra de la comunidad musulmana y responsabiliza a los Estados involucrados en las operaciones en su contra en Siria e Iraq de la ejecución de los rehenes capturados por Daesh.
3. **Videos de combate. -** Esta clase de videos muestra escenas de enfrentamiento. En ellos aparecen vehículos militares y armamento. Suelen estar acompañados por cantos que glorifican la yihad, también aparecen mensajes en inglés y árabe. Se muestran escenas de soldados orando y elevando la bandera de Daesh en escenarios de combate. La narrativa busca demostrar el poder militar de la organización.[416]

Los videos están elaborados con alta calidad y poseen diversos objetivos:

- Lanzar amenazas contra un Estado en particular
- Mostrar las atrocidades cometidas contra chiíes, yazidíes, cristianos, kurdos, soldados turcos, periodistas y cualquier persona que caiga en sus manos
- Ser una herramienta de propaganda, al mostrar escenas de combate y el dominio que ha logrado sobre diversos territorios al norte de Iraq y al oeste

[416] Ver Anexo III Fichas de observación del material autiovisual del Daesh

de Siria, también se muestra el armamento y los vehículos militares que posee la organización, así como la destrucción de ruinas antiguas y de patrimonio cultural

- Promover el reclutamiento, incentivando a la audiencia a incorporarse a la yihad. El mensaje se dirige tanto a la comunidad musulmana en todo el mundo como a cualquier persona que decida convertirse en un combatiente extranjero
- Adjudicarse ataques terroristas, como en el caso del ataque en Barcelona
- Mostrar las rutinas de entrenamiento y adoctrinamiento del Daesh, en esta clase de material incluso aparecen niños.[417]

La presencia del Estado Islámico en línea está influenciada por dos fuertes factores: 1) el poderío económico que ha logrado obtener por medio del saqueo y venta de piezas arqueológicas; la producción de pozos petroleros bajo su dominio y actividades criminales como secuestros y extorsiones, lo cual le ha permitido producir contenido de diversas modalidades con un nivel avanzado de producción para su constante colocación en línea, y 2) la base "religiosa" sobre la que coloca su lucha, el recurso a los pasajes del Corán y a las batallas históricas en las que se ha involucrado al islam son empleadas para posicionarse como salvadores y defensores legítimos de la Sharía, la reproducción de este tipo de mensaje tanto en árabe como en inglés busca atraer a personas del todo el mundo para adherirse a la causa "justa".[418]

Es importante mencionar que Daesh cuenta con su propia marca productora, pues en diversos videos aparece el logo "Islamic State".[419] Luego de su edición, los videos son colocados en línea en donde circulan por diversas redes socio-digitales. Sin embargo, gracias a la cooperación entre empresas como *Twitter* y *Facebook* con autoridades estatales el material es eliminado de forma relativamente rápida de dichas plataformas.

[417] *ídem*
[418] *Ídem*
[419] Ver Anexo III Fichas de observación del material autiovisual del Daesh

El proceso de radicalización, por tanto, potencia su capacidad al contar con una herramienta como Internet. En las redes socio-digitales entre el 4 de octubre y 27 de noviembre de 2014 existían aproximadamente 46 000 cuentas en *Twitter* a favor del Daesh.[420]Por lo que, a partir de 2014, se comenzaron a endurecer las medidas en contra de la actividad de la organización, sin embargo, Daesh ha encontrado formas para mantener su presencia en las plataformas más utilizadas, e incluso se ha trasladado a foros en la *deep web*.[421]

Dentro del proceso de radicalización en línea existen dos vertientes: los mensajes dirigidos a incentivar terrorismo del lobo solitario[422] y los que buscan a traer combatientes extranjeros a Siria e Iraq.

El Comité del Senado de Estados Unidos para Seguridad Nacional y Asuntos Gubernamentales ha determinado varias etapas en el proceso de radicalización en línea, éstos consisten en:

1. Pre-radicalización: es el punto de partida de los individuos a los que se dirige la radicalización, su situación de vida antes de recibir los mensajes de la yihad
2. Auto-identificación: es el momento en el que los individuos influidos por factores internos o externos comienzan a explorar el islam salafista. Entonces, gradualmente se alejan de la antigua identidad y comienzan a asociarse con individuos afines a las nuevas ideas
3. Adoctrinamiento: el individuo intensifica sus creencias y adopta totalmente la ideología yihadista-salafista

[420] Berger, J.M. y Jonathon Morga. (Marzo 15, 2015). The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter. *Analysis Paper*, p. 7. [En línea]. Disponible en: <https://www.brookings.edu/wp-conten t/uploads/2016/06/isis_twitter_census_berger_morgan.pdf>

[421] Lejarza Illaro, Eguskiñe. (Septiembre 15, 2015). "Terrorismo islamista en las redes – La yihad electrónica". Documento Opinión. [En línea]. Disponible en: <http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO100-2015_IslamismoenRed_EguskineLejarza.pdf>.

[422] Se refiere a aquellas acciones intencionadas cometidas por un individuo que: 1) actual en solitario (aunque algunos autores aceptan la posibilidad de grupos pequeños); 2) no pertenecen a alguna red o grupo terrorista (aunque pueden estar inspirado o adoctrinado por éstos); 3) actúa sin contacto directo con un líder o jerarquía; 4) las tácticas y métodos son diseñados y dirigidos por el individuo, y 5) tiene objetivos políticos, ideológicos o religiosos. Fuente: Nieves (2012)

4. Yihadización: es la fase en la que los miembros del grupo aceptan su deber individual de participar en actos terroristas y se designan a sí mismos como guerreros islámicos o muyahidín.[423]

En la última etapa el grupo comienza la planificación operativa del ataque terrorista, seguido de la preparación y la ejecución.[424] Es preciso señalar que el material audiovisual del Daesh se ha traducido a diversos idiomas como el inglés, francés, alemán, ruso, indonesio y urdu, por lo que el mensaje puede llegar a diversas audiencias.[425]

Las operaciones en línea del Daesh han logrado atraer, desde 2011, a cerca de 30 000 combatientes provenientes de más de 100 países a Siria e Iraq.[426]Este fenómeno posee consecuencias críticas para la seguridad internacional, pues además del riesgo que representa para la población a quien se dirige el mensaje, emerge otra importante cuestión: el retorno de los ex combatientes.

Entre los principales países con mayor número de ciudadanos unidos a la yihad figuran Túnez, Arabia Saudita, Rusia, Turquía y Jordania. Particularmente Turquía, es el país con mayor número de retornos, en noviembre de 2015 las autoridades encarcelaron a cerca de 500 ciudadanos acusados de haber formado parte del Daesh, en adición 100 personas más fueron juzgadas por haberse unido a las filas de Jabhat al-Nusra.[427]

---

[423] Lieberman, Joseph y Susan Collins. (Mayo 8, 2008). Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat. *United States Senate Committee on Homeland Security and Governmental Affairs*, p. 4. [En línea]. Disponible en: <https://fas.org/irp/congress/2008_rpt/violent.pdf>.

[424] *ídem*

[425] Aly, Anne; Stuart Macdonald; Lee Jarvis y Thomas M. Chen. (2016). "Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization". *Studies in Conflict & Terrorism*. [En línea]. Disponible en: <http://dx.doi.org/10.1080/1057610X.2016.1157402>.

[426] Schmitt, Eric y Somini Sengupta (Septiembre 25, 2015). "Thousands Enter Syria to Join ISIS Despite Global Efforts". *The New York Times*. [En línea]. Disponible en: <https://www.nytimes.com/2015/09/27/world/middleeast/thousands-enter-syria-to-join-isis-despite-global-efforts.html?smid=tw-share&_r=1>.

[427] The Soufan Group. (Diciembre, 2015). *Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*. [En línea]. Disponible en: <http://soufangroup.com/wp-content/uploads/2015/12/TSG_ForeignFightersUpdate3.pdf>.

La forma en la que los excombatientes pueden ser reintegrados a la sociedad en su país de origen está aún sujeta a debate. Un estudio elaborado por el *International Centre for Counter-Terrorism* de la Haya, delimita 5 posibles perfiles de los combatientes que retornan: 1) el mártir, se trata de aquel combatiente que murió en el conflicto y cuya imagen puede ser empleada con fines de reclutamiento; 2) el veterano, continua peleando en otros escenarios de conflicto, ve a la yihad como una forma de vida; 3) el reclutador, retorna a su país para alentar a la comunidad yihadista local con el fin de conseguir nuevos miembros; 4) el combatiente reintegrado, consigue retomar su vida anterior y se retira de las actividades terroristas, y 5) el terrorista, experimenta un cambio radical en su identidad, se convence que no sólo es necesario conducir la yihad en el extranjero sino también en su propio país.[428]

No sólo Daesh ha recurrido al reclutamiento y propaganda en línea, pues fue Al Qaeda quien comenzó a explotar la ventaja otorgada por la red de redes. Actualmente, organizaciones como Anṣār al-Sharī'ah, Jabhat al-Nusra, Asbat al-Ansar, Ansar al-Islam, entre otros, propagan su mensaje a través del ciberespacio.

3.7.2. Otras tecnologías

Además de Internet, el Estado Islámico cuenta con laboratorios clandestinos en donde se encarga de desarrollar nuevos tipos de tecnologías bélicas.

En Mosul existen casos en donde Daesh ha realizado experimentos con prisioneros a quienes ha expuesto a cloro y gas mostaza con el fin de desarrollar armamento químico.[429]En adición, se han descubierto instalaciones en donde se realizaba investigación con explosivos en la provincia de Anbar.[430]

---

[428] De Roy van Zuijdewijn, Jeanine y Edwin Bakker. (Junio, 2014). *Returning Western Fighters: Te case of Afghanistan, Bosnia and Somalia*. ICCT Background Note. [En línea]. Disponible en: <https://icct.nl/publications/icct-papers/returning-western-foreign-fighters-the-case-of-afghanistan-bosnia-and-somalia>.

[429] Ensor, Josie. (Mayo 22, 2016). "Isil carrying out chemical experiments on its prisoners as it moves labs into residential neighbourhoods". *The Telegraph*. [En línea]. Disponible en: <http://www.telegraph.co.uk/news/2016/05/22/isil-carrying-out-chemical-experiments-on-its-prisoners-as-it-mo/>.

[430] Adel, Loaa. (Diciembre 11, 2016). "Security forces discover 3 explosives labs near Ramadi". *Iraqi News*[En línea]. Disponible en: <http://www.iraqinews.com/iraq-war/security-forces-discover-3-explosives-labs-near-ramadi/>.

En el Fallujah, al oeste de Bagdad, se localizaron sustancias como nitrato de potasio utilizado en la fabricación de cohetes. Asimismo, se descubrió que la sustancia es de origen belga, aunque no se ha comprobado la forma en la que llegó a manos de la organización. Debido a que las regiones bajo control del Daesh son fuente de acero, la organización cuenta con abastecimiento para su industria armamentista a pequeña escala. Sin embargo, la mayor parte de los productos empleados para la manufactura de armas explosivas son de origen turco.[431] Es importante recalcar que no se ha logrado identificar la vía por la que se obtiene dicho material, pues Daesh suele apropiarse tanto de armamento como de vehículos militares cuando resulta vencedor en una batalla, por ello el origen del material en su posesión no es una prueba válida para sugerir vínculos entre Daesh y algún Estado.

En enero de 2017, fuerzas de la coalición internacional atacaron drones fabricados por Daesh, sitios de lanzamiento e instalaciones de producción de armamento en Siria e Iraq. El 4 de enero de ese mismo año, la coalición también bombardeó instalaciones que se dedicaban a la manufactura de drones. Los Vehículos Aéreos Inanimados en manos de Daesh tienen la capacidad de lanzar morteros y granadas, los cuales se han empleado para combatir a las fuerzas iraquíes. Asimismo, la organización emplea drones que adquiere a través de Internet para labores de vigilancia tanto en Iraq como en Siria[432]

Como resultado las batallas del futuro, tanto ideológicas como físicas, en contra de organizaciones como Daesh tendrán que librarse por dos frentes: en el campo de batalla e Internet, para lo cual la cooperación entre autoridades estatales, y entre éstas y el sector privado es pieza clave.

[431] Conflict Armament Research. (Diciembre, 2016). "Standardisation and Quality Control in Islamic State's Military Production". *Dispatch from The Field*. [En línea]. Disponible en: <http://www.conflictarm.com/download-file/?report_id= 2454&file_id=2457>

[432] Watson, Ben. (Enero 12, 2017). "The Drones of ISIS". *Defense One*. [En línea]. Disponible en: <http://www.defenseone.com/technology/2017/01/drones-isis/134542/>

CONCLUSIONES

El papel de la seguridad en los estudios de las Relaciones Internacionales ha estado sujeto a continuos debates. Desde su aparición formal como disciplina hasta las transformaciones generadas por la evolución de la interacción interestatal, los estudios de seguridad han debido enfrentar controversias respecto a qué constituye el propio concepto y su relación con el término poder.

Aunque la tendencia a clasificar y delimitar conceptualmente es una práctica que facilita la organización del pensamiento hacia la profundización teórica, puede representar un obstáculo para el desarrollo de estudios académicos. Ya que, en estos casos, el debate se estanca en la estructuración de un término formalmente aceptado, olvidando la evolución del acontecer internacional y sus efectos sobre el campo estudiado. Es de esta forma que, aunque transformaciones como la innovación de las comunicaciones ejercen influencia sobre los conceptos mismos de amenaza, seguridad y defensa, el análisis de sus efectos en la interacción entre Estados no debe ser relegado.

Con este fin, la presente investigación partió de la consideración de la ciencia y de las comunicaciones como agentes transformadores con un efecto histórico sostenido en la práctica belicista. Este agente posee la capacidad de modificar la doctrina, estrategia y armamento empleados en los escenarios de guerra. Así, entre los hallazgos de esta investigación se tiene que la evolución de la guerra, especialmente después de la Segunda Guerra Mundial condujo a prácticas cada vez menos políticamente aceptables debido al costo humano que acarreaban los choques entre fuerzas armadas, lo cual incentivó el desarrollo de tecnología encaminada a reducir el número de bajas en un ejército y el daño colateral resultado de las operaciones militares. Este proceso continuó hasta que la innovación militar permitió incluso ejecutar operaciones sin la presencia física de un soldado y la posibilidad de sabotear infraestructura vital a través de un código malicioso.

Asimismo, fue posible observar que la Guerra Fría produjo conflictos en donde las partes en contienda estaban conformadas por fuerzas asimétricas, mismas que en adelante se beneficiarían del potencial proporcionado por la red de redes. De

esta forma, con el paso del tiempo y la evolución tecnológica militar, los escenarios bélicos incluyeron no sólo el choque de fuerzas estatales equipadas con armamento altamente tecnológico sino de actores no estatales capaces de emplear el mismo tipo de armas.

A lo largo de esta investigación pudo observarse que la idea de cambio radical como el que sugiere la Revolución Tecnológico Informacional de los Asuntos Militares (IT-RM) es ampliamente cuestionable, ya que es imposible delimitar temporalmente la evolución de la doctrina militar, pues la influencia que hoy ejercen las Tecnologías de la Información y Comunicación (TIC) se trata de efectos visibles de un proceso que comenzó desde el propio surgimiento de la guerra. De esta manera, su ritmo de evolución no posee rangos temporales definidos, sino que se trata de un proceso que se acelera y desacelera de forma indeterminada a lo largo del tiempo.

Por ello, esta investigación considera que el papel de la IT-RMA es fungir sólo como indicador de una fuerza (la innovación de las comunicaciones) que modifica el pensamiento y la práctica militar. Teniendo esto en cuenta, es posible afirmar que el ciberespacio ocupará un lugar cada vez más importante en la doctrina e incluso generará el surgimiento de nuevos subcampos de estudio, pero no constituirá el único campo de batalla de las guerras del futuro. Así, el espectro cibernético se presenta como un complemento a las prácticas militares convencionales con efectos sobre el armamento y la estrategia.

A nivel macro, las nuevas prácticas belicistas generan un cambio en la correlación de fuerzas en el orden internacional que involucra tanto actores estatales como no estatales, y obliga al pensamiento militar a priorizar cada vez más el empleo de la innovación científica y el ciberespacio.

En el caso particular de Medio Oriente, este trabajo pudo determinar que la inserción de las comunicaciones digitales ha sido analizada en relación con la supuesta capacidad democratizadora de la red de redes y sus efectos en la estabilidad de la región, y que la mayoría de esos análisis se efectuaron cuando la penetración de Internet era limitada.

Hoy en día países como Qatar, Arabia Saudita, Israel, Turquía, entre otros, cuentan con infraestructura informacional desarrollada. En adición, la aparición del virus Stuxnet en 2010, incentivó el surgimiento debates entorno a lo que pudiera representar la militarización de Internet o bien la digitalización de la guerra.

Eventos de esta naturaleza influyen tanto la teoría como la práctica de las relaciones internacionales, generando demandas para la regulación de Internet, e incluso suscitando la estructuración de propuestas jurídicas respecto a la guerra cibernética como lo es El Manual de Tallín presentado por la OTAN en 2013.

En el campo estrictamente militar los efectos de la adopción de un paradigma digital se materializan en acciones combinadas en donde las batallas se libran por ambos frentes, el surgimiento de ejércitos electrónicos, el desarrollo de ciberarmas y su incorporación a la estrategia, dando origen a lo que esta investigación ha denominado “guerra multi-espectro”.

Sin embargo, el empleo de armamento con alto nivel de tecnología y de Vehículos No Tripulados genera consecuencias en el ámbito del Derecho Internacional Humanitario debido al daño colateral producido por su empleo, como se analizó en el caso de Iraq, en donde el número de civiles asesinados en el marco de operaciones militares es alarmante. En adición, el uso de armamento automatizado incentiva el sostenimiento de enfrentamientos de larga duración, ya que se elimina el riesgo a los miembros de un ejército y se reducen los costos a expensas del daño que se inflige a la población civil. Y en el plano de las relaciones internacionales aparecen críticas respecto al valor de una victoria táctica carente de una victoria civil.

Por su parte, el movimiento de capital hacia Empresas Militares Privadas en el marco de escenarios de combate es un tópico que demanda especial atención. Asimismo, su actuación en regiones como Medio Oriente ha resultado en problemáticas de carácter jurídico, en especial vinculadas a los Derechos Humanos, pues a raíz de la declaración de la llamada guerra contra el terrorismo grandes sumas de capital empezaron a destinarse a Empresas Militares Privadas, las cuales comenzaron a competir por la asignación de contratos en lugares como Afganistán

e Iraq, en donde miembros de estas empresas trasgredieron la ley. Este comportamiento llama reforzar los instrumentos internacionales para imponer obligaciones jurídicas a dichas empresas. Además, las EMP han comenzado a incorporar sus actividades al ámbito cibernético, donde se encargan del desarrollo de software con fines defensivos y sin duda también con fines de combate, ámbito en el que también la debilidad jurídica es una constate.

En lo que respecta al uso de armamento cibernético, la conducta constituye la evidencia más visible de una nueva modalidad de guerra moderna, pues es una herramienta que no sólo permanece en manos de los organismos de seguridad, sino que es accesible también para organizaciones criminales, grupos terroristas y prácticamente cualquier persona con las habilidades tecnológicas suficientes.

Las causas de su empleo en Medio Oriente son diversas. En el caso Stuxnet, presuntamente, ante la incapacidad de detener el desarrollo del programa nuclear iraní, Estados Unidos recurrió al uso de malware. Así, tanto los actores estatales como no estatales se benefician de anonimato de internet para ejecutar acciones en contra de infraestructura clave.

Su empleo en el marco de operaciones como Libertad para Iraq y Orchad, se debió a su efectividad militar, pues en esos casos se encargó de asistir al poder aéreo, desactivado radares, a fin de facilitar la incursión aérea. Asimismo, se encargó de aislar el objetivo afectando las comunicaciones e incluso de lanzando campañas de desinformación. También es resultado de la capacidad económica y táctica de países como Estados Unidos, Israel, Irán, Turquía, Siria, Rusia entre otros, y de la participación de Empresas Militares Privadas y Compañías especializadas en el uso de medios digitales.

La consecuencia del uso de ciberarmas en Medio Oriente presenta como curso de acción la generación de alianzas estratégicas para su desarrollo y empleo sin un marco normativo. Alianzas que no sólo pueden efectuarse entre Estados sino entre actores no estatales como Empresas Militares Privadas, grupos terroristas y ejércitos electrónicos.

Otro rasgo muy importante del uso de Internet dentro de las estrategias de guerra es presentado por Daesh. Para la organización terrorista Internet constituye una nueva herramienta para propagar el miedo y emprender campañas de reclutamiento, generando lo que esta investigación ha denominado formas de "violencia transmedia". Esta práctica tiene como objetivo perpetuar la violencia cometida por la organización terrorista a través de imágenes y videos que se propagan por la red y emprender campañas de radicalización en línea, creando una amenaza invisible que se propaga en y por la red.

Se trata de un fenómeno que comenzó con Al Qaeda y en otros casos como los abusos en Abu Ghraib donde la reproducción de imágenes representó la perpetuación y propagación de actos de violencia. Esta táctica fue adoptada por Daesh y aplicada a mayor escala en su actividad terrorista, se trata de violencia transmedia porque replica asesinatos individuales y colectivos a través de diversos medios: imágenes, mensajes, videos y audio, cuyo único propósito es propagar el miedo. Es transmedia por que traslada los actos terroristas que también se presentan en los medios tradicionales como la televisión, la radio y la prensa a Internet y las redes socio-digitales, y se coloca de forma transversal en un flujo de comunicación que parte de Daesh y se dirige a amplio número de receptores.

Por lo que es posible señalar que la evolución del armamento cibernético estará influenciada, más no determinada, por la estructuración de un marco legal en la materia. Si anteriormente, era posible esconder laboratorios e incluso armamento de la vista de las autoridades regulatorias internacionales, siempre existieron factores que ayudaban a descifrar la situación como la compra de material e incluso el movimiento de vehículos por determinada área o la construcción de instalaciones sospechosas. En la era de armas cibernéticas desvelar la capacidad del enemigo es prácticamente imposible más aún el atribuir la responsabilidad de un ataque a un Estado. Por lo tanto, el armamento cibernético se presenta como un arma invisible que puede emplearse tanto de forma aislada como complemento a estrategias militares complejas.

En síntesis, el resultado de esta investigación confirma la hipótesis respecto a que la Revolución Tecnológico Informacional de los Asuntos Militares ha transformado la concepción, generación y empleo de la fuerza en el siglo XXI. Sin embargo, no se trata de un momento revolucionario sino de la percepción de los efectos más visibles de un proceso que comenzó desde la aparición misma de la guerra, cuyo ritmo de evolución está marcado por eventos destacados como la Operación Tormenta de Desierto.

En Medio Oriente su aplicación ha derivado en el aumento de recursos destinados a la adquisición y uso de medios de alta tecnología por parte de las Fuerzas Armadas de países con capacidades económicas, pero también por parte de actores no estatales. Un efecto significativo de esta evolución en la región es, la ya mencionada, “violencia transmedia” por parte de Daesh con el fin de propagar el terror. Sin olvidar el papel cada vez más importante que juegan las Empresas Militares Privadas, que se enriquecen dentro de un débil marco legal que regule su actuación.

Esta investigación deja pendiente cuestiones importantes como profundizar respecto a las doctrinas de ciberseguridad nacional de países con fuertes antecedentes de ataques cibernéticos como Irán, Israel, Arabia Saudita, entre otros. También queda pendiente analizar los esfuerzos por parte de actores como la Unión Europea, Estados Unidos y Arabia Saudita para incentivar el desarrollo de instrumentos jurídicos y de prácticas que garanticen la regulación del ciberespacio en otros países. Esto con el fin de contrarrestar los ataques cibernéticos en contra de infraestructura clave e incluso para combatir actividades de ciberespionaje, como alternativa a la falta de un marco jurídico internacional.

En el plano sociológico, también surge la inquietud respecto a la expresión del nacionalismo en el espectro digital, la construcción de identidades en la red de redes y su relación con prácticas como el hacktivismo o los ejércitos electrónicos.

En el campo de la seguridad, queda pendiente analizar el desarrollo y construcción de la doctrina de ciberseguridad en Israel, ya que es uno de los países con mayor desarrollo tecnológico y, en el plano de la seguridad, posee el mejor

ejército en Medio Oriente. Por esta razón, resulta importante examinar la forma en cómo las estrategias ciberseguridad refuerzan la doctrina militar israelí.

ANEXO I. ALGUNOS EJEMPLOS DE ARMAS CIBERNÉTICAS

NOMBRE	AÑO/LUGAR	TIPO	OBJETIVO	DETALLES
WannaCry	2017-varios países	Ransomware (control de información)	Controlar datos	Fue detectado en mayo de 2017, afectó a más de 200 000 organizaciones en 150 países. El malware explotó una brecha de seguridad en el sistema Microsoft. Una vez que tomaba control de la información, los ciberdelincuentes demandaban un pago para la liberación de los datos. El malware era implantado en los sistemas a través de un correo electrónico malicioso, una vez ahí encriptaba el Disco Duro. (McGoogan, Titcomb y Krol: 2017)
Wiper malware	2013-Corea del sur	Wiper (limpiador)	Borrar datos	El ataque fue detectado el 20 de marzo de 2013. Los sistemas afectados pertenecían a bancos y televisoras, se estima el malware afectó 48 000 equipos. (Mimoso:2013) El virus sobrescribió el Registro de Arranque Maestro (*Master Boot Record*, MBR) quien hace posible, a través de la identificación de la partición activa, iniciar el programa de arranque permitiendo que el sistema operativo funcione. (Symantec:2017) El malware también desactivó el antivirus. A esta naturaleza pertenecen ataques como los lanzados contra Aramco y contra la compañía qatarí RasGas. (Iasiello: 2015)
Bundestrojaner ligh	2011-Alemania	Caballo de Troya	Control, comando y vigilancia	En 2010 la *Chaos Computer Club* recibió información que acusaba al gobierno alemán de emplear un malware para vigilar a los ciudadanos. Un análisis realizado por misma organización arrojó que el Caballo de Troya utilizado tenía la capacidad de desviar datos personales, establecer comandos de control remoto y tomar el control del sistema para ejecutar otros programas. En 2008 el Tribunal Constitucional alemán prohibió su uso. (Meyer:2011)
Stuxnet	2010-Irán	Worm (gusano)	Control de sistemas SCADA	Stuxnet posee un diseño altamente sofisticado y tiene como objetivo principal atacar sistemas SCADA Siemens. La arquitectura de Stuxnet comprende cuatro *Zero Days* (brechas de seguridad), también emplea *rootkits* (técnicas avanzadas de ocultación contra el usuario y los antivirus), y emplea dos certificados digitales robados para firmar sus controladores. (Mueller y Yadegari: 2012)
DDoS	2008- Georgia	Denegación de servicio	Inhabilitación de sitios web	El ataque fue detectado en agosto de 2008. En el contexto de la Guerra de Osetia del Sur los sitios web de diversas instituciones gubernamentales, medios de comunicación y entidades financieras georgianas recibieron ataques DDoS. (Iasiello: 2015). Estos ataques consisten en cientos de solicitudes de conexión a una página web que terminan sobrecargando la plataforma hasta que finalmente colapsa, dichas solicitudes de información provienen de botnets que operan a través de comandos de control remoto. (Reyes:2017)

Fuente: Elaboración propia

ANEXO II. BASES IDEOLÓGICAS DEL ESTADO ISLÁMICO

IBN TAIMIAH (IBN TAYMYAH)	MUHAMMAD IBN ABDUL WAHHAB	ABDULLAH YUSUF AZZAM	SAYYID QUTB	OSAMA BIN LADEN	ABU MU'SAB AL-ZARQAWI
Su nombre en árabe es تقي الدين أحمد ابن تيمية, mejor conocido como Ibn Taymyah nació el 22 de enero de 1263 y murió el 26 de septiembre de 1328. Fue un erudito y teólogo islámico, vivió principalmente en Damasco. Fue miembro de la escuela fundada por Ahmad ibn Hanbal y es considerado por sus seguidores, junto a Ibn Qudamah, uno de los dos más grandes proponentes del Hanbalismo[433]. Taymyah, buscó el regreso del islam suní[434] a interpretaciones anteriores del Corán y la Sunna[435]. Se considera que su trabajo tuvo una fuerte influencia sobre Muhammad ibn Abd al-Wahhab, fundador de Wahabismo.[436] Las razones por las que Taymyah es un personaje trascendente son: 1.- La creencia en Dios en forma humana (antropomorfismo) 2.- Creer que no debe haber intercepción en lo absoluto de lo escrito en el Corán (aplicación directa)	Nació 1703 en ʿUyaynah, Arabia (hoy Arabia Saudita) y murió 1792. Fue teólogo y fundador del movimiento Wahhābī que intenta volver a los principios "verdaderos" de islam. Cuando terminó su educación formal en la ciudad santa de Medina se dedicó a la enseñanza en Barsa (Iraq), en 1736 comenzó a enseñar en contra de lo que consideró ideas extremas de exponentes pertenecientes a la ideología sufí. Al retornar a su ciudad natal escribió el Kitāb at-tawḥīd ("El libro de la unidad"), que constituye el principal texto de la doctrina Wahhābī. Ibn Abdul Wahhab estableció una postura clara contra todas las innovaciones (bidʿah) del islam e insistió en que la grandeza del islam sólo podía ser recuperada si la comunidad volvía a los principios enunciados por el profeta Muhammad. Por lo tanto, la doctrina Wahabí no permite un intermediario entre los fieles y Alá y condena el politeísmo. (The Editors of	Nació en Palestina en 1941 y murió en 1989, durante su vida desempeñó un papel central en el desarrollo y propagación del concepto islámico moderno de la "yihad". Azzam se dedicó a promover la lucha islámica contra el secularismo, el socialismo y el materialismo, llevó sus ideas a la práctica durante la guerra afgano-soviética, dónde organizó la agencia que más tarde se convertiría en Al Qaeda. (McGregor: 2013) Obtuvo un doctorado en *fiqh* (jurisprudencia islámica) por la Universidad de Al-Azhar en Egipto en 1973, donde estableció lazos personales con la familia Qutb, el jeque 'Umar Abd el-Rahman[438] y Ayman al-Zawahiri. El legado de Azzam es la internacionalización del movimiento islamista, así como la autoridad religiosa que prestó al movimiento. (Stanley:2005) Murió en noviembre de 1989, en un atentado con coche bomba en Peshawar, Pakistán junto a dos de sus hijos. (Rubin: 2013).	Nació en 1906 y murió 1966 en Egipto, fue uno de los principales ideólogos islamistas del siglo XX. Durante la primera mitad de su vida adulta formó parte del movimiento literario secular egipcio, además fue crítico literario y social. Sin embargo, en 1948 adoptó una posición islamista, cuyas ideas reflejó en su obra *Social Justice in Islam*. Luego de estudiar dos años en Estados Unidos a su regreso a Egipto se unió a la Hermandad Musulmana. En 1954 fue encarcelado junto a otros miembros de la Hermandad y condenado a 10 años en prisión. Sin embargo, durante su reclusión se le permitió escribir, durante este tiempo sus escritos se radicalizaron e incluso se volvieron revolucionarios, pues alegó que las llamadas sociedades musulmanas eran anti-islámicas (jahili). Luego de ser liberado en 1964 fue nuevamente apresado, acusado de cargos de conspiración y ejecutado en 1966. Su obra ha	Nació en 1957 en Riyadh (Arabia Saudita). Estudió Economía y administración pública en la Universidad de Abdel-Aziz en Jeddah (Adamec: 2012), en donde en 1980 tuvo como maestros de Estudios Islámicos a Abdullah Azzam y Mohammed Quttub[439]. Durante las primeras semanas de la invasión soviética viajó a Afganistán para reunirse con algunos líderes de la resistencia, a su regreso a Pakistán trabajó en la idea de una escuela para apoyar a los muyahidines, entonces comenzó a reunir combatientes y fondos que llevó a Afganistán. En 1986, estableció sus propios campos de entrenamiento en Afganistán, tras la retirada soviética en 1989 regresó a Arabia Saudita, sin embargo, luego de un frustrado intento por defender el reino frente a la posible invasión iraquí, regresó a Afganistán. En 1994, el régimen saudí le retiró la ciudadanía, en adelante Osama lucharía por evadir diversos planes de asesinato en su contra orquestados por EE. UU, Arabia Saudita y Pakistán	Nació en Jordania en 1966, su verdadero nombre era Ahmed Fadeel Nazal al-Khalayleh. No existe mucha información sobre su formación académica (Evans: 2006), a los 20 años viajó a Afganistán para unirse a los muyahidines que luchaban contra el ejército soviético fue entrenado en un campo creado por Osama bin Laden y Abdullah Azzam. En 1991 volvió a Jordania y se incorporó a la Jihad Islámica Egipcia, que se fusionó con Al Qaeda en el 98, tras un intento de ataque terrorista en Amman huyó a Pakistán. En el 2000 se trasladó a Afganistán donde estableció campos de entrenamiento con financiamiento de Al Qaeda, después de la invasión a Iraq, Zarqawi intensificó su actividad terrorista. Tras los ataques del 9/11 él y sus combatientes se unieron a Al Qaeda y al Talibán en Afganistán. En 2004 secuestró y asesinó a Nicholas Evan, ciudadano estadounidense, como protesta a las torturas en Abu Ghraib, por lo que EE. UU ofreció 25 millones de

3.- La creencia de que si alguien no acepta la versión exacta del Corán debe de ser perseguido y asesinado, y 4.- La creencia en Qiyas o el razonamiento inductivo.[437]	Encyclopædia Britannica: 2007a)		inspirado diversos grupos radicales violentos en todo el mundo. (Shepard:2010)	(Aronson-Rath: 2014a). Murió el 1 mayo 2011 en la Operación Lanza de Neptuno ejecutada por EE. UU (Schmidle: 2011).	dólares por su cabeza. En 2005 ejecutó diversos ataques contra Jordania. (Wallace:2017) Finalmente, en 2006 murió junto a otros líderes insurgentes en un ataque aéreo realizado por EE. UU en Baquba, Iraq. (Muir: 2010)

Fuente: Elaboración propia

[433] Hanbalismo: fue fundado por Ahmad ibn Hanbal (Bagdad 780-855) que se oponía radicalmente a cualquier forma de intromisión de la razón humana, considerándola arbitrariamente subjetiva -en la interpretación de las dos fuentes primarias del islam, el Corán y la Sunna. El Hanbalismo se caracteriza por un coherente rechazo del intelectualismo teológico. Fuente: Fayaz (2015).

[434] El islam suní constituye el mayor grupo dentro del islam. *Sunní* quiere decir tradición, ha sido considerado como la ortodoxia más tradicionalista. El sunismo siempre ha considerado que el cargo de sucesor del Profeta debe estar en manos de un líder elegido por consenso entre varios candidatos (*Shura*). Fuente: Castellanos (2010: 40-41).

[435] Islamic Philosopher. (Diciembre 9, 2015). "Ibn Taymiyyah: The Founder Of ISIS". *Islamic Philosophy.* [En línea]. Disponible en: <http://islam.hilmi.eu/ibn-taymiyyah-the-founder-of-isis/>.

[436] *Ídem*

[438] Omar Abdel-Rahman, también conocido como "el jeque ciego" fue un clérigo radical egipcio, condenado en Estados Unidos por su vinculación al atentado de 1993 contra el World Trade Center en Nueva York. A lo largo de su vida sostuvo vínculos con dos grupos terroristas Yihad Islámica y Gamaa al Islamiya. Abdel-Rahman murió en 18 de febrero de 2017, a los 78 en una prisión en Carolina del Norte. Fuente: Espinosa (2013) y Trott (2017).

[439] Mientras que Sayyid Qutb desempeñó un papel importante en la construcción intelectual de Al Qaeda, Muhammad Qutb (su hermano menor) también tuvo un papel significativo en la conformación de la organización debido a que, como maestro, educó tanto a Bin Laden como a Safar al- Hawali. Fuente: Nishino (2015).

[437] *Ídem*

ANEXO III. FICHAS DE OBSERVACIÓN DEL MATERIAL AUDIOVISUAL DEL DAESH

Las siguientes fichas son parte de una investigación realizada en diversas plataformas en línea con el fin de analizar la narrativa empleada en los videos del Daesh. De esta forma, bajo la guía de la etnografía digital y mediante métodos de observación no participante, se condujo el estudio en plataformas como *You Tube*, *LiveLeak*, y el blog *jihadology*. Esta observación comenzó a realizarse en febrero de 2017 y concluyó en mayo del mismo año bajo la supervisión de la Doctora Karina Bárcenas Barajas del Instituto de Investigaciones Sociales de la Universidad Nacional Autónoma de México.

Categoría: ejecuciones individuales

Título: A Message to America		
Tipo de video: video de ejecución	**Fecha:**19/ agosto/2014	**Duración:** 2:39 minutos
URL: https://www.liveleak.com/view?i=41b_1408515878&comments=1	**Plataforma de consulta:** LiveLeak	
País/ubicación: Iraq	**Autor:** Daesh	**Planos:**2
Fecha de reproducción:13 de febrero de 2017		
Contexto: James Foley, periodista estadounidense, fue capturado en Siria en noviembre de 2012 en Binesh, en el norte de Siria[440]. Tras la orden del entonces presidente de Estados Unidos, Barack Obama, de bombardear Iraq para proteger Erbi, en agosto de 2014,[441] comienza la actividad del Estado Islámico en Internet. Es el 19 de agosto de 2014 cuando en la web aparece el video de la ejecución del periodista estadounidense.		
Contenido: El video inicia con un fondo negro y la leyenda "A message to America" con la traducción en árabe. Posteriormente, aparecen dos hombres. Uno arrodillado y vestido con uniforme naranja, James Foley, quien se ubica a lado derecho del miembro de Daesh. El otro sujeto, miembro de Daesh, aparece vestido de negro de pie junto a Foley, su cara está cubierta. En el lado superior izquierdo aparece la bandera del Estado Islámico y un poco más abajo un recuadro que presenta el nombre de Foley (también traducido al árabe). Foley inicia el mensaje hacia su familia, cuando menciona a su hermano, quien trabaja en la Fuerza aérea de Estados Unidos, aparece la imagen de éste del lado izquierdo, vestido con ropa militar. Después que Foley termina su mensaje el miembro de Daesh coloca su		

[440] Winter, Michael y Kevin Johnson. (Agosto 19, 2014). "Video appears to show Islamic State beheading U.S. journalist". *USA TODAY*. [En línea]. Disponible en: <http://www.usatoday.com/story/news/world/2014/08/19/syria-isis-kidnapped-journalist-beheaded/14306021/>

[441] *Íbidem*

<table>
<tr><td colspan="3">mano derecha sobre el hombro izquierdo de Foley y con la otra mano sostiene un objeto punzocortante con el que se dirige a la cámara y a Foley mientras emite su mensaje, al terminar su mensaje asesina a Foley, en el siguiente cuadro aparece su cuerpo.
En los últimos segundos del video se muestra a otro periodista estadounidense desaparecido Steven Joel Sotloff, de Miami, (igualmente aparece un recuadro en árabe e inglés que le identifica). Steven está tomado del cuello de su vestimenta mientras el integrante de Daesh dirige otro mensaje.</td></tr>
<tr><td>No. de personas: 3</td><td>Lugar: Desértico, no identificado</td><td>Acción: amenaza a Estados Unidos mediante la ejecución de James Foley</td></tr>
<tr><td colspan="3">Transcripción:

James: “Llamo a mis amigos, familia y seres queridos a que se levanten en contra de mis verdaderos asesinos, el gobierno de Estados Unidos. Porque lo que me sucederá es sólo el resultado de su complacencia y criminalidad”.
“Mi mensaje para mis queridos padres: conserven algo de dignidad y no acepten ninguna pobre compensación por mi muerte de parte de las mismas personas que, efectivamente, martillaron el último clavo en mi ataúd con su reciente campaña aérea en Iraq”
“Llamo a mi hermano John, que es miembro de la Fuerza Aérea estadounidense. Piensa en lo que estás haciendo, piensa en las vidas que destruyes, incluyendo las de tu propia familia. Te llamo John, piensa en quién tomó la decisión de bombardear Iraq recientemente y matar a todas esas personas, quien quiera que haya sido. Piensa John, ¿a quiénes mataron realmente? Y ¿ellos pensaron en mí, en ti, en nuestra familia cuando tomaron esa decisión?”
“Morí ese día John, cuando tus colegas dejaron caer esa bomba en esas personas, firmaron mi certificado de muerte. Ojalá tuviera más tiempo. Ojalá pudiera tener la esperanza de la libertad y ver a mi familia una vez más, pero este barco ha partido. Considerándolo todo deseo no haber sido estadounidense”[442]

Daesh: “Este es James Wright Foley, un ciudadano estadounidense de su país. Como gobierno ha estado al máximo de su agresión hacia el Estado Islámico, ha conspirando contra nosotros y se ha esforzado mucho para encontrar razones para intervenir en nuestros asuntos.”</td></tr>
</table>

[442] Catholic Online. (Agosto 20, 2014). “Islamic State beheads journalist James Foley (WARNING, GRAPHIC VIDEO)”. [En línea]. Disponible en: <http://www.catholic.org/news/international/middle_east/story.php?id=56609>

"Hoy su fuerza aérea militar ha atacado diariamente en Iraq, sus tanques han causado muerte entre musulmanes. Ya no luchan contra una insurgencia, nosotros somos un ejército islámico y un estado que ha sido aceptado por un gran número de musulmanes en todo el mundo. Así que efectivamente cualquier agresión contra el Estado Islámico es una agresión hacia los musulmanes de todos los sectores de la sociedad que han aceptado el califato islámico como su líder." "Así que cualquier intento tuyo, Obama, de negar a los musulmanes el derecho de vivir con seguridad bajo el califato islámico resultará en un baño de sangre de tu gente" [Ejecución de Foley] Daesh: "La vida de este ciudadano estadounidense, Obama, depende de tu próxima decisión" James Foley fue ejecutado como consecuencia de la decisión del presidente Barack Obama de bombardear a combatientes del Estado Islámico que combaten a las fuerzas kurdas en el norte de Bagdad.[443]
Objetivo del video: Intimidación al gobierno de EE. UU para el cese de bombardeos contra Daesh y el mensaje de que el responsable de tales actos es Barack Obama por las acciones militares llevadas a cabo en Iraq.
Relación entre acción y hechos: Se trata de la primera ejecución del Daesh con el fin de advertir al gobierno estadounidense la consecuencia de su intervención en los "asuntos" del Estado Islámico. El gobierno de Estados Unidos decidió iniciar el bombardeo con el fin de apoyar a las fuerzas kurdas que combaten contra éstos en el norte de Bagdad
Comentarios:

[443] Winter Michael y Kevin Johnson. (Agosto 19, 2014). "Video appears to show Islamic State beheading U.S. journalist". *USA TODAY*. [En línea]. Disponible en: <http://www.usatoday.com/story/news/world/2014/08/19/syria-isis-kidnapped-journalist-beheaded/14306021/>

Clasificación: A Second Message to America		
Tipo de video: video de ejecución	**Fecha:**2/septiembre/2014	**Duración:** 1:42 (2:50)
URL: https://www.youtube.com/watch?v=z1pMuDfxAvo	**Plataforma de consulta:** Youtube	
País/ubicación: Iraq	**Autor:** Daesh	**Planos:**5 (6)
Fecha de reproducción:13 de febrero de 2017		
Contexto: En diciembre de 2014, Estados Unidos y Francia bombardearon posiciones del Estado Islámico en Iraq,[444]pocos días más tarde se publicó otro video. En esta ocasión aparece Steven Sotloff, periodista estadounidense, quien había sido amenazado en el video anterior.[445] Sotloff desapareció en agosto de 2013 cerca de la frontera sirio-turca donde trabajaba como *freelance* para las revistas *Time* and *Foreign Policy*.[446]		
Contenido: El video se titula "Un segundo mensaje a Estados Unidos". En la pantalla aparece un símbolo en color dorado en el extremo superior izquierdo de la pantalla, este símbolo alterna su aparición junto a la bandera del Estado Islámico y otra figura con la palabra "SITE" del lado superior derecho. También aparece un recuadro blanco con el nombre y nacionalidad de Steven Sotloff, estos datos aparecen en el mismo cuadro en árabe. Se enfoca la cara de Sotloff quién se dirige a la cámara, él aparece de rodillas, vestido de naranja acompañado de un hombre vestido de negro, encapuchado que está de pie a su lado izquierdo, sosteniendo un arma blanca. El video cambia a un segundo plano en el que se observan a los dos individuos en un lugar desértico. El hombre de negro comienza a hablar, entonces se dirige a la cámara con el arma, se cambia a un tercer plano en esta ocasión se puede observar a los dos hombres de frente. En su discurso se refiere a Sotloff señalándole con el arma y señalando la cámara. Se cambia a un plano más cercano de frente dónde se lleva a cabo la ejecución, un plano más se muestra a otro rehén: David Cawthome Haines de nacionalidad inglesa como refieren los datos que aparecen en un recuadro blanco de nuevo traducido al árabe. Haines está hincado y es sostenido por el cuello de la camisa por el hombre de negro.		

[444]La Vanguardia. (Junio 29, 2016). "Cronología de los dos años del califato del Estado Islámico

[445]Lewis, Paul; Spencer Ackerman, yi Ian Cobain. (Septiembre 3, 2014). "Steven Sotloff: Isis video claims to show beheading of US journalist". *The Guardian*. [En línea]. Disponible en: <https://www.theguardian.com/world/2014/sep/02/isis-video-steven-sotloff-beheading>.

[446]*Ídem*

<table>
<tr><td colspan="3">En un plano se muestra el cuerpo sin vida de Sotloff.</td></tr>
<tr><td>No. de personas: 3</td><td>Lugar: Desierto</td><td>Acción: Ejecución</td></tr>
<tr><td colspan="3">Transcripción:
Steven–“Soy Steven Sotloff, estoy seguro de que ya saben exactamente quién soy y por qué aparezco frente a ustedes. Y ahora es el momento de mi mensaje: Obama se suponía que tu política exterior de intervención en Iraq era para la preservación de vidas estadounidenses y sus intereses. Así que, ¿por qué es que estoy pagando con mi vida el precio de tu interferencia?, ¿no soy un ciudadano estadounidense? Has gastado millones de dólares de los contribuyentes y hemos perdido a miles de nuestras tropas en nuestra lucha contra el Estado Islámico ¿así que dónde está el interés de la gente para recomenzar esta guerra?”

“Por lo poco que sé de política exterior recuerdo un tiempo en que no podías ganar una elección son prometer traer de vuelta a casa desde Iraq y Afganistán a nuestras tropas y cerrar Guantánamo. Ahora aquí estás Obama, cerca del fin de tu mandato y habiendo logrado ninguna de esas cosas. Engañándonos, haciéndonos marchar a nosotros, el pueblo estadounidense, al fuego ardiente.”

Daesh – “He vuelto Obama y estoy de vuelta debido a tu arrogante política exterior hacia el Estados Islámico. Debido a tu insistencia de continuar y […] en la represa de Mosul, sin importar nuestras serias advertencias. Tú, Obama, por tus acciones obtendrás la muerte de otro ciudadano estadounidense. A medida que tus misiles continúen golpeando a nuestra gente, nuestro cuchillo continuará golpeando los cuellos de tu gente.”

“Aprovechamos esta oportunidad para advertir a aquellos gobiernos que entren a esta malvada alianza con Estados Unidos contra el Estado Islámico de que se retiren y dejen a nuestra gente en paz.”</td></tr>
<tr><td colspan="3">Objetivo del video: Reiterar la amenaza en contra de Estados Unidos por los bombardeos contra Daesh. En adición, se lanza una amenaza a otros gobiernos (en especial Reino Unido) de las consecuencias de unirse a la alianza con EE. UU, pues de hacerlo lo pagarán ciudadanos/periodistas capturados por Daesh.</td></tr>
<tr><td colspan="3">Relación entre acción y hechos:</td></tr>
</table>

El Primer Ministro británico, David Cameron condenó la ejecución como "un acto despreciable", mientras que los servicios de inteligencia de Estados Unidos en un primer momento se dedicaron a investigar la autenticidad de la grabación. Dos semanas antes de la grabación el gobierno estadounidense emprendió una campaña sin éxito en Siria para liberar a los rehenes estadounidenses. Hacia finales de agosto de 2014, el gobierno de Obama había realizado 123 ataques aéreos en contra de posiciones, artillería y vehículos del Estado Islámico.[447]
Comentarios:

Categoría: Reclutamiento

Clasificación: There Is No Life Without Jihad		
Tipo de video: Reclutamiento	**Fecha:**17/octubre/2016	**Duración:** 13:26
URL: https://archive.org/details/ThereIsNoLifeWithout Jihad	**Plataforma de consulta:** Archive.org	
País/ubicación: desconocido	**Autor:** Daesh	**Planos:** 2
Fecha de reproducción:13 de febrero de 2017		
Contexto:		
Contenido: El video comienza con un fondo negro y letras en árabe, comienza a recitarse el mensaje en árabe y en la pantalla aparece la traducción al inglés junto a fotografías de combatientes de Daesh, también aparecen personas de distinto origen étnico. Se muestra el equipo militar de Daesh, posteriormente aparece el logo de *Alhayat Media Center*. El siguiente plano es un sendero en medio de la maleza por el que se aproximan combatientes del Daesh, con armas en las manos, algunos con los rostros descubiertos y vistiendo ropa militar, en el extremo superior derecho de la pantalla aparece el logo de Alhayat. Estos combatientes aparecen en el siguiente plano sentados en el piso, la bandera del Estado Islámico está a sus espaldas. Entonces, un recuadro identifica al sujeto que habla con		

[447] Lewis, Paul; Spencer Ackerman, yi Ian Cobain. (Septiembre 3, 2014). "Steven Sotloff: Isis video claims to show beheading of US journalist". *TheGuardian*. [En línea]. Disponible en: <https://www.theguardian.com/world/2014/sep/02/isis-video-steven-sotloff-beheading>.

un texto en inglés como: “el hermano Abu Muthanna al Yemeni de origen británico” un texto más abajo dice: “Muhajid en el Estado Islámico de Iraq y Sham”. Después de unas palabras el plano cambia y se aproxima al rostro de Abu Muthanna, el plano cambia nuevamente mostrando de frente a tres sujetos incluido Muthanna. Los tres sujetos llevan la cabeza cubierta. La siguiente escena enfoca el rostro de Abi Muthanna, después de unas palabras aparece la escena de una reunión.
En las imágenes de la reunión es de noche, aparece más de una docena de combatientes algunos con los rostros cubiertos, elevando sus armas y blandiendo la bandera del Estado Islámico (EI). El siguiente plano se enfoca en otro de los compañeros de Muthamma, quien cubre su cabeza, usa lentes de sol y tiene un arma recargada en su hombro derecho, él sonríe y comienza su discurso, en seguida aparece un recuadro en inglés que le identifica como: “El hermano Abu Bara’al Hindi, de origen británico” y nuevamente el texto con la leyenda: “Muhajid en el Estado Islámico de Iraq y Sham”, el plano se aleja y se puede observar a Muthanna. En la siguiente escena aparecen nuevamente los tres combatientes de frente, en el siguiente plano aparece Abu Bara y un sujeto a su derecha con el rostro cubierto. Aparecen nuevamente escenas de la reunión nocturna de combatientes, en el fondo hay cantos y éstos aumentan de volumen al mostrar las escenas de la reunión y las banderas del EI en manos de un sujeto que la balancea en sus manos.

La siguiente escena comienza con el sujeto sentado en el extremo derecho, viste de negro, lleva la cabeza cubierta y el cuadro lo identifica como “El hermano Abu Yahyaash Shami de origen australiano” y más abajo otra leyenda que dice “Recibido de shahadah, peleando la shawat en Al-Khayr (que Alá lo acepte)”. El siguiente plano muestra a Abu Yahya de frente a su lado derecho otro combatiente, entonces saca un pequeño Corán de su chaqueta, se muestran nuevamente imágenes de la reunión nocturna, los cantos permanecen de fondo y aumentan su volumen.

En la siguiente escena aparece el combatiente con el rostro cubierto y sosteniendo un arma con su mano derecha, a su lado otro combatiente, éste de piel morena y mirando hacia abajo, viste de forma militar y su cabeza está cubierta. El recuadro lo identifica como “El hermano Abu Nour al Iraquí de origen australiano” y más abajo la leyenda: “Muhajid en el Estado Islámico de Iraq y Sham”.

En la siguiente escena habla el combatiente sentado de lado derecho de Abu Muthanna, el recuadro le identifica como “El hermano Abu Dujana al Hindi de origen británico”, aparece igualmente la leyenda “Muhajid en el Estado Islámico de Iraq y Sham”.

La siguiente escena toma a Abu Yahya hablando y puede observarse Abu Dujana, el siguiente corte de toma muestra a Abu Yahya continuando su discurso y puede observarse a Abu Muthanna.

Finalmente, los cantos aumentan su volumen y se muestra a los combatientes sonriendo. Al término del video se muestra la foto de otro sujeto vestido de militar con letras en inglés que dicen "Próximamente hermano Abu Khaled Al Cambodi de Australia"		
No. de personas: 6	**Lugar:** Una especie de selva	**Acción:** video de reclutamiento

Transcripción:

Inicio: pantalla fondo negro y texto blanco en árabe

¡Oh tú!, que has creído, responde a Alá y a su mensajero. Responde a Alá y a su mensajero, cuando te llama a lo que te da vida. Sura Al-Anfal:241

Logo Alhayat Media Center.

Abu Muthanna al Yemeni: [Palabras en árabe]

Abu Muthanna al Yemeni:

"Aparte de implementar la ley de Alá Azzawa Jal y luchar contra los enemigos de Alá, no ves a nadie más que lo haga como nosotros walillahilham. Y somos un estado que está implementando la Sharia en Irak y Sham. Y mira a los soldados, no entendemos fronteras."

"Wililahilham, hemos participado en batallas en Sham e iremos a Irak en unos días y vamos a luchar allí [indescifrable] y a volver e incluso iremos a Jordania y a Líbano sin problemas. Donde sea que nuestro […] quiera enviarnos. Y de nuevo, quiero enviar un mensaje a mi [inaudible, Abu Bakr al-Baghdadi[indescifrable] te envío este mensaje y quiero que sepas que la esperanza de esta ummah está en tu cuello, Por Alá, la esperanza de esta ummah está en tu cuello. Esperamos en el califa [sic] Es inminente si es por nosotros o por quienes nos siguen, entre [indescifrable] será inminente. Y por Alá, te hablo desde el corazón [indescifrable] quiero que sepas: no temas la culpa de los culpables y sé firme y no cambies del todo."

Abu Muthanna al Yemeni: "Estamos contigo, somos tu [indescifrable] arrójanos a tus enemigos donde sea que estén y [indescifrable]"

Abu Bara'al Hindi: "Primero [árabe] hermanos y hermanas, abre el Corán y lee [indescifrable] de yihad. Entonces todo se aclarará para ti, [indescifrable] en Reino Unido, cuando solía leer [indescifrable] del Corán, solía sentirme como un [indescifrable] y cuando solía leer[indescifrable] de la yihad, porque no lo hacía, me sentía como un [indescifrable] y es por lo que leer hizo todo más claro, todos esos eruditos diciéndote "Esto es falso, este no es tiempo de hacer yihad" olvídalos a todos. Lee el Corán, lee el libro de Alá, la instrucción de vida y descubrirás lo que es la yihad, y si estamos destinados o no a hacer la yihad."

Abu Bara'al Hindi: "Todos ustedes hermanos, wallah [indescifrable] Porque Alá no los necesita para pelear por él. Ustedes necesitan pelear por Alá [indescifrable] Dawlah no te necesita, no necesita tu dinero, pero tú necesitas gastar en Alá por tu [indescifrable]. Esta dunya es sólo una prueba y Alá te envía a esta dunya para ver cuánto estás dispuesto a sacrificar por Alá [indescifrable] ¿Vas a

sacrificar el trabajo que has obtenido, el gran auto que has obtenido y la familia te tienes?, ¿estás dispuesto a sacrificar esto por el bien de Alá?"

"Definitivamente, si sacrificas algo por Alá, Alá va a darte 700 veces más que eso. Para todos mis hermanos que viven en Occidente, sé cómo te sientes [indescifrable]. En el corazón te sientes deprimido, sabes que [indescifrable] dijo: "la cura para la depresión es la yihad fisabilillah" Sientes que no tienes honor [indescifrable] dijo: "El honor de un creyente es [indescifrable]" El honor de la ummah es la yihad fisabilillah, Oh mis hermanos vengan a la yihad y sientan el honor que estamos sintiendo. Sientan la felicidad que estamos sintiendo."

Abu YahyaashShami: "A mis hermanos de Australia…Así que este es el mensaje que quiero enviarte, un mensaje que insha'Allah, desde un corazón musulmán a otro [indescifrable] corazón.

[árabe], Mucho tiempo ha pasado, ha sido golpeado, los judíos lo han tomado. Nuestras hermanas en Fallujah, ellas días tras día dan a luz bebes deformes. Mira la desgracia que esta ummah atraviesa. Mira, observa y despierta, por qué está pasando esto.

El libro del Corán… este Corán, Allah Azzawa Jal envía Muhammad con para que podamos vivir [sic]… vive estas reglas. Para que podamos vivirlas que podamos tener [indescifrable] en nuestros corazones.

Las banderas de [indescifrable] se están levantando y el honor [indescifrable] está regresando y él [indescifrable] se está estableciendo. Despierta [indescifrable]"

Abu Nour al Iraquí: "[indescifrable] en Occidente, donde sea que esté, en Europa, en Australia, en América…Las razones para venir a la yihad. Las razones son muchas [indescifrable] una vez dijo: "Una vez que se trata de la yihad hay dos tipos de personas: aquellos que encontrarán cada pequeña excusa para no venir a la yihad". Para aquellos que quieren venir a la yihad y ellos quieren el [indescifrable] hay muchas excusas, hay muchas razones para venir a la yihad, especialmente en Bilad al-Sham.

Si estas luchando por hacer de Alá [indescifrable] el más alto. Si estas peleando para establecer el califato entonces, aquí en Bilad al-Shem, hay un estado que ya lo está haciendo, hay un estado, hay al-Dawlah al-Islamiyahal Iraqwa-al-Sham, que ya lo está haciendo, que ya está instalado y está buscando ser un califato. Y [indescifrable] me dio la oportunidad como Alá [indescifrable] da esta oportunidad a muchos otros muyahidines para venir a Bilad al-Sham a hacer precisamente eso [indescifrable] y insha'Allah tendremos éxito Insha'Allah."

Abu Dujana al Hindi: "Este es un mensaje para los hermanos que se han quedado atrás [árabe] necesitan preguntarse a sí mismos qué te impide venir a la tierra de [indescifrable] lo que te impide unirte a la fila de los muyahidines, aquellos que derraman su sangre para alzar la [árabe] para levantar [árabe]. ¿Qué te impide [árabe] y el [indescifrable] de tu señor? Mira a tu alrededor mientras te sientas cómodamente y te preguntas "¿es así como quieres morir?" Sepan que serán resucitados [indescifrable] en la forma en la que vivieron su vida. Deseas ser resucitado como polvo desde [árabe] kuffars todavía en tus pulmones o deseas ser resucitado mostrando

tus heridas y que sacrificaste por Alá Azzawa Jal. Sepan que [árabe] no es algo pequeño y si quieres mostrar a Allah Azzawa Jal qué sacrificaste por esto [indescifrable] por él. Es sólo a través de su misericordia que entramos al paraíso. Pero, aparte de eso, ¿no quieres mostrar a Allah Azzawa Jal que has dado algo por él? Pregúntate qué te impide y qué te mantiene detrás. Si es tu riqueza, sapan que [indescifrable] cuando la muerte llegue, y esto es una certeza, su riqueza no podrá retrasar la muerte. No será de ninguna utilidad para ti ni para tu hogar, tu verdadero hogar, la tumba. Se distribuirá entre las familias una vez que se haya ido. Sepa que si es su familia - su esposa, esas personas a las que dice amar- si realmente los amas entonces, quizá lo haga por ellos, porque puede dar [árabe] a ellos en tu [árabe]. Subhan Allah, mira a tu alrededor mientras estás viendo este video y pregúntate: "Es esto lo que seleccionado y que en lugar de [la resurrección]", Mientras sabes que tus hermanos están allá fuera en el frente, enfrentando balas, las bombas y todo el enemigo [indescifrable] mientras tú estás sentado cómodamente, mientras duermes, mientras vas de compras. Ellos han dado su sangre, ellos están durmiendo en el suelo, wallahi, conocí gente de [indescifrable]. Ellos están durmiendo en [indescifrable] camiones."

"Sepa que si tú [indescifrable] que te impide, la muerte te alcanzará de cualquier forma, pero será más doloroso que para aquello que consiguen [árabe]. Porque él [árabe] ellos no sienten la muerte, excepto como una picadura de un insecto. El profeta [indescifrable] una de sus últimas palabras fue [indescifrable] en muerte y agonía."

"Así que, si la muerte es a lo que le temes, será peor. Sepan que los valientes son aquellos que permanecen detrás, porque ellos no temen Allah Azzawa Jal. No temas [indescifrable]. No temas [indescifrable]. Y sabes que [indescifrable] te resucita desnudo y tienes tus pecados en el cuello. Alá te mostrará la [indescifrable]que fue violado por el[indescifrable], el niño que fue decapitado por ser musulmán [indescifrable], los hermanos que dieron su vida para que el [indescifrable]pueda ser en el mundo entero. Sus cuerpos serán entregados a [indescifrable]. Alá te preguntará ¿dónde estabas tú? Y wallah, no serás capaz de hablar. No serás capaz de responder. En ese día, tu lengua estará atada y tu cuerpo hablará. Así que mi consejo para ti es teme, AllahAzzawa Jal Allah Azzawa Jal deposita tu confianza en él."

"Y sabes que [indescifrable] dijo al profeta [indescifrable]: "Nadie vino a este camino excepto que ellos fueran [indescifrable]. [indescifrable] tienes personas que claman ser muyahidines dando [indescifrable]." Mira donde comenzamos y mira donde estamos hoy. Wallahi, estos kuffars temen a nosotros el Califato. Lo ven venir, pero no pueden retrasarlo, no pueden evitarlo [indescifrable] y estas personas [indescifrable] enteran su vida entera, han obtenido todas estas nuevas armas y wallahi, y limpian día tras día, pulgada tras pulgada. Estamos sacándolos de la [indescifrable] AllahAzzawa Jal. Esta es la prueba de que Alá está con nosotros. ¿cómo puede temer a aquellos que ni siquiera pueden hacerse daño a sí mismos sin el permiso de AllahAzzawa Jal?, y saben que la muerte está cerca, y saben que tendrán que responder [indescifrable] por quedarse atrás. Pregúntate a ti mismo, cualquiera que sea tu trabajo, tu

grado, wallahi, recuerda la [indescifrable] que tiene fechas en sus manos y él dijo que vivir y comer estas fechas era demasiado retrasar su encuentro con AllahAzzawa Jal. No necesitamos nada de ti, por Alá eres tú el que necesita la yihad. Nosotros sólo queremos conocer a nuestro señor. Sólo queremos dar nuestra sangre y usar nuestros cuerpos como un puente desde el Califato. Wallahi, el Califato está cerca. Así que, pregúntate a ti mismo. Si puedes estar aquí en esta época de oro, tú puedes estar aquí [indescifrable] o puedes estar en la banca [indescifrable]**.”**[448]
Objetivo del video: Persuadir a la audiencia de reunirse a la yihad
Relación entre acción y hechos: Según cifras de 2014, se estimó que cerca de 400 personas de nacionalidad británica estaban peleando con ISIS o algunas de sus organizaciones afiliadas. El fenómeno de los combatientes extranjeros plantea serios retos para la seguridad de diversos países, desde el proceso de radicalización que los lleva a abandonar sus hogares hasta la amenaza que, de acuerdo a determinados gobiernos, representa el regreso a su país natal.[449]
Comentarios: Se recurre a sentimientos como el honor, la felicidad, la justicia, etc., para incentivar a la audiencia a unirse a la yihad. A lo largo del video se hacen varias referencias: • **A la zona geográfica:** que se identifica como Sham, también como Hayat tierra de la vida, que según su interpretación del Corán es la tierra de la yihad. • **Al espacio temporal:** declaran que este el momento, “la época de oro” para formar parte de la yihad. • **A las batallas:** se refieren a las victorias que han tenido, la facilidad con la que pueden trasladarse a otros territorios y la rapidez con la que han conseguido conquistas • **A los combatientes:** sobre su origen, plantean que Daesh no conoce fronteras y que pueden unirse de todas combatientes partes del mundo a la yihad. • **A la vida en Occidente**: a la confortabilidad en la que se viven las personas, mientras los muyahidines derraman su sangre en nombre de Alá. Asimismo, se hace referencia al estilo de vida occidental.

[448] Traducción propia con ayuda de la transcripción al francés e inglés de Virginie Carrière. (Septiembre, 2016). Transcription de la vidéo «There is no life without jihad». [En línea]. Disponible: <http://virginiecarriere.com/wp-content/uploads/2016/11/19-juin-2014-Transcription-There-is-no-life-without-jihad.pdf>. (13/02/2017).

[449] Siddique, Haroon. (Junio 21, 2014). “Jihadi recruitment video for Islamist terror group Isis features three Britons”. *The Guardian*. [En línea]. Disponible: <https://www.theguardian.com/world/2014/jun/20/jihadi-recruitment-video-islamist-terror-group-isis-features-britons>. (13/02/2017).

- **A los valores personales:** "si amas a tu familia hazlo por ellos", también se habla de vivir con honor y que formar parte de la yihad es la cura para la depresión.
- **A la salvación:** plantean que la muerte será dolorosa para quienes no formen parte de la yihad, que Alá les pedirá cuentas por no haber formado parte de ella, por lo que no serán correctamente resucitados.
- **A los sacrificios:** que las personas que se unen estén dispuestas a sacrificar todo, ya que serán recompensados por Alá.
- **A la obligación divina:** señalan que eres tú quien necesita pelear por Alá y no Alá el que necesita que peleen por él.

Clasificación: The End of Sykes- Picot		
Tipo de video: Propaganda	**Fecha:**16/diciembre/2016	**Duración:**
URL: https://www.liveleak.com/view?i=d43_1404046312	**Plataforma de consulta:** YouTube	
País/ubicación: Iraq	**Autor:** Daesh	**Planos:**1
Fecha de reproducción:13 de febrero de 2017		
Contexto:		
Contenido: El video inicia con un hombre vestido de negro, con barba y gorra. Se encuentra en un lugar desértico. Un recuadro del lado inferior izquierdo de la pantalla le identifica como "Abu Safiyya de Chile". Del lado superior derecho aparece el logo de Alhayat. En el fondo comienzan los cantos del Estado Islámico. La siguiente toma enfoca a Abu izando la bandera del Estado Islámico (EI). Entonces, aparece la leyenda "The end of Sykes-picot" en letras rojas y blancas. Abu Safiyya se dirige a la cámara y señala el terreno a su alrededor, otra toma muestra más detalles del lugar en el que están ubicados. La siguiente toma es de Abu hablando a la cámara de frente, comienza a caminar, la cámara le sigue, en su espalda lleva un arma. Abu cruza la frontera y los cantos del EI aumentan de volumen. Se dirige a un letrero en el suelo que dice "Commandos Battalion Border" y se coloca encima de él. En otra escena Abu muestra el mapa de la frontera en una pared, la frontera entre Iraq y Sham, señala el mapa y los cantos se escuchan nuevamente. En la siguiente escena aparece frente a una construcción de un piso, en la zona frontal superior está la bandera de Iraq. Abu muestra las instalaciones y la cámara le sigue, en el fondo comienza a aumentar de volumen nuevamente los cantos del EI.		

Abu muestra emblemas del ejército iraquí quedaron en la construcción. La siguiente toma es Abu izando la bandera del EI y los cantos de fondo. Abu se dirige a la cámara nuevamente, en la siguiente toma aparece a lado de un auto en ruinas y se dirige a otros 3 autos en condiciones similares, Abu se aleja la cámara lo toma de espaldas y los cantos se escuchan nuevamente.
Abu Safiyya muestra un letrero en la pared, escrito en árabe. La siguiente toma lo muestra enfrente de un vehículo militar en buenas condiciones, con pintado con la bandera de Iraq, con una huella de un disparo en el para brisas. En la siguiente escena se aproxima a otro vehículo, es blanco y tiene letras en árabe e inglés "Border Patrol 3/13" cherokee, muestra dos autos más del mismo tipo mientras los cantos aumentan de volumen.
La siguiente escena es frente al vehículo militar, la cámara toma a Abu y al vehículo, el hombre camina hacia la patrulla, los cantos siguen en el fondo. La cámara toma los símbolos pintados en los autos y los cantos aumenta de volumen. En otra ubicación, entre dos autos y bajo la sombra de un árbol Abu continua su discurso.
La siguiente escena es dentro de una construcción que Abu identifica como una prisión, abre una celda 14 prisioneros yazidíes. La cámara muestra a los prisioneros, sentados en el suelo.
La siguiente escena muestra un letrero, un trozo de tela negra con letras en árabe pintadas con color blanco, la toma deja ver a otro sujeto con mascada roja en la cabeza, al entrar a la construcción aparecen 4 sujetos, vestidos con ropa militar, la cabeza cubierta, dos con el rostro cubierto y los otros dos llevan barba, todos llevan armas. Un sujeto más parece y cruza frente a la cámara, vestido de militar y con el rostro descubierto. La toma muestra a Abu explicando lo que ocurrió en ese lugar, los cantos aumentan, en la toma se ve a Abu y otros dos sujetos, en el fondo se ve un desierto, autos y alrededor de 10 sujetos más, la bandera del EI aparece mástil.
Posteriormente, aparece Abu en una patrulla, con otros sujetos, la bandera del EI está del lado derecho a lo lejos se muestra la estación de policía y de pronto explota.
La siguiente escena Abu está frente a los escombros, los cantos aumentan se muestran los escombros y a Abu sonriendo. En la siguiente escena aparece la patrulla atrás otro auto oscuro, alguien habla por un megáfono y otro sujeto sube a la patrulla vestido de militar, después de activa la sirena de patrulla, se muestra al conductor y a su acompañante sonriendo, mientras este habla por el megáfono, los cantos aumentan, el auto se aleja y se puede observar a otro hombre y a un niño en la patrulla como acompañantes.

No. de personas: 30 aprox.	**Lugar:** Algún lugar en la frontera entre Siria e Iraq	**Acción:** Propaganda

Transcripción:
-En el nombre de Alá, el Compasivo, el Misericordioso-
[árabe]

Abu Safiyya: Como pueden ver ahora estamos en la frontera entre Iraq y Sham.
-Oh mi nación, aparece el alba, espera la victoria-
-El Estado Islámico fue construido por la sangre sincera-
Título: El fin de Sykes-Picot
Abu Safiyya: "Ahora mismo estamos del lado de Sham, como pueden ver esta es la llamada frontera de Sykes-Picot. Nosotros no la reconocemos, y nunca vamos a reconocerla. Esta no es la primera frontera que vamos a romper, Insha'Allah vamos a romper otras fronteras también. Vamos a empezar con esta, Insha'Allah. Si caminamos Insha'Allah vamos a cruzar la frontera. Como se ve Insha'Allah aquí es donde estaba el ejército Safawí."
"Esto se conoce como frontera con la policía y puntos de control, no hay nadie ahí excepto los soldados del Estado Islámico. "Insha'Allah. Vamos a cruzar la frontera. En el nombre de Alá."
Este es el llamado, punto de control. Soldados Maliki. Como se ve aquí hay un letrero, en él está escrito: 'Commandos Battalion Border'. Aquí no hay batallones, ni comandos, excepto los del islam. Y como ves esta placa está bajo nuestros pies. Los que apoyan a Abu Bakr al-Baghdadi dijo que se trata de las presas de interruptores. Insha'Allah romperemos la barrera de Iraq, Jordania, Líbano y todas las naciones a Jerusalén Insha'Allah. Es la primera barrera de muchas barreras que vamos a romper Insha'Allah."
"Vamos Insha'Allah."
"Esto es como el mapa de la frontera, este es Iraq, este es Sham, pero ahora es sólo un Estado y una comunidad Insha'Allah, una umma Insha'Allah. Es más no hay más fronteras."
"Esta es la bandera de Iraq, del politeísmo. El mensajero de Alá dijo: "quien clama el tribalismo no es para mí". Es por ello, que negamos esta bandera Insha'Allah. Este es el sitio donde los soldados eran apostatas safawíes, este es el punto de control cerca de la frontera, este es el lugar donde solía estar. Lleno de símbolos de la incredulidad y el politeísmo."
"Como puedes ver aquí, el arma, la espada y la bandera, per están apenas por debajo, sólo huye. 'Ejército iraquí'. ¿dónde está el ejército iraquí? Los soldados se deshicieron de sus uniformes y los tiraron en el suelo, huyeron como cobardes civiles [árabe].
No hay ejército en el mundo que pueda lidiar con el Estado islámico, con el permiso de Alá."
"La bandera de Tawhid (monoteísmo), se elevará por encima de todas las banderas y de la incredulidad y del politeísmo Insha'Allah. Sin nacionalidad, somos musulmanes, un Estado, también tenemos sólo un Imam Insha'Allah y él será califa Abu Bakr al-Baghdadi (que Alá lo proteja)."
"Y como ves el Estado Islámico bombardeó el coche durante el ataque y la incursión. Alabanzas a Alá, nuestros hermanos en la Wilaya de Al-Barakah atacados cerca del punto de control. Se puede ver aquí los autos dañados, pero no todos porque tomamos unos como botín. [árabe] Como puedes ver estos autos explotaron, pero había otros como, *Hummer*, y otros más que tomamos como botín. [árabe]

matamos a la mayoría de los soldados, algunos de ellos han escapado, pero la mayoría fueron encarcelados, gracias a Alá, *Alabado sea Dios.* Es una gracia de Alá, *Alabado sea Dios*."

"En el nombre de Alá, mira este letrero, que se encuentra cerca del punto de control fronterizo, está escrito: 'las fronteras de Iraq están en el cuello (es responsabilidad de todos)'."

"Insha'Allah estarán nuestras espadas en sus cuellos. Venimos por ustedes Insha'Allah. Como pueden ver detrás de mí el botín, el Estado ha cercado Mosul *Alabanzas a Alá. Alabado sea Alá*. Un mensaje a occidente: sigan financiando a sus socios y seguiremos tomándolos como botines todo lo que se envía Insha'Allah. Esos son los grupos que cooperan con Estados Unidos, mira siempre dice que necesita ayuda y apoyo de Estados Unidos, necesita cooperar con Estados Unidos, mira, mira como ha llegado hasta ahora *Alabado sea Alá*. A pesar, del gran apoyo con el que Estados Unidos le ha ayudado. todo está en nuestras manos y gratis. *Alabado sea Dios*. Ahora estamos admirando el motín que obtuvimos, este *Hummer*. Este coche pertenece a los guardias de la frontera, al igual que otros, como pueden ver "Patrulla de la frontera". Todos estos carros pertenecen a la policía fronteriza. *Alabanzas a Alá* ahora pertenecen a los muyahidines."

"Mira la cantidad que Estados Unidos gasta para pelear contra el islam, pero *Alabado sea Dios* todo lo que está en nuestro bolsillo. Mira este gran auto, *Ford* estadounidense. *Alabado sea Alá*, pertenece a nosotros ahora. Gastan millones, Estados Unidos gasta, he leído las noticias han pagado casi 20 mil millones, ahora que están en la quiebra, no pueden poner pie en Iraq de nuevo, ya que han perdido en Iraq, perdieron en Afganistán, también y perderán en Siria cuando vengan Insha' Allah. *Alabado sea Alá*.

Alá dice en el Corán: 'Desean apagar la luz de la boca de Alá, pero Alá sólo perfeccionará su luz' [Sura As-Saf:8]. *Alabanzas a Alá*. Insha'Allah se obtendrá más botín más tarde. Tenemos helicópteros, tenemos aviones, tenemos *Hummers*. Insha'Allah es un gran futuro de esta forma."

"Ahora estamos en la prisión, tenemos algunos prisioneros aquí de la batalla de Mosul. Algunos son chitas, otros son apostatas y otros son yazidíes. Para aquellos de ustedes que no conozcan a los 'yazidíes', es decir, aquellos que adoran al diablo, Iblís, Satán. Vamos a echar un vistazo Insha'Allah... Algunas imágenes en directo. Aquí se puede apreciar, estos prisioneros, son sólo un pequeño grupo, que es uno de los cientos que tenemos, la mayoría de ellos son chitas y yazidíes. Los que levantan sus manos en este momento son yazidíes. Dicen que Iblis (Satanás) se transfirió al paraíso y, sin embargo, ellos lo aman. Esos son los que patrullaban la frontera entre Iraq y Sham, esos son los que lucharon y muyahidín *Istich-hâdiyîn* preso, que les impedía llegar a Iraq. *Alabanzas a Alá*. Si pronunciamos la palabra 'Istich-hâdiyîn' se mueren de miedo. Mira a estos idiotas, que dicen que son sunitas, pero nada que ver con "*Ahlou-s-Sunnah*. En árabe: Clamas ser ahlus-sunna, pero peleas que la muyahidín no proviene de la sunna."

Aquí se encuentra la estación de la policía fronteriza, ahora nuestros hermanos se están preparando para explotar este edificio Insha' Allah. Ahora preparan los explosivos, vamos a echar un vistazo al interior Insha' Allah. Nuestros hermanos harán estallar cualquier

edificio perteneciente al gobierno iraquí safawí. Van a destruir todos los edificios gubernamentales Insha' Allah, ya sea comisarias o puntos de control etc. Alá acepta lo que nuestros hermanos están haciendo, le pedimos que no conceda éxito y nos comunique fuerza. Recordamos a nuestros hermanos que deben tener buenas intenciones hacia Alá, Insha' Allah. El Estado de extenderá Insha' Allah. Que Alá los recompense con bien. Estos hermanos son responsables de los explosivos, que Alá acepte sus acciones, le pedimos que aumente sus grados en el paraíso, Insha' Allah. Qué Alá les recompense así."
"Aquí la estación de policía que nuestros hermanos explotarán ¡Insha' Allah! ¡Oh¡ Alá."
"*Allahou Akbar*, la verdad siempre vencerá a la falsedad, la alabanza de Alá"
"Allahou Akbar, la verdad siempre vencerá a la falsedad, la alabanza a Allah"
"Este es el resultado al que se someterán todos los edificios de la incredulidad y el politeísmo"
"No un lugar en esta tierra que vaya a estar a salvo, donde estos edificios estén a salvo de los muyahidines"
"vendremos a través de todos los edificios de la incredulidad y el politeísmo […] es para Allah"
"También quiero transmitir un mensaje: 'no estamos aquí para luchar por tierra o por las fronteras imaginarias de Sykes-Picot
Quiero transmitir un mensaje: no se lucha por la tierra o por fronteras imaginarias de Sykes-Picot, no estamos aquí para cambiar *Taghout* árabe por una *Taghout* occidental"
"Nuestra yihad es mayor que todos, luchamos por la religión de Allah
luchamos por hacer la tierra de nuestro señor grande, para que sea completamente a Él, vamos a liberar Palestina insha'Allah, llegaremos a Quds (Jerusalén) y rezaremos en el Aqsa insha'Allah Al, la primera (dirección de la oración) de los musulmanes insha'Allah. Pedimos Allah que nos conceda su éxito, que nos proteja, nos guie y nos guarde, le pedimos a Allah que nos use y no nos cambie, pedimos a Allah que nos perdone y a todos los creyentes."
Hombre en la patrulla: "¿Quieres que le diga algo bueno o malo?"
Persona grabando: "Bueno, bueno, bueno"
Hombre en la patrulla "Quiero decir que Irak y Sham se convirtieron en un país ahora y otros países están en lista de espera insha'Allah. El Estado Islámico tomará todos los países musulmanes insha'Allah, insha'Allah"
"Los llevaremos de la incredulidad al islam, del politeísmo hacia el *Tawhid insha'Allah* (monoteísmo)"
"Una pregunta para Obama, antes de mandar tropas a Bagdad, ¿preparaste suficientes pañales para tus soldados o no?"
[árabe]

Objetivo del video: Demostrar los logros del Estado Islámico, la capacidad militar en cuanto a armamento, el dominio que tiene en la región y sus próximos objetivos.

Relación entre acción y hechos:
Comentarios:

Clasificación: No Respite		
Tipo de video: Propaganda	**Fecha:**	**Duración:**
URL:	**Plataforma de consulta:**	
País/ubicación: No aplica	**Autor:** Daesh	**Planos:** Producción audiovisual
Fecha de reproducción:15 de mayo de 2017		
Contexto:		
Contenido: El video comienza con el logo de Alhayat Media Center y un fondo negro, la imagen se acerca al logo y muestra una población en donde ondea la bandera del Estado Islámico. La imagen se aleja y muestra el mapa del área dominada por Daesh en Siria e Iraq. Del lado superior izquierdo de la pantalla aparece el logo de Alhayat Media Center, el fondo es negro, las letras son anaranjadas y del lado derecho aparece un mapa en que se muestran puntos naranjas en Argelia, Libia, Nigeria, Somalia, Siria, Iraq, Arabia Saudita, Yemen, Rusia, Afganistán, Bangladesh, Indonesia y Filipinas. El mapa se mueve a la derecha y en el lado izquierdo tras un cuadro naranja aparece una imagen de Abu Bakr al-Baghdadi. La imagen mueve a la izquierda y aparece el mapa de Reino Unido, comparando el tamaño de los dominios de Daesh, del lado derecho aparece un “8x” y ocho pequeñas imágenes del mapa de Bélgica, la pantalla se mueve nuevamente a la derecha y aparece “30x” y treinta pequeñas imágenes del mapa de Qatar. La siguiente imagen es un fondo blanco y azul, aparecen algunas nubes, hay dos banderas entrecruzadas del Estado Islámico (EI) atravesadas por la palabra “Califato” abajo letras en árabe y en inglés que dicen “en la metodología profética”. La pantalla se acerca a la letra “A” del califato, la siguiente escena es un fondo de nubes negras y el logo de la Organización de Naciones Unidas en azul marino, la imagen se mueve deja de ella		

aparece el Capitolio (en Estados Unidos), que es sustituida por la imagen de soldados estadounidenses. Un acercamiento más da paso a la bandera estadounidense, que se aleja para mostrar a Obama (la bandera es un dije en su traje) y otros personajes de la política estadounidense detrás de él, las imágenes se mueven y muestran al ex presidente George W. Bush, un movimiento más muestra a otro ex presidente Bill Clinton. Los personajes son colocados en pantallas de televisión, las pantallas se alejan y aparecen logos de corporaciones como: Citi, Chevron, AEGIS, The Carlyle Group, Hallburton, Washington Group International, General Electric, el Sistema de Reserva Federal de Estados Unidos, Dyn Corp, Shell, Exxon Mobil (2 veces), United Technologies, Northrop Grumman y Merrill Lynch.

La siguiente imagen es una reunión del Consejo de Seguridad de Naciones Unidas y arriba de esta imagen una mano sosteniendo un móvil, en él se puede leer la noticia "La persecución LGBT de ISIS, En una reunión del Consejo de Seguridad de Naciones Unidas (el nombre del consejo aparece subrayado) se discuten las victimas gay del Estado Islámico en Siria e Iraq". La siguiente escena muestra a un soldado del Daesh, sosteniendo la bandera del EI arriba en lo alto de una montaña, los rayos del sol cruzan esta imagen y el cielo es limpio y azul, poco a poco aparecen más montañas y el combatiente con la bandera queda al fondo. La siguiente escena soldados del EI levantando sus armas, atrás aparece la bandera de Daesh, aparecen nuevamente soldados de Daesh alzando sus manos en oración, iluminados por un fondo blanco. Después un combatiente con un arma en la mano, su pie apoyado sobre una ropa en gesto de victoria a su espalda un camión militar arde y a su lado otro más está destruido.

La siguiente escena muestra muchas banderas, algunas de grupos yihadistas que también combaten en Siria, al frente está la bandera de Estados Unidos, el viento las mueve a la izquierda. La siguiente imagen es otro combatiente, con un arma, ropa militar, recargando su pie derecho en una roca, al fondo un escenario que pareciera ser Palmira, el cielo es negro, hay llamas y la bandera de Daesh está del lado derecho, la imagen se mueve a la derecha y se muestran escombros de las columnas que aparecían en la imagen pasada, la pantalla muestra el cielo y letras en rojo que dice "Sykes Picot". La transición a la siguiente escena se da en medio de llamas, aparecen letras que dicen "shirk and nationalism". Posteriormente, se muestran a miembros de Daesh tomados de los hombros: se trata de cuatro hombres, vestidos con ropa militar, gorros, guantes, todos llevan barba, sonríen y los dos hombres de los extremos alzan su dedo índice al cielo.

Se muestra a más combatientes con los brazos cruzados, mirando al suelo a sus espaldas el cielo es limpio y azul, la siguiente escena es el Corán. Después en un fondo de montañas a parecen niños soldados, vestidos con ropa militar, un arma en sus manos, llevan un gorro negro y leen lo que parece ser el Corán, la siguiente imagen son los niños soldados de pie con el arma en sus manos y la bandera

del Daesh a sus espaldas, la transición a la siguiente escena se da con un acercamiento al ojo de un niño combatiente hay dos banderas de Estados Unidos cruzadas, el fondo es el cielo negro y nuboso, en el fondo aparece una nube de hongo (explosión nuclear) de las banderas salen helicópteros militares, abajo hay tanques militares y filas de soldados.

La siguiente escena es un hombre cubriendo su rostro con las manos, no tiene cabello, viste de blanco, a su espalda hay imágenes de combate y al su lado derecho píldoras y un diagrama de fórmulas químicas. La siguiente imagen en una mancha roja de donde surge la imagen de un soldado herido, otra imagen más está a la derecha enmarcada por una mancha gris, en la imagen aparece un soldado con la cabeza vendada u otros más que lo cargan en una camilla.

Aparecen muchos soldados de espaldas cargando féretros, sobre ellos la bandera de Estados Unidos, el fondo es negro y con llamas, en medio está la cifra 50 000, la escena se mueve hacia abajo y aparece un soldado, en blanco y negro, mirando al suelo y apoyando su cabeza en la mano derecha, frente a él aparece la cifra 6 500, después el soldado es cubierto por una mancha roja, la transición muestra dos papeles con datos en la parte superior de la hoja derecha se lee "Comando Central de Estados Unidos" abajo "Ataques Militares contra ISIL en Iraq y Siria" y los siguientes datos: soldados – 12 000; edificios – 3 262; HMMWV's – 340, Tanques – 119; Infraestructura petrolera – 196; Otros – 3 680.

La siguiente imagen es un soldado gritando, mirando al cielo, el fondo el blanco y detrás de su cabeza hay una mancha negra. La transición muestra un fondo blanco sobre el que van apareciendo manchas rojas, se escucha sonido de espadas chocando y surge el número 18, Después en un fondo de nubes negras se muestra la cantidad 6 000 000 000 000 que gotea sangre, tras una explosión, seguido de edificios en ruinas y escenarios de guerra en donde hay soldados vendados se muestra una gráfica con una línea en aumento. La transición a la siguiente imagen se da por medio de aviones militares, se muestra un misil y arriba de éste la cifra 65, abajo se agrega la cantidad 250 000.

En la siguiente secuencia se muestra un soldado con un arma, el fondo es de nubes oscuras, en seguida se muestra una munición y la cifra 50. En un fondo de fuego se puede apreciar la insignia de "Fuerza de Trabajo Conjunta" y "Operación de determinación inherente". La imagen que sigue es la del presidente de la República Islámica de Irán Hasán Rouhaní acompañado de la bandera iraní a su espalda en un fondo negro y con llamas, después aparece otro personaje, se trata de Recep Tayyip Erdoğan, presidente de Turquía, igualmente con la bandera turca a su espalda. El siguiente personaje es Vladimir Putin, presidente de Rusia, acompañado con la bandera rusa a su espalda.

La escena que sigue es una reunión de la Asamblea General de Naciones Unidas, a esta imagen se superponen dos espadas cruzadas y la insignia de la "Fuerza de Trabajo Conjunta", sucedida por llamas un fondo negro una imagen que muestra 60 banderas de los siguientes países: Australia, Bahréin, Albania, Dinamarca, Bélgica, China, Croacia, Austria, Egipto, República Checa, Grecia, Canadá, Estonia, Francia, Finlandia, Iraq, Jordania, Alemania, Irlanda, Hungría, Países Bajos, Nueva Zelanda, Rumania, Líbano, Kosovo, Corea del Norte, Kuwait, Israel, Irán, Italia, Japón, Qatar, Luxemburgo, Suecia, Rusia, Noruega, Arabia Saudita, Siria, Eslovaquia, Suiza, Lituania, Macedonia, Bosnia, Taiwán, Estados Unidos, Reino Unido, Emiratos Árabes Unidos, España, Turquía, Omán, Ucrania, Túnez, Serbia, Eslovenia, Polonia, Portugal, Marruecos, Moldavia, México y Malta.

Después se muestra una larga formación de soldados y el número 80, después de muchas llamas, se muestra a un combatiente de Daesh de espaldas, portando un arma, de frente al fuego. La siguiente escena es un soldado del EI señalando con el dedo índice hacia enfrente, a su espalda está la bandera de EI y un fondo con nubes negras y estrellas, la imagen se recorre y se puede apreciar un cielo nocturno, estrellas, el espacio y finalmente la tierra, el sol destella un poco al fondo y arriba está sura que comienza a recitarse.

No. de personas: N/A	**Lugar:** N/A	**Acción:** Propaganda Daesh

Transcripción:
Alhayat Media Center

Este es nuestro Califato, en toda su gloría. Perdurando y expandiéndose. Fue establecido en el año 1435 AH, su líder de la tribu Quaraysh, Abu Bakr al-Baghdadi y su territorio es ya más grande que Reino Unido, ocho veces el tamaño de Bélgica y treinta veces el tamaño de Qatar. Es un estado construido a base de la metodología profética, esforzándose por seguir el Corán y la Sunna. No un estado secular construido a base de leyes hechas por el hombre, cuyos soldados pelean por el interés de legisladores, mentirosos, fornicadores, corporaciones y por las libertades de saudíes. Somos hombres con honor, con islam que encontraran su cumbre al ejercer la yihad, respondiendo al llamado de unidad, bajo una bandera.

Esta es la fuente de nuestra gloria, nuestra obediencia hacia nuestro señor. Nosotros somos intransigentes en nuestro llamado hacia él. Nosotros sólo nos inclinamos hacia Alá. A diferencia de las incontables facciones desviadas, alzando sus falsa banderas y cambiando los vientos [indescifrable] políticas. Sí, somos los soldados que detuvieron los ídolos del nacionalismo demoliendo y disparando los símbolos de Palmira y [indescifrable] y destruyendo las fronteras Sykes Picot, por donde no hay honor que pueda encontrarse, los restos de la [indescifrable] y el nacionalismo. Y la diferencia entre un árabe y un no árabe o un hombre negro y uno

blanco, excepto piedad esta es la gloria de a fe que nos une. La justicia está servida y establecida en las cortes islámicas y en los cientos de masjid y escuelas para nuestros cachorros y perlas donde se preparan así mismos para compartir en la gran recompensa de expandir este califato.

América, tú clamas tener el ejército más grande en la historia, como te conozco puedes tener números y armas, pero soldados como esos [indescifrable] cicatrices de sus derrotas en Afganistán e Iraq. Ellos regresaron muertos o siendo suicidas con cerca de 6 500 cometiendo suicidio cada tanto tiempo [indescifrable] recorrer los hechos y los resultados de sus bombardeos aéreos continuarán encontrando las mentes de sus soldados tanto miedo dentro de sus corazones, 18 de sus cometen suicido cada día, incluso antes de avanzar y en adición a los 6 billones de dólares etiqueta de precio en su suelo, ahí ahora con sus pies sobre el terreno en lugar de atacarnos por aire con misiles, cada uno con un valor de 250 000 dólares mientras nosotros dijimos que contamos con balas de 50 centavos.

Entonces existe una Coalición de demonios con Irán, Turquía y Rusia sumándose, esto es porque la mitad del *Kufr* (infieles) siempre se unen para pelear contra la verdad [indescifrable] sus números solo incrementan nuestra fe, para contar sus bandera, las cuales nuestro Profeta dijo [indescifrable] 80 en número, entonces [indescifrable] de la guerra finalmente los quemará en las colinas de la muerte [indescifrable] llevándoles el eco poderoso de nuestro Profeta, reúnan a sus aliados, conspiren contra nosotros y no nos den prórroga. Nuestro aliado es el más grande, él es Alá y toda su gloria.

"Así que resuelve tu plan y [invoca] a tus asociados. Entonces, no dejes que sea oscuro para ti. Luego, llévalo a cabo en mí y no me des respiro" Corán (Surah Yunus 71)

Objetivo del video: Propaganda de Daesh- declarar enemigos y demostrar fortalezas militares y espirituales del EI

Relación entre acción y hechos:

Comentarios:

Se muestra a los soldados de Daesh como combatientes protegidos por Dios, hombre con honor que luchan por una causa justa, frente a los soldados estadounidenses quienes han sufrido serias bajas y daños psicológicos derivadas de la intervención militar en Afganistán e Iraq. Se deja claro el poder militar de Daesh, al contar con soldados cuya principal fuerza es el valor espiritual de su batalla. También

se presentan los costos humanos y económicos que ha costado a Estados Unidos combatirlos. Se recurre a la moral para establecer que el EI se basa en normas de Corán y no en leyes hechas por el hombre y se expone la inmoralidad de los dirigentes estadounidenses. El video identifica a los "aliados" de EE. UU, así como a los infieles entre a los que menciona a Irán y Turquía. Sin embargo, sostiene que no importa el número de aliados, pues su mayor aliado es Alá.

BIBLIOGRAFÍA

ADAMEC, Ludwig W. (2012). *Historical Dictionary of Afghanistan*. Reino Unido: The Scarecrow Press, Inc.

ADAMS, James. (1999). *La próxima guerra mundial: los ordenadores son las armas y el frente está en todas partes*. Argentina: Granica.

ADAMSKY, Dima & Kjell Inge Bjerga. (2010). "Introduction to the Information-Technology Revolution in Military Affairs". *Journal of Strategic Studies*. Vol. 33, No.4. pp. 463–468. [En línea]. Disponible en: <http://dx.doi.org/10.1080/01402390.2010.489700>. (Consulta 10/09/2016)

ADEL, Loaa. (Diciembre 11, 2016). "Security forces discover 3 explosives labs near Ramadi". *Iraqi News*. [En línea]. Disponible en: <http://www.iraqinews.com/iraq-war/security-forces-discover-3-explosives-labs-near-ramadi/>. (Consulta 10/04/2017)

ADVAMEG. (2017). "Israel, Intelligence and Security". *Espionage Encyclopedia*. [En línea]. Disponible en: <http://www.faqs.org/espionage/Int-Ke/Israel-Intelligence-and-Security.html>. (Consulta 22/06/2017).

AFTERGOOD, Steven. (Julio 17, 2000a). "MiG-23 Flogger YF-113". *Federation of American Scientist.* [En línea]. Disponible en: <https://fas.org/nuke/guide/russia/airdef/mig-23.htm>. (Consulta 22/06/2017).

AFTERGOOD, Steven. (Abril 14, 2000b). "M1 Abrams Main Battle Tank". *Federation of American Scientist.* [En línea]. Disponible en: <https://fas.org/man/dod-101/sys/land/m1.htm>. (Consulta 10/05/2017).

AIRPLANES OF THE PAST. (*s.f.*). C-141 Starlifter. [En línea]. Disponible en: <http://www.airplanesofthepast.com/c141-starlifter.htm>. (Consulta 10/04/2017)

ALBERTS, David S. y Thomas J. Czerwinski. (1997). *Complexity, Global Politics, and National Security*. Washington: National Defense University Press.

ALBERTS, David S. y Daniel S. Papp. (Edits). (1997). *The Information Age: An Anthology of Its Impacts and Consequences*, Volume I. Washington: National Defense University Press.

ALBERTS, David S; John J. Garstka y Frederick P. Stein. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority.* EE. UU: CCRP publication series.

ALCARAZ, Yetlaneci. (Julio 14, 2013). "Hipocresía europea". *Proceso*, No. 1915, pp. 52-55.

ALY, Anne; Stuart Macdonald; Lee Jarvis y Thomas M. Chen. (2016). “Introduction to the Special Issue: Terrorist Online Propaganda and Radicalization”. Studies in Conflict & Terrorism. [En línea]. Disponible en: <http://dx.doi.org/10.1080/1057610X.2016.1157402>. (24/08/2017)

AL-RAWI, Ahmed K. (2014). “Cyber warriors in the Middle East: The case of the Syrian Electronic Army”. *Public Relations Review*, no. 40, pp. 420-428.

AMIR, Samir. (1989). *El Eurocentrismo: una crítica a una ideología*. México: Siglo XXI

AMINE Belarbi, Mohamed. (2015). “Cybersecurity in the Middle East: You’re Not As Safe As You Think”. *Gulfelitemag*. [En línea]. Disponible en: <http://gulfelitemag.com/cybersecurity-in-the-middle-east-youre-not-as-safe-as-you-think/>. (Consulta 28/05/2017)

ARONSON-RATH, Raney. (2014a). “A Biography of Osama Bin Laden”. *Frontline*. [En línea]. Disponible en: <http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/bio.html>. (Consulta 10/05/2017).

ARONSON-RATH, Raney. (2014b). “Weapons: mim-104 patriot”. *Frontline*. [En línea]. Disponible en: <http://www.pbs.org/wgbh/pages/frontline/gulf/weapons/patriot.html>. (Consulta 10/05/2017).

ARONSON-RATH, Raney. (2014c). “Weapons: e3 awacs sentry”. *Frontline*. [En línea]. Disponible en: <http://www.pbs.org/wgbh/pages/frontline/gulf/weapons/awacs.html>. (Consulta 10/05/2017).

ARONSON-RATH, Raney. (2014d). “The Gulf War”. *Frontline*. [En línea]. Disponible en: <http://www.pbs.org/wgbh/pages/frontline/gulf/weapons/>. (Consulta 22/06/2017).

ARQUILLA, John y David Ronfeldt. (2001). *Redes y guerras en red: el futuro del terrorismo, el crimen organizado y el activismo político*. Madrid: Alianza.

ASAMBLEA GENERAL DE NACIONES UNIDAS. (Agosto 2, 1990). Resolución 660. La situación entre Iraq y Kuwait. Consejo de Seguridad de la Organización de Naciones Unidas. [En línea]. Disponible en: <http://www.un.org/es/comun/docs/?symbol=S/RES/660%20(1990)>. (Consulta 10/04/2017)

ASAMBLEA GENERAL DE NACIONES UNIDAS. (Noviembre 29, 1990). Resolución 678 (1990). Consejo de Seguridad de la Organización de Naciones Unidas. [En línea]. Disponible en: <http://www.cinu.org.mx/temas/iraq/doctos/678.pdf>. (Consulta 10/04/2017)

ASSANGE, Julian y staff. (Noviembre 8, 2007). “US Military Equipment in Iraq (2007)”. WikiLeaks. [En línea]. Disponible: <https://wikileaks.org/wiki/US_Military_Equipment_in_Iraq_(2007)#Cryptographic_and_communications_security_equipment>. (Consulta 10/04/2017)

ASIF, Usman. (Noviembre 15, 2014). “Boeing AH-64 Apache”. *Stratford Chapter*. [En línea]. Disponible en: <http://stratford.vtol.org/?p=110>. (Consulta 10/05/2017).

AVAST. (2017). “WannaCry”. [En línea]. Disponible en: <https://www.avast.com/es-es/c-wannacry>. (Consulta 10/05/2017).

BANERJEA, Udit. (2015). “Revolutionary Intelligence: The Expanding Intelligence Role of the Iranian Revolutionary Guard Corps”. *Journal of Strategic Security*. Number 3, Volume 8. [En línea]. Disponible en: <http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1449&context=jss>. (Consulta 07/07/2017).

BARDAJÍ, Rafael L. (1991). “Operaciones En El Golfo: Escudo Del Desierto, Un Análisis Provisional.” *Política Exterior*, vol. 5, no. 19, pp. 84–93. [En línea]. Disponible en: <www.jstor.org/stable/20643059>. (Consulta 10/04/2017)

BARDAJÍ, Rafael L. e Ignacio Cosidó. (2000). “La RMA y España. Algunas reflexiones sobre el camino a seguir”. Grupo de Estudios Estratégicos (GEES). Análisis 56, Mayo-Junio 2000. [En línea]. Disponible en: <http://www.gees.org/articulos/la-rma-y-espanacorreo una-algunas-reflexiones-sobre-el-camino-a-seguir>. (Consulta 30/09/2016)

BARDAJÍ, Rafael L. (Ed.) (2003). *Irak: Reflexiones sobre una guerra*. [En línea]. Disponible en: <http://www.realinstitutoelcano.org/wps/portal /rielcano_es/publicacion?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/publicaciones/irak_+reflexiones+sobre+una+guerra>. (Consulta 30/09/2016)

BARKER, J. Paul (Ed). (Octubre, 2013). The Clash of Civilizations: Twenty Years On. Bristol: e-International Relations.

BASSIL, Youssef. (2012). “The 2003 Iraq War: Operations, Causes, and Consequences”. *Journal of Humanities And Social Science (JHSS),* Volumen 4, Issue 5. [En línea]. Disponible en: <www.lacsc.org/papers/papera1.pdf>. (Consulta 30/09/2016)

BASSIOUNI, M. Cherif. (2013). *Libya: From Repression to Revolution: A Record of Armed Conflict and International Law Violations*. Países Bajos: Martinus Nijhoff Publishers.

BEHAR, Richard. (Marzo 25, 2017). “Así funciona la fábrica secreta de startups de Israel”. *Forbes*. [En línea]. Disponible en: <http://forbes.es/actualizacion/7575 /asi-funciona-la-fabrica-secreta-destartups-de-israel>. (Consulta 10/04/2017)

BERGEN, Peter; David Sterman; Alyssa Sims; Albert Ford, y Christopher Mellon. (2017). *In Depth World of Drones*. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/1-introduction-how-we-became-world-drones/>. (Consulta 10/04/2017)

Who Has What: Countries with Drones Used in Combat. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-dro nes/2-who -has-what-countries-drone s-used-combat/>. (Consulta 10/04/2017)

Who Has What: Countries Developing Armed Drones. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-dro nes/4-who-has-what-countries-developing-armed-drones/>. (Consulta 10/04/2017)

Non-State Actors with Drone Capabilities. New America. [En línea]. Disponible: <https://www.newamerica.org/in-depth/world-of-drones/5-non-state-actors-drone-capabilities/>. (Consulta 10/04/2017)

BERGER, J.M. y Jonathon Morga. (Marzo 15, 2015). The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter. *Analysis Paper*, p. 7. [En línea]. Disponible en: <https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf>. (Consulta 24/08/2017)

BERKSOY, Biriz. (Junio, 2013). “Military, Police and Intelligence in Turkey: Recent Transformations and Needs for Reform”. *Demokratikleşme Programi*. [En línea]. Disponible en: <http://tesev.org.tr/wp-content/uploads/2015/11/Military_Police_And_Intelligence_In_Turkey_Recent_Transformations_And_Needs_For_Reform.pdf>. (Consulta 30/06/2017).

BERTRAND, Natasha. (Marzo 27, 2015). “Iran is building a non-nuclear threat faster than experts 'would have ever imagined'”. *Bussines Insider*. [En línea]. Disponible en: <http://www.businessinsider.com/irans-cyber-army-2015-3>. (Consulta 10/04/2017)

BBC. (Mayo 14, 2014). “Las ‘armas inteligentes’ que no quieren los defensores de las armas”. *BBC Mundo*. [En línea]. Disponible en: <http://www.bbc.com/mundo/noticias/2014/05/140523_tecnologia_arma_intligente_oposicion_mz>. (Consulta 22/05/2016).

BBC. (Octubre 11, 2015). “El virus que tomó control de mil máquinas y les ordenó autodestruirse”. [En línea]. Disponible en: <http://www.bbc.com/mundo/notici

as/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet>. (Consulta 13/11/2016).

BECKER, Markus. (Agosto 27, 2014). “Israel's War Business”. *Spiegel*. [En línea]. Disponible: <http://www.s piegel.de/international/world/defense-industry-the-business-of-war-in-israel-a-988245.html>. (23/05/2017)

BELK, Robert y Matthew Noyes. (Marzo 20, 2012). On the Use of Offensive Cyber Capabilities. *Creative Commons*. [En línea]. Disponible en: <http://ecir.mit.edu/images/stories/cybersecurity-pae-belk-noyes%202012.pdf>. (Consulta 01/11/2016).

BERMÚDEZ, Emma. (Agosto 6, 2014). “Así funciona el escudo antimisiles de Israel”. *El Confidencial.* [En línea]. Disponible en: <http://www.elconfidencial.com/tecnologia/2014-08-06/asi-funciona-el-escudo-antimisiles-deisrael_172468/>. (Consulta 13/11/2016).

BENÍTEZ Manaut, Raúl. (1986). “El pensamiento militar de Clausewitz”. *Revista Mexicana de Ciencias Políticas y Sociales*. Año XXXII. Nueva Época octubre-diciembre 1986, no. 126, pp. 97-123

BOEING. (2017). “AGM/RGM/UGM-84 Harpoon Missile”. [En línea]. Disponible en: <http://www.boeing.com/history/products/agm-84d-harpoon-missile.page>. (Consulta 28/06/2017).

BOEING. (2017). “Boeing Defense, Space & Security in the Middle East”. [En línea]. Disponible en: <http://www.boeing-me.com/en/boeing-in-the-middleeast/about-boeing-in-the-middle-east/defense-space-and-security.page>. (Consulta 27/05/2017)

BOULANIN, Vincent. (Diciembre, 2016). *Mapping the Development of Autonomy in Weapon Systems, A primer on autonomy*. Stockholm International Peace Research Institute. Working Paper, pp. 11-16. [En línea]. Disponible: <https://www.sipri.org/sites/default/files/Mapping-development-autonomy-in-weapon-systems.pdf>. (Consulta 02/05/17)

BRAVO Tejos, Gonzalo. (Enero, 2010). “El Proceso de Inteligencia, Vigilancia, Adquisición de blancos y reconocimiento”. *Revismar*, pp. 58-64 [En línea]. Disponible en: <http://revistamarina.cl/revistas/2010/1/bravo.pdf>. (Consulta 13/11/2016).

BRANDER Palacios, Juan Manuel; Roberto Zegers Leighton y Álvaro Marchessi Acuña. (2007). “Network Centric Warfare”. *Revista de Marina*. [En línea]. Disponible en: <http://revistamarina.cl/revistas/2007/5/brander.pdf>. (Consulta 28/05/16).

BROCH Hueso, Joaquín. (Diciembre, 2012). “La Contribución del ET a la Defensa Antimisil”. *Instituto Español de Estudios Estratégicos*. Documento Marco. [En línea]. Disponible en: <http://www.ieee.es/Galerias/fichero/doc s_marco/2012/DIEEEM122012_ContribucionETDefensaAntimisil_JBrochHUeso.pdf>. (Consulta 24/11/2016).

BRONK, Christopher y Eneken Tikk-Ringas. (2013). “The Cyber Attack on Saudi Aramco”. *Survival Global Politics and Strategy*, vol. 55 no. 2, pp.81-96

BROWN, Carl L., 1984. International Politics and the Middle East. Old Rules, Dangerous Game. London: I. B. Tauris.

BRUNO, Greg (Julio 23, 2012). “Iran’s Ballistic Missile Program”. Council on Foreign Relations, pp. 8. [En línea]. Disponible en: <https://www.cfr.org/backgrounder/irans-ballistic-missile-program>. (Consulta 12/02/2018).

BUTLER, Sean C. (2013). “Reenfoque del Pensamiento de la Guerra Cibernética”. *Air & Space Power Journal*, pp. 86-94. [En línea]. Disponible en: <http://www.airpower.maxwell.af.mil/apjinternational/apj-s/2013/20132/2013_2_09_butler_s.pdf>. (Consulta 11/01/15).

BUNZEL, Cole. (Marzo, 2015). From Paper State to Caliphate: The Ideology of the Islamic State. The Brookings Project on U.S. Relations with the Islamic World Analysis Paper, No. 19, p. 3 [En línea]. Disponible: <https://www.brookings.edu/wp-content/uploads/2016/06/The-ideology-of-the-Islamic-State.pdf>. (Consulta 10/04/2017)

CALVO Albero, José Luis. (2001). La Revolución de los Asuntos Militares. Escuela de Guerra del Ejército en Tierra. [En línea]. Disponible en: <http://csis.org/publication /real-revolution-military-affairs>. (Consulta 10/09/2016)

CAMBRIDGE DICTIONARIES ONLINE. (2016). *Digital Age*. Cambridge University Press. [En línea]. Disponible en: <http://dictionary.cambridge.org/es/diccionario/ingles/digital-age>. Consulta (22/05/2016).

CAMBRIDGE DICTIONARIES ONLINE. (2016). *Information Infrastructure*. Cambridge University Press. [En línea]. Disponible en: <http://dictionary.cambridge.org/es/diccionario/ingles/information-infrastructure>. (Consulta 22/05/2016).

CARNEY, Stephen A. (2011). *Allied Participation in Operation Iraqi Freedom*. Washington: Center of Military History.

CAROZO Blumsztein, Eduardo. (Marzo 5, 2013). “Centro de Respuesta a Incidentes Informáticos… ¿Para qué?”. *Seguridad*. [En línea]. Disponible en: <https://revista.seguridad.unam.mx/node/2168>. (Consulta 27/05/2017)

CARR, Jeffrey. (Agosto 22, 2012). “Was Iran Responsible for Saudi Aramco's Network Attack?”. *Digital Dao.* [En línea]. Disponible en: <http://jeffreycarr.blogspot.mx/2012/08/was-iran-responsible-for-saudi-aramcos.html>. (Consulta 21/05/2017)

CASTELLANOS, Diego Giovanni. (2010). *Islam en Bogotá: presencia inicial y diversidad.* Bogotá: Universidad del Rosario.

CASTELLS, Manuel. (2002). *La Era de la Información. Vol. I: La Sociedad Red*. México: Siglo XXI Editores.

CATHOLIC ONLINE. (Agosto 20, 2014). “Islamic State beheads journalist James Foley (WARNING, GRAPHIC VIDEO)”. [En línea]. Disponible en: <http://www.catholic.org/news/international/middle_east/story.php?id=56609> (Consulta 25/08/2017)

CASUS BELLI. (2016). Tecnología "Stealth" (furtividad). [En línea]. Disponible en: <http://cssbl.com/aire/stealth(2).htm>. (Consulta 10/11/2016)

CEBROWSKI, Arthur K. y John J. Garstka. (1998). “Network-Centric Warfare: Its Origin and Future”. *Proceedings*. [En línea]. Disponible en: <http://www.kinection.com/ncoic/ncw_origin_future.pdf>. Consulta (22/05/2016).

CENTRO DE ESTUDIOS SUPERIORES NAVALES. (1992). “Grandes Pensadores Estratégicos”. *Revista del Centro de Estudios Superiores Navales*, pp.57-67.

CHANG, Welton y Sarah Granger. (2012). “La Guerra en el Ámbito Cibernético”. *Air & Space Power Journal*, vol. 4, no. 3. [En línea]. Disponible en: <http://www.au.af.mil/au/afri/aspj/apjinternational/apj-s/2012/2012-3/2012_3_10_chang_s.pdf>. (Consulta 10/09/2016)

CHEPKEMOI, Joyce. (Agosto 1, 2017). “The Worst Cases Of Cyber Attacks In History”. *World Atlas.* [En línea]. Disponible en: <https://www.worldatlas.com/articles/the-worst-cases-of-cyber-attacks-in-history.html>. (Consulta 18/02/2018)

CHOUCRI, Nazli. (2012). *Cyberpolitics in international relations*. Cambridge: MIT Press.

CLARK, Wesley K. (2004). *¿Qué ha fallado en Irak? La guerra, el terrorismo y el imperio americano*. Barcelona: Crítica.

CLARKE, Richard A. (2012). *Cyber War: The Next Threat to National Security and What to Do About It.* EE.UU: Harper Collins.

COFFEY, J. I. (Diciembre 27, 1966). “The Anti-Ballistic Missile Debate”. *Foreign Affairs*. [En línea]. Disponible en: <https://www.foreignaffai rs.com/articles/1967-04-01/anti-ball istic-missile-debate>. (Consulta 13/11/2016).

COHEN, Amir. (Mayo 13, 2015). “Las cinco armas de guerra más mortíferas de Israel”. *RT*. [En línea]. Disponible: <https://actualidad.rt.com/actualidad/174692-armas-guerra-mortiferas-israel>. (Consulta 23/05/2017)

COHEN, Eliot A. (Marzo 1, 1996). “A Revolution in Warfare”. *Foreign Affairs*. [En línea]. Disponible en: <https://www.foreignaffairs.com/articles/united-states/1996-03-01/revolution-warfare>. (Consulta 10/09/2016)

CORDESMAN, Anthony. (Septiembre 26, 2003). *Iran-Iraq War*. Capílulo X, pp. 9-10. [En línea]. Disponible en: <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/9005lessonsiraniraqii-chap10.pdf>. (Consulta 12/02/2018)

CORDESMAN, Anthony H. (Febrero 10, 2011). “The Egyptian Military and the Arab-Israeli Military Balance”. *Center for Strategic and International Studies.* [En línea]. Disponible en: <https://www.csis.org/analysis/egyptian-military-and-arab-israeli-military-balance>. (Consulta 23/05/2017)

CORDESMAN, Anthony. (Enero 14, 2017). The Changing Nature of War in the Middle East and North Africa. *Harvard International Review*. [En línea]. Disponible en: <http://hir.harvard.edu/article/?a=14493>. (Consulta 10/08/2017).

COMITÉ INTERNACIONAL DE LA CRUZ ROJA. (Mayo 10, 2013). “El uso de los drones armados debe estar sujeto a la ley”. [En línea]. Disponible en <https://www.icrc.org/spa/resources/documents/interview/2013/05-10-drone-weapons-ihl.htm> (Consulta 10/11/2016)

COMPUTER EMERGENCY RESPONSE TEAM – GROUP-IB (CERT-GIB). (*s.f.*). “Computer Emergency Response Team (CERT-GIB)”. [En línea]. Disponible en: <http://www.group-ib.com/cert.html>. (Consulta 28/06/2017).

CONFLICT ARMAMENT RESEARCH. (Diciembre, 2016). “Standardisation and Quality Control in Islamic State’s Military Production”. *Dispatch from The Field*. [En línea]. Disponible en: <http://www.conflictarm.com/download-file/?report_id= 2454&file_id=2457>

CRAWFORD, Neta C. (Marzo, 2013). *Civilian Death and Injury in the Iraq War, 2003-2013.* Waston Institute. [En línea]. Disponible: <http://watson.brown.edu/costsofwar/files/cow/imce/papers/2013/Civilian%20Death%20and%20Injury%20in%20the%20Iraq%20War%2C%202003-2013.pdf>. (Consulta 14/05/2017)

CYBER SECURITY INTELLIGENCE. (*s.f.*) CERT-IL. [En línea]. Disponible en: <https://www.cybersecurityintelligence.com/cert-il-1928.html>. (Consulta 28/05/2017).

CYLANCE. (Diciembre 2, 2014). Operation Cleaver. [En línea]. Disponible en: <https ://www.cylance.com/content/dam/cylance/pages/operationcleaver/Cylance_ Operation_Cleaver_Report.pdf>. (Consulta 22/05/2017).

DE ROY VAN ZUIJDEWIJN, Jeanine y Edwin Bakker. (Junio, 2014). Returning Western Fighters: Te case of Afghanistan, Bosnia and Somalia. ICCT Background Note. [En línea]. Disponible en: <https://icct.nl/publication s/icct-papers/returning-western-foreign-fighters-the-case-of-afghanistan-bosnia-and-somalia>. (Consulta 25/08/2017).

DEFENSE INDUSTRY DAILY. (Junio 5, 2017). "AGM-158 JASSM: Lockheed's Family of Stealthy Cruise Missiles". [En línea]. Disponible en: <http://www.defenseindustrydaily.com/agm-158-jassm-lockheeds-family-of-stealthy-cruise-missiles-014343/>. (Consulta 24/06/2017).

DEFENSE INTELLIGENCE AGENCY. (DIA). (*s.f.*). "About DIA". [En línea]. Disponible en: <http://www.dia.mil/About/>. (Consulta 05/06/2017).

DEFENSE SCIENCE BOARD (DSB). (2012). *Task Force on Resilient Military Systems and the Advanced Cyber Threat*, pp. 49-50. [En línea]. Disponible en: <http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf> (Consulta 1011/2016)

DOWD, Alan W. (2013). "Drone Wars: Risks and Warnings". *Parameters*. Winter/Spring 2013, p. 2. [En línea]. Disponible en: <http://strategicstudiesinstitute.army.mil/pubs/parameters/Issues/Winter_2013/TheQuarterly_Winter2013-14_v43n4.pdf>. (Consulta 13/11/2016).

DREW, Christopher y John Markoff. (Mayo 30, 2009). "Contractors Vie for Plum Work, Hacking for U.S.". *The New York Times.* [En línea]. Disponible en: <http ://www.nytimes.com/2009/05/31/us/31cyber.html>. (Consulta 14/11/2016).

DUDNEY, Robert S. (Febrero, 2011). "Rise of the Cyber Militias". *Air Force Magazine*, febrero 2011, p.89.

DUNBAR, Brian. (Abril 4, 2014). "Global Positioning System". *National Aeronautics and Space Administration (NASA)*. [En línea]. Disponible en: <https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html>. (Consulta 10/05/2017).

DUNN Cavelty, Myriam. (2012). "The Militarisation of Cyberspace: Why Less May Be Better". *NATO CCD COE Publications*. [En línea]. Disponible en: <https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf>. (Consulta 28/11/2016).

DUNN, Myriam y Isabelle Wigert. (2004). *The International CIIP Handbook 2004: An Inventory of Protection Policies in Fourteen Countries*. Zurich: Center for Security Studies. [En línea]. Disponible en: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=452&lng=en>. (Consulta 11/01/15)

EBRAHIMNEYAD, Mohammad. (s.f.). "El Estado 'Islámico' de Iraq y Siria EI, ISIS o Daesh". Islam Oriente. Fundación Cultural Oriente. [En línea]. Disponible en: <http://islamoriente.com/node/140802>. (Consulta 10/04/2017)

EFE. (Julio 28, 2015). "Miles de científicos piden que se detenga el desarrollo de armas inteligentes y autónomas". *El diario.* [En línea]. Disponible en: <http://www.eldiario.es/turing/armamento-inteligencia_aritificial-carrera_armamentistica_0_414009439 .html>. (Consulta 13/11/2016).

EHTESHAMI, Anoushiravan. (2014). "Middle East Middle Powers: Regional Role, International Impact". *Uluslararası İlişkiler Dergisi*, Volume 11, No. 42. pp. 29-49. [En línea]. Disponible en: <http://www.uidergisi.com.tr/wpcontent/uploads/2016/0 6/42_1.pdf>. (Consulta 10/04/2017)

ELLIOT, Stephen. (Agosto 20, 2010). *Cyber Warfare and the Conflict in Iraq*. Security Week. [En línea]. Disponible en: <http://www.infosecisland.com/blogview/6750-Cyber-Warfare-and-the-Conflict-in-Iraq.html>. (Consulta10/03/2016)

EMRE KARABULUT, Yunus; Gulistan Boylu; Ecir Ugur Kucuksille, y Mehmet Ali Yalçınkaya. (Diciembre, 2015). "Characteristics of Cyber Incident Response Teams in the World and Recommendations for Turkey". *Balkan Journal of Electrical & Computer Engineering*. [En línea]. Disponible en: <https://www.researchgate.net/publication/289118287_Characteristics_of_Cyber_Incident_Response_Teams_in_the_World_and_Recommendations_for_Turkey>. (Consulta 27/05/2017)

ENLACE JUDÍO. (Agosto 28, 2013). "La mejor escuela sobre el planeta es la unidad 8200 del Ejército de Israel". [En línea]. Disponible en: <http://www.enlacejudio.com/2013/08/28/la-mejor-escuela-sobre-el-planeta-es-la-unidad-8200-del-ejercito-de-israel/>. (Consulta 27/05/2017)

ERIKSSON, Johan y Giampiero Giacomello (Eds.). (2007). *International Relations and Security in the Digital Age*. Londres: Routledge.

ESCUELA SUPERIOR DE LAS FUERZAS ARMADAS. (Octubre 16, 2014). *Apuntes de Inteligencia, Contrainteligencia y Seguridad. Fase Conjunta del Curso de Actualización de Ascenso a Comandante*. Departamento de Inteligencia y Seguridad, p. 3 [En línea]. Disponible en: <http://www.defensa.gob.es/cesede

n/Galerias/esfas/cursos/curActAscensoCte/ficheros/M5_1DocApoyoCTE_APUNTES_DE_INTELIGENCIA_CACES.pdf>. (Consulta 26/11/2016).

ESPINOSA, Ángeles. (Enero 18, 2013). "El jeque ciego". *El País.* [En línea]. Disponible en: <http://internacional.elpais.com/internacional/2013/01/18/actualidad/1358532614_954937.html>. (Consulta 10/05/2017).

ENSOR, Josie. (Mayo 22, 2016). "Isil carrying out chemical experiments on its prisoners as it moves labs into residential neighbourhoods". *The Telegraph*. [En línea]. Disponible en: <http://www.telegraph.co.uk/ne ws/2016/05/22/isilc arrying-out-chemical-experiments-on-its-prisoners-as-it-mo/>. (Consulta 29/05/2017)

ESTARELLAS y López, Juan C. (Febrero, 2011). "Los medios de comunicación de Al-Qaeda y su evolución estratégica". *Documento de opinión. Instituto Español de Estudios Estratégicos*, Número 15, p.13. [En línea]. Disponible en: <www.ieee.es/Galerias/fichero/.../DIEEEO16_2011MediosComunicacionAl-Qaeda.pdf>. (Consulta 29/05/2017)

ESTRADA Corona, Adrián. (Septiembre 10, 2014). "Protocolos TCP/IP de Internet". *Revista Digital Universitaria*. Volumen 5 Número 8. [En línea]. Disponible en: <http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf>. (Consulta 10/09/2016)

EVANS, Chris. (Junio 9, 2006). "Abu Musab al-Zarqawi". *The Telegraph*. [En línea]. Disponible en: <http://www.telegraph.co.uk/news/obituaries/1520703/Abu-Musab-al-Zarqawi.html>. (Consulta 10/05/2017).

FAHRENKRUG, David T. (2012). *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy.* NATO CCD COE Publications, Tallinn. [En línea]. Disponible en: <https://ccdcoe.org/cycon/2012/proceedings/fahrenkrug.pdf>. (Consulta 10/09/2016)

FALLIERE, Nicolas; Liam O Murchu, y Eric Chien. (Febrero 2011). W32.Stuxnet Dossier. *Symantec*. [En línea]. Disponible en: <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. (Consulta 22/05/2017)

FARLEY, Robert. (Febrero 26, 2015). "The 5 Most Lethal Drones of All Time*". The National Interest*. [En línea]. Disponible en: <http://nationalinterest.org/feature/the-5-most-lethal-drones-all-time-12326>. (Consulta 13/11/2016).

FARS NEWS AGENCY. (Mayo 21, 2015). "Saudileaks 2: Yemen Cyber Army Releases Hacked Contents". [En línea]. Disponible en: <http://en.farsnews.com/newstext.aspx?nn=13940231001097>. (Consulta 28/05/17)

FAYAZ Torshizi, Hossein. (2015). *Las Jóvenes afganas: Historias de Guerra y de Amor Narradas a Través de Los Nudos de Una Alfombra* [Edición Kindle]. Fayaz Editore.

FEDERAL BUREAU OF INVESTIGATION. (FBI). (*s.f.*). "About". [En línea]. Disponible en: <https://www.fbi.gov/about>. (Consulta 05/07/2017).

FEDERAL RESEARCH DIVISION, LIBRARY OF CONGRESS (FRDLC). (Diciemnbre, 2012). "Iran's Ministry of Intelligence ans Security: A profile". [En línea]. Disponible en: <https://fas.org/irp/world/iran/mois-loc.pdf>. (Consulta 06/07/2017).

FERNÁNDEZ, Álvaro. (Agosto 12, 2015). "Estonia, baluarte de la ciberseguridad europea". *El Orden Mundial en el Siglo XXI*. [En línea]. Disponible en: <http://elordenmundial.com/2015/08/estonia-ciberseguridad-europea/>. (Consulta 10/09/2016)

FERNÁNDEZ Merino, Félix. (Marzo, 2012). *Los sistemas no tripulados*. España: Ministerio de Defensa.

FERNÁNDEZ Rodríguez, José Julio; Javier Jordán Enamorado, y Daniel Sansó-Rubert Pascual (Edts.). (2008). *Seguridad y Defensa hoy: Construyendo el futuro*. Madrid: Plaza y Valdés.

FIGUEROA, Alfonso. (2002). "Misil aire-superficie AGM-65 Maverick". *La Armada Española.* [En línea]. Disponible en: <http://www.revistanaval.com/www-alojados/armada/flotaero/maverick.htm>. (Consulta 22/06/2017).

FOLLATH, Erich y Holger Stark. (Febrero 11, 2009). "How Israel Destroyed Syria's Al Kibar Nuclear Reactor". *SPIEGEL*. [En línea]. Disponible: <http://www.spiegel.de/international/world/0,1518>. (Consulta 20/05/2017)

FOX BUSINESS. (Mayo 12, 2017). "Gulf Arab States Push to Develop Their Own Defense Industries". [En línea]. Disponible en: <http://www.foxbusiness.com/features/2017/04/26/ted-nugent-on-cruzs-wall-proposal-idea-is-absolutely-bulletproof.html>. (Consulta 20/05/2017)

FRANCESCHI-Bicchierai, Lorenzo. (Noviembre 23, 2014). "Egyptian Cyber Army: The hacker group attacking ISIS propaganda online". *Mashable*. [En línea]. Disponible en: <http://mashable.com/2017/05/23/aerones-drone-jump/#VY9LW.beNmqI>. (Consulta 20/05/2017)

GARCÍA Sánchez, Pablo. (2016). "La Guerra del Golfo Operaciones Desert Shield y Desert Storm". Grupo de Estudios de Historia Militar. [En línea]. Disponible: <http://www.gehm.es/biblio/La_Guerra_del_Golfo_GEHM.pdf.pdf>. (Consulta 27/03/2017).

GARTENSTEIN-ROSS, Daveed; Nathaniel Barr, y Bridget Moreng. (Marzo, 2016). “The Islamic State’s Global Propaganda Strategy”. *ICCT Research Paper*. [En línea]. Disponible en: <https://www.icct.nl/wp-content/uploads/2016/03/ICCT-Gartenstein-Ross-IS-Global-Propaganda-Strategy-March2016.pdf>. (Consulta 27/03/2017).

GENYS, Andrius. (2007). “BMD-1”. *Military-Today*. [En línea]. Disponible en: <http://www.military-today.com/apc/bmd1.htm>. (Consulta 22/06/2017).

GENYS, Andrius. (2007b). “2S3 Akatsiya”. *Military-Today*. [En línea]. Disponible en: <http://www.military-today.com/artillery/2s3_akatsiya.htm>. (Consulta 22/06/2017).

GLOBAL SECURITY. (Junio 16, 2012). “Defense Industry”. [En línea]. Disponible: <http://www.globalsecurity.org/military/world/iran/industry.htm>. (Consulta 27/03/2017).

GLOBAL SECURITY. (Diciembre 15, 2016). “Emirati Military Spending”. [En línea]. Disponible en: <http://www.globalsecurity.org/military/world/gulf/uae-budget.htm>. (Consulta 27/03/2017).

GLOBAL SECURITY. (2016). Saudi Secret Service (Istakhbarat). *Intelligence*. [En línea]. Disponible en: <http://www.globalsecurity.org/intell/world/saudi/istakhbarat.htm>. (Consulta 10/05/2017).

GLOBAL SECURITY. (Noviembre 5, 2016). “Turkey Domestic Arms Industry”. [En línea]. Disponible en: <http://www.globalsecurity.org/military/world/europe/tu-industry.htm>. (Consulta 27/03/2017).

GOEBEL, Greg. (Octubre 1, 2016). “[2.0] Sukhoi Su-17/20/22”. *Air Vectors*. [En línea]. Disponible en: <http://www.airvectors.net/avsu17_2.html>. (Consulta 22/06/2017).

GRIFFITHS, Martin. (1992). *Fifty Key Thinkers in International Relations*. EE.UU: Routledge.

GROHE, Edwin. (2015). “The Cyber Dimensions of the Syrian Civil War”. *The Johns Hopkins University Applied Physics Laboratory*. [En línea]. Disponible en: <http://www.jhuapl.edu/ourwork/nsa/papers/TheCyberDimensionsoftheSyrianCivilWar.pdf>. (Consulta 27/03/2017).

GUARNIERI, Claudio y Collin Anderson. (Agosto, 2016). “Iran and the Soft War for Internet Dominance”. *Black Hat USA.* [En línea]. Disponible: <https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf>. (Consulta 22/05/2017)

GUTIÉRREZ Amaya, Camilo. (Enero 25, 2013). “¿Qué tan críticos son los sistemas SCADA?”. *We live security*. [En línea]. Disponible en: <http://www.welivesecurity.com/la-es/2013/01/25/criticos-sistemas-scada/>. (Consulta 10/11/2016)

GUTIERREZ DEL MORAL, Leonardo. (2014). *Curso de Ciberseguridad y Hacking Ético*. España: Lantia Publishing 2013.

HALL, Charles H. (Mayo 4, 2011). *Operational Art in The Fifth Domain*. Joint Military Operations Department, Naval War College. [En línea]. Disponible en: <http://www.dtic.mil/dtic/tr/fulltext/u2/a546255.pdf>. (Consulta 28/05/16).

HAMID, Triska. (Junio 6, 2013). “Hacktivism the motivator of cyber attacks in Middle East”. *The National*. [En línea]. Disponible en: <http://www.thenational.ae/business/industry-insights/technology/hacktivism-the-motivator-of-cyber-attacks-in-middle-east>. (Consulta 27/03/2017).

HENDI, Ahed Al. (Mayo 3, 2011). "The Structure of Syria's Repression." *Foreign Affairs*. [En línea]. Disponible en: <https://www.foreignaffairs.com/articles/middle-east/2011-05-03/structure-syrias-repression/>. (Consulta 05/07/2017).

HENNIGAN, W.J. (Septiembre 9, 2011). “Small military contractors flourished after 9/11 attacks”. *Los Angeles Times*. [En línea]. Disponible en: <http://articles.latimes.com/2011/sep/09/business/la-fi-911-aerospace-20110910>. (Consulta 27/03/2017).

HERDEM. (Septiembre 9, 2015). “Turkish Defence Industry: A Step Towards a Nation-Oriented Production”. [En línea]. Disponible en: <http://herdem.av.tr/turkish-defence-industry-step-nationoriented-production/>. (Consulta 23/05/2017).

HILLIER, Stephen. (2017). “Reaper MQ9A RPAS”. *Royal Air Force*. [En línea]. Disponible en: <https://www.raf.mod.uk/equipment/reaper.cfm>. (Consulta 30/06/2017).

HISPANTV. (Diciembre 21, 2016). “HAMAS alerta a Israel que seguirá fabricando drones más avanzados”. [En línea]. Disponible: <http://www.hispantv.com/noticias/palestina/327899/hamas-fabrica-drones-israel-asesinato-experto>. (Consulta 10/04/2017)

HOBSBAWM, Eric. (2009). *La Era de la Revolución, 1789-1848*. Buenos Aíres: Crítica.

HUMAN RIGHTS WATCH. (Diciembre 12, 2003). “Off Target, The Conduct of the War and Civilian Casualties in Iraq”. [En línea]. Disponible en: <https://www.hrw.org/report/2003/12/11/target/conduct-war-and-civilian-casualties-iraq>. (Consulta 19/05/2017)

HUNTINGTON, Samuel. (2005). *El Choque de Civilizaciones y la Reconfiguración del Orden Mundial.* Barcelona: Paidos Iberica.

IASIELLO, Emilio. (Marzo, 2015). “Are Cyber Weapons Effective Military Tools?”. *Military and Strategic Affairs*. Volume 7, No. 1. [En línea]. Disponible en: <http://www.inss.org.il/he/wpcontent/uploads/sites/2/systemfiles/SystemFiles/2_Iasiello.pdf>. (Consulta 13/02/2018)

INTERNATIONAL BUSINESS PUBLICATIONS. (IBP). (2015). *Global National Security and Intelligence Agencies Handbook Volume 1 Strategic Information and Important Contacts*. Estados Unidos: International Business Publications Inc.

INTERNATIONAL TELECOMMUNICATIONS (ITU). (Diciembre 2013). “Cyberwellness Profile Republic of Iraq”. [En línea]. Disponible en: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Iraq.pdf>. (Consulta 27/03/2017).

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU). (Diciembre 2013). “Cyberwellness Profile State of Kuwait”. [En línea]. Disponible en: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Kuwait.pdf>. (Consulta 27/03/2017).

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU). (2014). “Cyberwellness Profile Syria”. [En línea]. Disponible en: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Syria.pdf>. (Consulta 05/07/2017).

INTERNATIONAL TELECOMMUNICATIONS UNION (ITU). (2015). “Cyberwellness Profile Russian Federation”. [En línea]. Disponible en: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Russia.pdf>. (Consulta 06/07/2017).

INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES. (2016). “Drones by country: who has all the UAVs?”. *The Guardian*. [En línea]. Disponible en: <https://www.theguardian.com/news/datablog/2012/aug/03/drone-stocks-bycountry>. (Consulta 13/11/2016).

INTERNET WORLD STATS. (2017). Internet Usage in the Middle East. [En línea]. Disponible en: <http://www.internetworldstats.com/stats5.htm#me>. (Consulta 27/03/2017).

ISLAMIC PHILOSOPHER. (Diciembre 9, 2015). “Ibn Taymiyyah: The Founder Of ISIS”. *Islamic Philosophy*. [En línea]. Disponible en: <http://islam.hilmi.eu/ibn-taymiyyah-the-founder-of-isis/>. (Consulta 10/05/2017).

JELER, Grigore Eduard y Daniel Roman. (2016). “The Graphite Bomb: An Overview of its Basic Military Applications”. *Review of the Air Force Academy*, Núm. 1.

[En línea]. Disponible en: <http://www.afahc.ro/ro/revista/2016_1/Jeler_Roman_2016_1.pdf>. (Consulta 30/06/2017).

JORDÁN, Javier. El Daesh. En *Cuadernos de Estrategia 173 La Internacional Yihadista.* (2015) Instituto Español de Estudios Estratégicos. [En línea]. Disponible: <http://www.ieee.es/Galerias/fichero/cuadernos/CE_173 .pdf>. (Consulta 10/04/2017)

JORDÁN, Javier. (Abril 28, 2014). "Una introducción al concepto de innovación militar*". Grupo de Estudios en Seguridad Internacional (GESI)*. [En línea]. Disponible: <http://www.seguridadinternacional.es/?q=es/content/una-introducci%C3%B3n-al-concepto-de-innovaci%C3%B3n-militar>. (Consulta 26/11/2016).

JORDÁN, Javier. (Junio 9, 2014). "Innovación y Revolución en los Asuntos Militares: una perspectiva no convencional". *Grupo de Estudios en Seguridad Internacional* (GESI). [En línea]. Disponible en: <http://www.seguridadinternacional.es/?q=es/content/innovaci%C3%B3n-yrevoluci%C3%B3n-en-los-asuntos-militares-una-perspectiva-no-convencional>. (Consulta 11/01/15).

KABLE. (2017). "AH-64A/D Apache Attack Helicopter, United States of America". *Army-technology*. [En línea]. Disponible en: <http://www.army-technology.com/projects/apache/>. (Consulta 10/05/2017).

KABLE. (2017b). "SA316 / SA319 Alouette III Light Utility Helicopter, France". *Army-technology*. [En línea]. Disponible en: <http://www.airforce-technology.com/projects/a316sa319alouetteiii/>. (Consulta 22/06/2017).

KABLE. (2017c). "TALON Tracked Military Robot, United States of America". *Army-technology*. [En línea]. Disponible en: <http://www.armytechnology.com/projects/talon-tracked-military-robot/>. (Consulta 22/06/2017).

KABLE. (2017d). "Predator RQ-1 / MQ-1 / MQ-9 Reaper UAV, United States of America". *Army-technology*. [En línea]. Disponible en: < http://www.airforce-technology.com/projects/predator-uav/>. (Consulta 30/06/2017).

KAHANA, Ephraim y Muhammad Suwaed. (2009). *Historical Dictionary of Middle Eastern Intelligence*. Estados Unidos: The Scarecrow Press, Inc.

KAHANA, Ephraim. "Israeli Intelligence: Organization, Failures, and Successes". En Loch K. Johnson (Edit). (2010). *The Oxford Handbook of National Security Intelligence*. Nueva York: Oxford University Press, Inc.

KAPLAN, Caren. (Noviembre 5, 2014). "Air power's visual legacy: Operation Orchard and aerial reconnaissance imagery as ruses de guerre". *Critical Military Studies*. Vol. 1, No. 1, 61–78. [En línea]. Disponible: <http://www.tandf

online.com/doi/pdf/10.1080/23337486.2014.974949?needAccess=true>. (Consulta 20/05/2017).

KAPLAN, Marcos. (2000). C*iencia, Estado y Derecho en las Primeras Revoluciones Industriales*. México: Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas.

KECHICHIAN, Joseph y Jeanne Nazimek. (Septiembre 1997). "Challenges to the Military in Egypt". *Middle East Policy*. [En línea]. Disponible en: <http://www.mepc.org/challenges-military-egypt>. (Consulta 20/05/2017).

KERR, Paul K., John Rollins y Catherine A. Theohary. (Diciembre 9, 2010). "The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability". *Congressional Research Service.* [En línea]. Disponible en: <https://fas.org/sgp/crs/natsec/R41524.pdf>. (Consulta 20/05/2017).

KENG Kuek Ser, Kuang. (Junio 1, 2016). "Where did Iran get its military arms over the last 70 years?". *Public Radio International.* [En línea]. Disponible: <https://www.pri.org/stories/2016-06-01/where-did-iran-get-its-military-arms-over-last-70-years>. (Consulta 20/05/2017).

KINGDOM OF SAUDI ARABIA. (Enero 17, 2010). GIP History. General Intelligence Presidency. [En línea]. Disponible en: <https://web.archive.org/web/20080603022237/http://www.gip.gov.sa:80/sites/English/Pages/History.aspx>. (Consulta 10/05/2017).

KISSINGER, Henry. (2016). *Orden Mundial*. [Versión Kindle]. DOI: 47-49 08021.

KISSINGER, Henry. (1996). *Diplomacia*. México: Fondo de Cultura Económica.

KOPP, Carlo. (Abril, 2012). "NIIP 2K12 Kub/Kvadrat. Self Propelled Air Defence System / SA-6 Gainful". *Air Power Australia*. [En línea]. Disponible en: <http://www.ausairpower.net/APA-2K12-Kvadrat.html>. (Consulta 22/06/2017).

KOPP, Carlo. (2005). "Operation Desert Storm The Electronic Battle". *Air Power Australia*. [En línea]. Disponible: <http://www.ausairpower.net/Analysis-ODS-EW.html>. (Consulta 10/04/2017)

KREPINEVICH, Andrew (1994). "From Cavalry to Computer: The Pattern of Military Revolutions". *The National Interest*. Núm 37, pp. 30-42. [En línea]. Disponible en: <http://users.clas.ufl.edu/zselden/Course%20Readings/Krepinevitch.pdf>. (Consulta 14/01/15).

KUEHL, Daniel. (1997). "Defining Information Power". *Strategic Forum, Institute for National Strategic Studies*. No. 115, junio 1997.

KUPERWASSER, Yosef. (Octubre, 2007). "Lessons from Israel's Intelligence Reforms". *The Saban Center at The Brookings Institution*. Analysis Paper. Número 14. [En línea]. Disponible en: <https://www.brookings.edu/wp-

content/uploads/2016/06/10_intelligence_kuperwasser.pdf>. (Consulta 27/06/2017).

LATAMISRAEL. (Mayo 18, 2017). “Nuevo sistema de defensa aéreo protege a todo Israel contra misiles de alto rango.” [En línea]. Disponible en: <http://latamisrael.com/nuevo-sistema-defensa-aereo-protege-israel-misiles-alto-rango/>. (Consulta 23/05/2017).

LEED, Maren. (Septiembre, 2013). Offensive Cyber Capabilities at the Operational Level: The Way Ahead. *Center for Strategic and International Studies (CSIS)*. [En línea]. Disponible en: <http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf>. (Consulta 01/11/2016).

LEJARZA Illaro, Eguskiñe. (Septiembre 15, 2015). “Terrorismo islamista en las redes – La yihad electrónica”. *Documento Opinión.* [En línea]. Disponible en: <http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO100-2015_IslamismoenRed_EguskineLejarza.pdf>. (Consulta 24/08/2017).

LEWIS, Bernard. (1968). *The Middle East and the West*. London: Weidenfeld and Nicolson.

LEYDEN, John. (Enero 12, 2012). “US killer spy drone controls switch to Linux”. *The Register*. [En línea]. Disponible en: <http://www.theregister.co.uk/2012/01/12/drone_consoles_linux_switch/>. (Consulta 30/06/2017)

LIBICKI, Martin. (1996). “The Emerging Primacy of Information”. *Orbis,* vol. 40, no. 2, primavera, pp. 261-276.

LIEBERMAN, Joseph y Susan Collins. (Mayo 8, 2008). Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat. *United States Senate Committee on Homeland Security and Governmental Affairs*. [En línea]. Disponible en: <https://fas.org/irp/congress/2008_rpt/violent.pdf>. (Consulta 24/08/2017).

LIDDELL Hart, Basil. (1989). *Estrategia: la aproximación indirecta*. Madrid: Ministerio de Defensa, Secretaría Gral. Técnica.

LIDDEL Hart, Basil. (1941). *La Estrategia de la Aproximación Indirecta.* La Editorial Virtual. [En línea]. Disponible en: <https://estrategiauruguay.files.wordpress.com/2014/04/liddel-hart-basil-h_la-estrategia-de-la-aproximacic3b3nindirecta.pdf>. Consulta (22/05/2016).

LIDDELL Hart, Basil Henry. (1991). *Strategy*. EE.UU: Meridian.

LIBICKI, Martin C. (2009). *Cyberdeterrence and Cyberwar*. EE.UU: Rand Corporation.

LINDSAY, Jon R. (Enero 15, 2013). “Stuxnet and the Limits of Cyber Warfare”. *Security Studies*, Volume 22, 2013 - Issue 3, pp. 356-404.

LOCATELL, Andrea. (Octubre, 2013). The Offense/Defense Balance in Cyberspace. *Analysis*. No. 203, p.2. [En línea]. Disponible en: <http://www.ispionline.it/sites/defa ult/files/pubblicazioni/analysis_203_2013.pdf>. (Consulta 1/11/2016).

LONSDALE, David J. (2004). *The Nature of War in the Information Age: Clausewitzian Future*. Gran Bretaña: Frank Cass.

MARKOFF, John y Thom Shanker. (Agosto 1, 2009). “Halted ’03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk”. *The New York Times*. [En línea]. Disponible: <http://www.nytimes.com/2009/08/02/us/politics/02cyber.html>. (Consulta 10/05/2017)

MALLIK, Amitav. (2004). *Technology and Security in the 21st Century A Demand-side Perspective*. SIPRI Research Report No. 20. Stockholm International Peace Research Institute y Oxford University Press. [En línea]. Disponible en: <http://books.sipri.org/files/RR/SIPRIRR20.pdf>. (Consulta 4/11/2016)

MANDIAT. (*s.f.*). APT1: Exposing One of China’s Cyber Espionage Units. [En línea]. Disponible en: <https://www.fireeye.com/content/dam/fireeyewww/services/pdfs/mandiant-apt1-report.pdf>. (Consulta 28/05/2017)

MARTÍ Sempere, Carlos. (2016). *Tecnología de la defensa. Análisis de la situación española*. Madrid: Instituto General Gutiérrez Mellado (UNED).

MARTÍN Muñoz, Gema. (2003). *Iraq. Un fracaso de Occidente (1920-2003)*. Tusquest Editores: Barcelona.

MAZARR, Michael; Jeffrey Shaffer, y Benjamin Ederington. (1993). *The Military Technical Revolution: A Structural Framework*. Washington DC: Center for Strategic & International Studies.

MAWLANA SHAYKH NAZIM ADIL AL-HAQQANI, Sayyid. (Noviembre 16, 2006). “Laylat al Qadr”. *WebIslam*. [En línea]. Disponible en: <http://www.webislam.com/articulos/30070-laylat_al_qadr.html>. (Consulta 21/05/2017)

MCELROY, Damien. (2007). “Armed robots to go to war in Iraq”. *The Telegraph*. [En línea]. Disponible en: <http://www.telegraph.co.uk/news/worldnews/1559521/Armed-robots-to-go-to-war-in-Iraq.html>. (Consulta 30/06/2017).

MCGOOGAN, Cara; James Titcomb y Charlotte Krol. (Mayo18, 2017). “What is WannaCry and how does ransomware work?”. *The Telegraph*. Disponible en: <http://www.telegraph.co.uk/technology/0/ransomware-does-work/>. (Consulta 13/02/2018).

MCGREGOR, Andrew. (2003). « “Jihad and the Rifle Alone”: ‘Abdullah’ Azzam and the Islamist Revolution». *The Journal of Conflict Studies*. Vol 23, No 2. [En línea]. Disponible en: <https://journals.lib.unb.ca/index.php/jcs/article/view/219/377>. (Consulta 10/05/2017).

MCKITRICK, Jeffrey; James Blackwell; Fred Littlepage; Georges Kraus; Richard Blanchfield, y Dale Hill. (1998). *The Battlefield of the Future - 21st Century Warfare Issues*. Air University, No. 3. [En línea]. Disponible en: <http://www.au.af.mil/au/cpc/books/ass ets/battlefield_future.pdf>. (Consulta 30/09/2016)

MEDIA NET. (2017). “Profile a major organization: Nothrop Grumman Middle East”. [En línea]. Disponible en: <http://dhow.com/organization-profile/38863828/northrop-grumman-middle-east/>. (Consulta 21/05/2017)

MELZER, Nils. (2013*). Human Rights Implications of the Usage of Drones and Unmanned Robots in Warfare*. Bélgica: European Union, p. 14. [En línea]. Disponible en: <http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/410220/EXPO-DROI_ET(2013)410220_EN.pdf>. (Consulta 13/11/2016).

MEMRI. (Febrero 11, 2015). “Turkish Media Reports: Syrian Electronic Army (SEA) Leaks Official Confidential Turkish Documents From 2012, Exposing Turkish, Saudi, And Qatari Support for Terrorist Groups”. *Special Dispatch No.5964*. [En línea]. Disponible en: <https://www.memri.org/reports/turkish-media-reports-syrian-electronic-army-sea-leaks-official-confidential-turkish>. (Consulta 21/05/2017)

MESA Delmonte, Luis y Rodobaldo Isasi Herrera. (2004). *Estados Unidos e Iraq, Prólogo para un golpe preventivo*. México: CIESAS

MEYER, David. (Octubre 10, 2011). “Germany accused of using Trojan to spy on citizens”. *ZDNet*. [En línea]. Disponible en: <http://www.zdnet.com/article/microsoft-brings-scale-up-to-sydneys-new-startup-hub/>. (Consulta 13/02/2018).

MICHAEL Duggan, P. (2015). “Strategic Development of Special Warfare in Cyberspace”. *Joint Force Quarterly 79*, pp.46-53. [En línea]. Disponible en: <http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-79/jfq-79_46-53_Duggan.pdf> (Consulta 22/11/2016).

MILITARY FACTORY (2017). “Gulf War (Desert Storm) Weapons (1991)”. [En línea]. Disponible en: <http://www.militaryfactory.com/battles/weapons-of-desert-storm.asp>. (Consulta 22/06/2017).

MILLI İSTIHBARAT TEŞKILATI. (MIT). (2016). “History of the MIT”. [En línea]. Disponible en: <http://www.mit.gov.tr/eng/tarihce.html>. (Consulta 30/07/2017).

MILLI İSTIHBARAT TEŞKILATI. (MIT). (2016). “Organizational structure of the National Intelligence Organization”. [En línea]. Disponible en: <http://www.mit.gov.tr/eng/teskilat.html>. (Consulta 30/07/2017).

MIMOSO, Michael. (Marzo 21, 2013). “Theories abound on Wiper Malware Attack against South Korea”. *Threat Post*. [En línea]. Disponible en: <https://threatpost.com/theories-abound-wiper-malware-attack-against-south-korea-032113/77654/>. (Consulta 13/02/2018).

MINISTRY OF COMUNICATIONS AND TECHNOLOGY. (MCT). (*s.f.*). “لمحة عن الوزارة”. [En línea]. Disponible en: <http://www.moct.gov.sy/moct/?q=ar/node/21>. (Consulta 05/06/2017).

MOLINA Rabadán, David. (2005). “La Revolución de los Asuntos Militares (RMA) en el contexto de la Era de la Información”. *Revista de Estudios de Ciencias Sociales y Humanidades*, no. 14. [En línea]. Disponible en: <http://helvia.uco.es/xmlui/bitstream/handle/10396/10563/7.pdf?sequence>. (Consulta 22/05/2016).

MORGAN, James. (Diciembre 12, 2015). “El bombardero B-52, el avión que simboliza el poderío militar de Estados Unidos”. *BBC*. [En línea]. Disponible en: <http://www.bbc.com/mundo/noticias/2015/12/151210_eeuu_avion_bombardero_b52_finde>. (Consulta 22/06/2017).

MORGUS, Robert; Isabel Skierka; Mirko Hohmann, y Tim Maurer. (Noviembre 19, 2015). “National CSIRTs and Their Role in Computer Security Incident Response”. *GPPi & New America*. [En línea]. Disponible en: <http://www.gppi.net/publications/data-technology-politics/article/national-csirts-and-their-role-in-computer-security-incident-response/>. (Consulta 27/08/2017)

MORRIS, Nigel. (Junio 7, 2013). “Q&A: What is Prism, what does it do, is it legal and what data can it obtain?”. *The Independent*. [En línea]. Disponible en: <http://www.indep endent.co.uk/news/world/americas/qa-what-is-prismwhat-does-it-do-is-it-legal-an d-what-data-can-it-obtain-8650239.html>. (Consulta 10/11/16).

MOTEFF, John y Paul Parfomak (Octubre 1, 2004). *Critical Infrastructure and Key Assets: Definition and Identification*. CRS Report for Congress. [En línea]. Disponible en: <https://www.fas.org/sgp/crs/RL32631.pdf>. (Consulta 11/01/15).

MUELLER, Paul y Babak Yadegari. (2012). “The Stuxnet Worm”. *University of Arizona*. [En línea]. Disponible en: <https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/rept.pdf>. (Consulta 13/02/18).

MUIR, Jim. (Abril 19, 2010). “Senior Iraqi al-Qaeda leaders 'killed'”. *BBC*. [En línea]. Disponible en: <http://news.bbc.co.uk/2/hi/middle_east/8630213.stm>. (Consulta 10/05/2017).

MUNDO MILITAR. (*s.f.*). *El carro de combate M60A3 TTS.* [En línea]. Disponible en: <http://www.pegatiros.com/03_mundomilitar_repor_0020_vehiculos-carro-combate-m60-a3.php>. (Consulta 10/04/2017)

NAAR, Ismaeel. (Enero 23, 2017). “Why does the GCC need its own electronic army?”. *Al Arabiya English.* [En línea]. Disponible en: <http://english.alarabiya.net/en/media/digital/2017/01/23/Why-does-the-GCC-need-its-own-cyber-army-.html>. (Consulta 10/04/2017)

NATIONAL AGENCY FOR NETWORK SERVICES. (NANS). (*s.f.*). “إحداث الهيئة الوطنية لخدمات الشبكة” [En línea]. Disponible en: <http://www.nans.gov.sy/index.php/about-nans/39-about-us>. (Consulta 05/07/2017).

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY. (NGA). (*s.f.*). “ABOUT NGA”. [En línea]. Disponible en: <https://www.nga.mil/About/Pages/Default.aspx>. (Consulta 06/07/2017).

NATIONAL RECONNAISSANCE OFFICE. (NRO). (*s.f.*). “What we do”. [En línea]. Disponible en: <http://www.nro.gov/about/nro/what.html>. (Consulta 06/07/2017).

NATIONAL SECURITY AGENCY (NSA). (Agosto 19, 2016). “Mission & Strategy”. [En línea]. Disponible en: <https://www.nsa.gov/about/mission-strategy/>. (Consulta 06/07/2017).

NAKASHIMA, Ellen. (Mayo 29, 2012). “Iran acknowledges that Flame virus has infected computers nationwide”. *The Washington Post*. [En línea]. Disponible en: <https://www.washingtonpost.com/world/national-security/iran-acknowledges-that-flame-virus-has-infected-computers-nationwide/2012/05/29/gJQAzlEF0U_story.html?utm_term=.e9ef9806a61b>. (Consulta 10/04/2017)

NIEVES, Gema. (Agosto 21, 2012). “El concepto de ‘lobo solitario’”. *Campus Internacional de Seguridad y Defensa (CISDE).* [En línea]. Disponible en: <https://cisde.es/observatorio/el-concepto-de-lobo-solitario>. (Consulta 24/08/2017)

NISHINO, Masami. (Diciembre 16, 2015). “Muhammad Qutb’s Islamist Thought: A Missing Link between Sayyid Qutb and al-Qaeda?”. NIDS Journal of Defense

and Security. [En línea]. Disponible en: <http://www.nids.mod.go.jp/english/publication/kiyo/pdf/2015/bulletin_e2015_6.pdf>. (Consulta 10/05/2017).

NORTHROP GRUMMAN CORPORATION. (2017). *Northrop Grumman in Saudi Arabia*. About us. [En línea]. Disponible en: <http://www.grumman.com/AboutUs/OurGlobalPresence/MiddleEastAndAfrica/SaudiArabia/Pages/default.aspx>. (Consulta 10/05/2017).

NYE, Joseph S. Jr. (Mayo, 2010). *Cyber Power*. Paper, *Belfer Center for Science and International Affairs* – Harvard University. [En línea]. Disponible en: <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>. (Consulta 10/01/15).

OBSERVATORIO DE LA SEGURIDAD DE LA INFORMACIÓN. (*s.f.*). *Esteganografía, el Arte de Ocultar Información.* [En línea]. Disponible en: <http://www.egov.ufsc.br/portal/sites/default/files/esteganografia1.pdf>. (Consulta10/09/2016)

ODOM, William E. (1988). "Soviet Doctrine". *Foreign Affairs*. Invierno, pp. 120-121.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. (*s.f.*). "History". [En línea]. Disponible en: <https://www.dni.gov/index.php/who-we-are/mission-vision>. (Consulta 06/07/2017).

OHLIN, Jens David; Claire Oakes Finkelstein, y Kevin Govern (Edts). (2015*). Cyber War: Law and Ethics for Virtual Conflicts.* Reino Unido: Oxford University Press.

OIC-CERT. (2017). History. [En línea]. Disponible en: <https://www.oiccert.org/en/history.html#.WSsS1WiGPIU>. (Consulta 28/05/2017)

ORGANIZACIÓN DEL TRATADO DEL ATLÁNTICO NORTE (OTAN). (2017). "The history of cyber attacks - a timeline". *NATO Review*. [En línea]. Disponible en: <https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm>. (Consulta 18/02/2018)

OWEN, Taylor. (2015). *Disruptive power*. Estados Unidos: Oxford University Press

OXFORD DICTIONARIES. (2016). "Hacker". *Oxford University Press*. [En línea]. Disponible en: <http://www.oxforddictionaries.com/definition/english/hacker>. Consulta (22/05/2016).

ÖZALP Nuri, Osman. (2011). "Where is the Middle East? The Definition and Classification Problem of the Middle East as a Regional Subsystem in International Relations". TJP Turkish Journal of Politics Vol. 2 No. 2 Winter 2011. [En línea]. Disponible en: <http://www.tau.edu.tr/img/files/where_is_the_middle_east2012_onozalp.pdf>. (Consulta 27/03/2017).

QAIDAARI, Abbas. (Marzo 24, 2016). “Is Iran becoming a major regional arms producer?”. *Al-Monitor*. [En línea]. Disponible en: <http://www.almonitor.com/pulse/en/originals/2016/03/iran-weapons-arms-experts-iraq-syria-lebanon.html>. (Consulta 27/03/2017).

QUIVOOIJPP, Romain. (Junio, 2015). The Islamic State. Policy Report. S. Rajaratnam School of International Studies. [En línea]. Disponible en: <https://www.rsis.edu.sg/rsis-publication/cens/the-islamic-state/>. (Consulta 27/03/2017).

PAGLIERY, Jose. (Agosto 5, 2015). “The inside story of the biggest hack in history”. *CNN*. [En línea]. Disponible en: <http://money.cnn.com/2015/08/05/technology/aramco-hack/>. (21/05/2017)

PANDEY, Ashish. (Julio 18, 2016). “Web of terror: ISIS lists dos and don'ts of social media for jihadis”. *India Today*. [En línea]. Disponible en: <http://indiatoday.intoday.in/story/web-of-terror-isis-lists-dos-and-donts-of-social-media-for-jihadis/1/7142 60.html>. (Consulta 01/03/2017).

PARDO, Pablo. (Abril 7, 2017). “El Tomahawk, un misil con un margen de error de 10 metros”. *El Mundo*. [En línea]. Disponible en: <http://www.elmundo.es/internacional/2017/04/07/58e71e15468aebc5308b45e2.html>. (Consulta 10/05/2017).

PARSCH, Andreas. (2008). “Boeing (McDonnell Douglas) AGM/RGM/UGM-84 Harpoon”. *Directory of U.S. Military Rockets and Missiles*. [En línea]. Disponible en: <http://www.designation-systems.net/dusrm/m-84.html>. (Consulta 10/05/2017).

PARNELL, Brid-Aine. (Mayo 29, 2013). “'Secret Pentagon papers' show China hacked into Patriot missile system”. *The Register*. [En línea]. Disponible en: <http://www.theregi ster.co.uk/2013/05/29/us_weapons_systems_hacked/>. (Consulta10/09/2016)

PASTOR Acosta, Oscar. (Enero 21, 2013). “Seguridad Nacional y Ciberdefensa: Estrategias, Capacidades y Tecnologías”. *Capacidades para la defensa en el ciberespacio, Catedra Isdefe*. [En línea]. Disponible en: <http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Oscar-Pastor.pdf>. (Consulta 28/11/2016).

PIZZI, Michael. (Mayo 29, 2014). “Iran hackers set up fake news site, personas to steal U.S. secrets”. *Al Jazeera America*. [En línea]. Disponible en: <http://america.aljazeera.com/articles/2014/5/29/iran-newscaster-hackers.html>. (Consulta 22/05/2017)

PHILLIPS, Andrew. (Octubre 14, 2012). “The Asymmetric Nature of Cyber Warfare”. *USNI News*. [En línea]. Disponible en: <https://news.usni.org/2012/10/14/asymmetric-nature-cyber-warfare>. (Consulta 27/11/2016).

PHILLIPS, Russell. (2017). *Tanks and Combat Vehicles of the Warsaw Pact.* Reino Unido: Shilka Publishing.

POMPEO, Mike. (Noviembre 9, 2012). “Acerca de la CIA”. *Central Intelligence Agency*. [En línea]. Disponible en: <https://www.cia.gov/es>. (Consulta 24/06/2017).

PRESS TV. (Septiembre 27, 2015). “Some 30,000 foreign fighters have joined the ranks of Daesh: report”. The Syrian Observatory for Human Rights. [En línea]. Disponible en: <http://www.syriahr.com/en/?p=33494>

PRIETO Osés, GB. D. Ramón, et al. (Abril, 2013). *Guerra Cibernética: Aspectos organizativos.* CESEDEN, XXXIII Curso de Defensa Nacional, p. 3 [En línea]. Disponible en: <http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf>. (Consulta 22/11/2016).

PRINGLE, Robert W. “The Intelligence Services of Russia”. En Loch K. Johnson. (2010). *The Oxford Handbook of National Security Intelligence*. EE.UU: Oxford University Press

PRIVACY INTERNATIONAL. (Febrero, 2016). *The President’s Men? Inside the Technical Research Department, the secret player in Egypt's intelligence infrastructure.* [En línea]. Disponible en: <https://privacyinternational.org/sites/default/files/egypt_reportEnglish.pdf>. (Consulta 24/06/2017).

PUYANA García, Gabriel. (2003). “Teorías de la Guerra en Moltke y Liddell Hart”. *Revista de Estudios Sociales,* no. 15, junio de 2003, 109-121.

RAKKAH, Azzedine. (2005). “El mundo árabe después del 11 de septiembre”. *OASIS*, núm. 10, pp. 55-78. [En línea]. Disponible en: <http://www.redalyc.org/pdf/531/53101004. pdf>. (Consulta 27/03/2017).

RASKA, Michael. (Enero, 2015). “Confronting Cyber Security Challenges: Israel’s Evolving Cyber Defense Strategy”. *S. Rajaratam School of International Studies.* Policy Report. [En línea]. Disponible en: <https://www.rsis.edu.sg/wp-content/uploads/2015/01/PR150108_Israel_Evolving_Cyber_Strategy_WEB.pdf>. (Consulta 24/06/2017).

RATTRAY, Gregory J. (2001). *Strategic Warfare in Cyberspace*. Cambridge, MA: MIT Press.

REYES Plata, Alejandro. (2007). "¿Qué es y cómo funciona un ataque DDoS?". *Seguridad IT*. [En línea]. Disponible en: <https://revista.seguridad.unam.mx/numero-12/que-es-y-como-funciona-un-ataque-ddos>. (Consulta 12/02/2018).

ROCHINA, Paula. (Mayo 18, 2016). "Hacktivismo: Qué hay detrás de este movimiento activista?". *Revista digital INESEM.* [En línea]. Disponible en: <https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/>. (Consulta 28/05/2017)

ROSECRANCE, Richard. (Julio 1, 1996). "The Rise of the Virtual State: Territory Becomes Passé". *Foreign Affairs*. Vol. 75, no. 4, pp. 45-71.

RODRÍGUEZ, Alex. (2015). "Cyber: guerra, ataque, espacio y disuasión…". La Ciberguerra. Vanguardia Dossier, No. 54, Enero-Marzo 2015.

RODRÍGUEZ Angulo, Rodrigo D. (2012, Junio). *El hegemonismo militar estadounidense. El impacto de las TIC sobre la realización de la Guerra.* Guerra cibernética. Documento de trabajo nº 103, Buenos Aires. Disponible en: <http://www.ceid.edu.ar/serie/2012/ceid_dt_102_rodrigo_d_rodriguez_angulo_el_hegemonismo_militar_estadounidense_el_impacto_de_las_tic_sobre_la_realizacion_de_la_guerra_guerra_cibernetica.pdf>. (Consulta 14/01/15).

ROGERS, A.P.V. (Marzo 31, 2000). "Una guerra sin víctimas". *Revista Internacional de la Cruz Roja*. [En línea]. Disponible en: <https://www.icrc.org/spa/resources/documents/misc/5tdnzd.htm>. (Consulta 24/11/2016).

ROUSE, Margaret. (Agosto, 2012). "Computer Security Incident Response Team (CSIRT)". *TechTarget*. [En línea]. Disponible en: <http://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT> (Consulta 27/05/17).

ROTHKOPF, David J. (1998). "Cyberpolitik: The Changing Nature of Power in the Information Age". *Journal of International Affairs*. Spring 98, Vol. 51 Issue 2, pp. 325-60.

RUBIN, Barnett R. (2013). *Afghanistan from the Cold War through the War on Terror*. EE.UU: Oxford University Press.

RUBÍN CENTER. (Marzo 3, 2011). "Russia's Military Involvement in the Middle East". *MERIA Journal*, Volumen 5, Número 1. [En línea]. Disponible en: <http://www.rubincenter.org/2001/03/antonenko-2001-03-03/>. (Consulta 27/05/17).

RUBIN, Uzi. (2006). "The Global Reach of Iran's Ballistic Missiles". *Institute for National Security Studies*. [En línea]. Disponible en: <http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/(FILE)1188302 022.pdf>. (Consulta 12/02/18).

RUDNER, Martin. (2013). “Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge”. *International Journal of Intelligence and Counterintelligence*, Núm. 26, pp.453-481.

RUSTICI, Ross M. (2011). “Cyberweapons: Leveling the International Playing Field”. *Parameters*. Autumn, pp. 32-42. [En línea]. Disponible en: <http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2011autumn/Rustici.pdf>. (Consulta 14/01/15).

SAAB, Bilal Y. (Mayo, 2014). *The Gulf Rising*. Washington: The Atlantic Council of the United State.

SAID, Edward. (2002). *Orientalismo.* Madrid: Debate.

SALACANIN, Stasa. (Marzo 13, 2017). “Weapons sales: The key to Russia's Middle East agenda”. *The New Arab*. [En línea]. Disponible en: <https://www.alaraby.co.uk/english/indepth/2017/3/13/weapons-sales-the-key-to-russiasmiddle-east-agenda>. (Consulta 27/05/2017)

SALINAS, Juan José. (Julio 28, 2016). “ISIS – DAESH – ESTADO ISLÁMICO. El origen de la pesadilla”. *Pájaro Rojo.* [En línea]. Disponible en: <http://pajarorojo.com.ar/?p=26290>. (Consulta 12/02/2018)

SÁNCHEZ Méndez, José. (2003). “Las nuevas armas en la Operación Libertad para Irak”. *El País*. [En línea]. Disponible en: <http://elpais.com/diario/2003/03/28/internacional/1048806022_850215.html>. (Consulta 30/06/2017).

SANGER, David E. (Junio 1, 2012). “Obama Order Sped Up Wave of Cyberattacks Against Iran”. *The New York Times.* [En línea]. Disponible en: <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-ofcyberattacks-against-iran.html>. (Consulta 22/05/2017).

SANGER, David E. (Abril 24, 2016). “U.S. Cyberattacks Target ISIS in a New Line of Combat”. *The New York Times*. [En línea]. Disponible en: <http://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?smid=fb-share>. (Consulta 30/09/2016)

SAVIR, Uri. (Julio 5, 2015). “The Middle East's Internet revolution”. *Al-Monitor*. [En línea]. Disponible en: <http://www.almonitor.com/pulse/originals/2015/07/israel-middle-east-internet-revolution-democracy-youth.html>. (Consulta 27/03/2017).

SHERMAN, Robert. (Julio 5, 1999). “Type 63 107mm Rocket Launcher”. *Federation of American Scientists.* [En línea]. Disponible en: <https://fas.org/man/dod-101/sys/land/row/type-63-r.htm>. (Consulta 10/05/2017).

SCHMIDLE, Nicholas. (Septiembre 4, 2011). “La caza del monstruo Bin Laden”. *El País*. [En línea]. Disponible en: <http://elpais.com/diario/2011/09/04/eps/1315117617_850215.html>. (Consulta 10/05/2017).

SCOLARI, Carlos A. (Febrero 10, 2010). “Narrativas Transmedia: 15 Principios”. *Hipermediaciones*. Disponible en: <https://hipermediaciones.com/2010/02/04/narrativas-transmedia-15/>. (Consulta 09/09/2017).

SENGUPTA, Kim. (Enero 29, 2016). “War in Syria: Russia’s 'rustbucket' military delivers a hi-tech shock to West and Israel”. *Independent*. [En línea]. Disponible en: <http://www.independent.co.uk/news/world/middle-east/war-in-syria-russia-s-rustbucket-military-delivers-a-hi-tech-shock-to-west-and-israel-a6842711.html>. (Consulta 27/03/2017).

ŞENTÜRK, Hakan; C. Zaim Çil, y Şeref Sağıroğlu. (2012). “Cyber Security Analysis of Turkey”. *International Journal of Information Security Science*, vol. 1, no. 4. [En línea]. Disponible en: <http://www.ijiss.org/ijiss/index.php/ijiss/article/view/18/112-125>. (Consulta 04/06/2017).

SERRANO, Andres S. (Febrero 14, 1991). “Armas inteligentes para 'disparar y olvidarse'”. *El país*. [En línea]. Disponible en: <http://elpais.com/diario/1991/02/14/internacional/666486026_850215.html>. (Consulta 22/11/2016).

SERVAES, Alain. (Marzo 15, 2011). “SA-2 Guideline Ground-to-air missile system”. *Army Recognition*. [En línea]. Disponible en: <http://www.armyrecognition.com/russia_russian_missile_system_vehicle_uk/sa-2_guideline_s-75_dvina_desna_volchov_ground_air_missile_system_technical_data_sheet_specification.html>. (Consulta 10/05/2017).

SHEPARD, William. (Febrero 15, 2010). “Sayyid Qutb”. *Oxford Bibliographies*. [En línea]. Disponible en: <http://www.oxfordbibliographies.com/view/document/obo-9780195390155/obo-9780195390155-0072.xml>. (Consulta 10/05/2017).

SCHMITT, Michael N. (Edit.). (Marzo, 2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Reino Unido: Cambridge University Press.

SCHREIER, Fred. (2015). *On Cyberwarfare.* DCAF Horizon 2015 Working Paper No. 7. [En línea]. Disponible: <www.dcaf.ch/content/download/.../OnCyberwarfare-Schreier.pdf>. (Consulta 21/05/2017).

SHALAL, Andrea. (Septiembre 28, 2016). “U.S. approves Boeing, Lockheed fighter jet sales to Gulf: sources”. *Reuters*. [En línea]. Disponible en: <http://www.reuters.com/article/us-boeing-fighters-gulf-idUSKCN11Y2TX>. (Consulta 21/05/2017).

SHARMA, Sanjana. (2017). “Cyber Security for the Defence Industry”. *Cyber Security Review*. [En línea]. Disponible: <http://www.cybersecurity-review.com/industry-perspective/cyber-security-for-the-defence-industry/>. (Consulta 21/05/2017).

SIBONI, Gabi. (Abril 29, 2015). “The Impact of Cyberspace on Asymmetric Conflict in The Middle East”. *Georgetown Journal of International Affairs.* [En línea]. Disponible en: <http://journal.georgetown.edu/the-impact-of-cyberspace-on-asymmetric-conflict-in-the-middle-east/>. (Consulta 28/11/2016).

SIERRA Kobeh, María de Lourdes. (2002). *Introducción al Estudio de Medio Oriente. Del surgimiento del Islam a la repartición imperialista de la zona*. México: Universidad Nacional Autónoma de México.

SIGHOLM, Johan. (Abril, 2013). “Non-State Actors in Cyberspace Operations.” *Journal of Military Studies*. [En línea]. Disponible: <https://journal.fi/jms/article/view/7609>. (Consulta 21/05/2017).

SINGER, Peter W. (2015). “Ciberarmas y carreras de armamentos: un análisis”. *La ciberguerra*. Vanguardia dossier, No. 54, pp. 42-47.

SCHMITT, Eric y Somini Sengupta (Septiembre 25, 2015). “Thousands Enter Syria to Join ISIS Despite Global Efforts”. *The New York Times.* [En línea]. Disponible en: <https://www.nytimes.com/2015/09/27/world/mid dleeast/thousands-enter-syria-to-join-isis-despite-global-efforts.html?smid=twshare&_r=1>. (Consulta 25/08/2017).

SMITH, Greg. (2017). “E-8C Joint STARS”. *Military.com.* [En línea]. Disponible en: <http://www.military.com/equipment/e-8c-joint-stars>. (Consulta 10/05/2017).

SMITH, Greg. (2017). “AGM-114 Hellfire”. *Military.com.* [En línea]. Disponible en: <http://www.military.com/equipment/agm-114-hellfire>. (Consulta 10/05/2017).

SMITH, Greg. (2017). “AGM-86 Conventional Air Launched Cruise Missile”. *Military.com.* [En línea]. Disponible en: <http://www.military.com/equipment/agm-86-conventional-air-launched-cruise-missile>. (Consulta 10/05/2017)

SMITH, Rupert. (2005). *The Utility of Force: The art of war in the modern world.* EE.UU: Vintage.

SOBELMAN, Ariel T. (Junio, 1998). “An Information Revolution in the Middle East?”. *Strategic Assessment*, Volume 1, No. 2, pp.13-15. [En línea]. Disponible en: <http://www.inss.org.il/uploadImages/systemFiles/An%20Information %20Revolution%20in%20the%20Middle%20East.pdf>. (Consulta 27/03/2017).

SOFTWARE ENGINEERING INSTITUTE. (2017). *List of National CSIRTs*. Carnegie Mellon University. [En línea]. Disponible: <http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?>. (Consulta 28/05/2017)

SPRINGER, Paul J. (Ed). (2017). *Encyclopedia of Cyber Warfare.* Estados Unidos: ABC-CLIO.

SPUTNIK. (Agosto 13, 2015). "Las mejores armas con tecnologías furtivas". [En línea]. Disponible en: <https://mundo.sputniknews.com/industriamilitar/20150813104031746 3/>. (Consulta 10/05/2017)

SORIA Guzmán, Irene. (Noviembre 2016). *Ética hacker, seguridad y vigilancia*. México: Universidad del Claustro de Sor Juana, p. 23. [En línea]. Disponible en: <http://www.ucsj.edu.mx/pdf/EticaHackerSeguridadVigilancia.pdf>. (Consulta 28/05/2017)

STANFORD UNIVERSITY. (*s.f.*). "The U.S. Defense Industry and Arms Sales". [En línea]. Disponible en: <https://web.stanford.edu/class/e297a/U.S.%20Defense%20Industry%20and%20Arms%20Sales.htm>. (Consulta 27/03/2017).

STANLEY, Trevor. (2005). "Abdullah Azzam 'The Godfather of Jihad'". *Perspectives on World History and Current Events*. [En línea]. Disponible en: <http://www.pwhce.org/azzam>. (Consulta 10/05/2017)

STONE, Corin. (2013). *U.S National Intelligence: An overview 2013*. [En línea]. Disponible en: <https://www.dni.gov/files/documents/USNI%202013%20Overview_web.pdf>. (Consulta 10/05/2017)

STORK, Joe. (1987). "Arms Industries of the Middle East". *Middle East Research and Information Project*. [En línea]. Disponible en: <http://www.merip.org/mer/mer144/arms-industries-middle-east>. (Consulta 27/03/2017).

STROBEL, Warren. (Febrero 10, 2015). "The US is establishing a new cybersecurity agency". *Business Insider*. [En línea]. Disponible en: <http://www.businessinsider.com/the-us-is-establishing-a-new-cybersecurity-agency-2015-2>. (Consulta 06/07/2017)

SUCIU, Peter. (Septiembre 1, 2015). "Why Israel dominates in cyber security". *Fortune*. [En línea]. Disponible en: <http://fortune.com/2015/09/01/why-israel-dominates-in-cyber-security/>. (Consulta 27/03/2017).

SULLIVAN, Gordon y Dubik, James. (1995). *War in the Information Age*. Carlisle Barracks: SSI. [En línea]. Disponible en: <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub243.pdf>. (Consulta 13/01/2015).

SYMANTEC. (2017). "Master Boot Record (MBR) (Registro de arranque maestro [MBR])". *Glosario*. [En línea]. Disponible en: <https://www.symantec.com/es/

mx/security_response/glossary/define.jsp?letter=m&word=master-boot-record-mbr>. (Consulta 13/02/2018).

SYRIAN COMPUTER SOCIETY. (SCS). (s*.f.*). "الجمعية عن لمحة". [En línea]. Disponible en: <http://www.scs.org.sy/ArticlesDetail.aspx?ArticleID=5>. (Consulta 30/06/2017).

TAHIR Ashraf, Mian Muhammad. (2012). "The Clash of Civilizations? A Critique". *Pakistan Journal of Social Sciences (PJSS)*. Vol. 32, No. 2, pp.521-527.

THE CYBER & JIHAD LAB. (Julio 21, 2015). "Experts Suggest Yemen Cyber Army Could Actually Be Iranian". En línea]. Disponible en: <http://cjlab.memri.org/lab-projects/monitoring-jihadi-and-hacktivist-activity/experts-suggest-yemen-cyber-army-could-actually-be-iranian/>. (Consulta13/01/2015).

THE EDITORS OF ENCYCLOPÆDIA BRITANNICA. (2007). *Muhammad ibn 'Abd al-Wahhab*. Encyclopædia Britannica, inc. [En línea]. Disponible en: <https://www.britannica.com/biography/Muhammad-ibn-Abd-al-Wahhab>. (Consulta 10/05/2017).

THE HERITAGE FOUNDATION. (2017). *Middle East.* 2017 Index of U.S. Military Strength. [En línea]. Disponible en: <http://index.heritage.org/military/2017/assessments/operating-environment/middle-east/>. (Consulta 27/03/2017).

THE INTERNATIONAL TRADE ADMINISTRATION. (Diciembre 8, 2016). "United Arab Emirates - Defense". *Export.gov* [En línea]. Disponible en: <https://www.export.gov/article?id=United-Arab-Emirates-Defense>. (Consulta 27/03/2017).

THE SOUFAN GROUP. (Diciembre, 2015). *Foreign Fighters: An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*. [En línea]. Disponible en: <http://soufangroup.com/wp-content/uploads/2015/12/TSG_Foreign FightersUpdate3.pdf>. (Consulta 27/03/2017).

THE WORLD BANK GROUP. (Abril 24, 2017). "Military expenditure (% of GDP)". [En línea]. Disponible en: <http://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?contextual=max&end=2015&locations=RU-1A-US&start=2001&view=chart>. (Consulta 24/04/2017).

THEOHARY, Catherine A. y John W. Rollins. (Marzo27, 2015). "Cyberwarfare and Cyberterrorism: In Brief". *Congressional Research Service*. [En línea]. Disponible en: <https://fas.org/sgp/crs/natsec/R43955.pdf>. Consulta (22/05/2016).

TOFFLER, Alvin. (1980). *The Third Wave*. Londres: Collins Publishers.

TOFFLER, Alvin y Heidi. (1993). *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little Brown.

TOFFLER, Alvin y Heidi. (1994). *Las Guerras del Futuro*. Century. España: Plaza & Janes Editores, S.A.

TOPERCZER, István. (2012). MiG-17 and MiG-19 Units of the Vietnam War. Reino Unido: Osprey Publishing.

TROTT, Bill. (Febrero 18, 2017). "'Blind sheikh' convicted in 1993 World Trade bombing dies in U.S. prison". *Reuters*. [En línea]. Disponible en: <http://www.reuters.com/article/us-usa-tradecenter-rahman-idUSKBN15X0KU>. (Consulta 10/05/2017).

UNITED STATES AIR FORCE. (Diciembre, 2015). "B-52 Stratofortress". [En línea]. Disponible en: <http://www.af.mil/About-Us/FactSheets/Display/Article/104465/b-52-stratofortress/>. (Consulta 10/05/2017).

UNITED STATES AIR FORCE. (Junio 29, 2012). "F-117A Nighthawk". [En línea]. Disponible en: <http://archive.is/20120629101020/http://www.af.mil/information/heritage/aircraft.asp?dec=1970-1980&pid=123006550#selection-442.0-453.16>. (Consulta 10/05/2017).

UNITED STATES CYBER COMMAND (CYBERCOM). (Septiembre 30, 2016). "U.S. Cyber Command (USCYBERCOM)". [En línea]. Disponible en: <http://www.stratcom.mil/Media/Factsheets/FactsheetView/Article/960492/us-cyber-command-uscybercom/>. (Consulta 06/07/2017).

URLI, Joe. (2014). "What do we call them: UAV, UAS or RPAS?". *Association of Australian Certified UAV Operators Inc. (ACUO)*. [En línea]. Disponible en: <http://www.acuo.org.au/industry-information/terminology/what-do-we-call-them/>. (Consulta 10/05/2017).

USA TODAY. (2002). "Operation Iraqi Freedom". [En línea]. Disponible en: <https://usatoday30.u satoday.com/news/world/iraq/bigmap.htm>. (Consulta 23/08/2017).

US AIR FORCE. (Septiembre 23, 2015). "MQ-1B Predator". *Official United States Air Force Website.* [En línea]. Disponible en: <http://www.af.mil/AboutUs/Fact-Sheets/Display/Article/104469/mq-1b-predator/>. (Consulta 30/06/2017).

VALERIANO, Brandon y Ryan C. Maness. (2016). "Cybervictory: The efficacy of Cyber Coerción". Artículo Inédito.

VALLE, Mónica. (Agosto 11, 2015). "Sacan a la luz el mayor ciberataque de la historia". *Globb Security*. [En línea]. Disponible en: <http://globbsecurity.com/aramco-mayor-ciberataque-historia-35593/>. (Consulta 27/03/2017).

VAN CREVELD, Martin. (2005). *The changing face of war: combat from the Marne to Iraq.* EE.UU.: Ballantine.

VENTRE, Daniel. (2015). “Evolución de la guerra desde hace un siglo: aparición de la ciberguerra”. *La ciberguerra.* Vanguardia Dossier, No. 54. Enero-Marzo, 2015, pp. 18-25.

VON Clausewitz, C. (2005). *De la guerra*. España: La Esfera de los Libros.

WALLACE, Mark. (2017). “Abu Musab al-Zarqawi”. *Counter Extremist Project*. [En línea]. Disponible en: <https://www.counterextremism.com/extremists/abu-musab-al-zarqawi>. (Consulta 10/05/2017).

WAGSTAFF, Jeremy y Raju Gopalakrishna. (Mayo 23, 2016). “Hackers probe defenses of Middle East banks: FireEye”. *Reuters*. [En línea]. Disponible en: <http://www.reuters.com/article/us-cyber-heist-mideast-idUSKC N0YE19Q>. (Consulta 22/05/2017)

WALCHKO, Kevin J. (2016). “Cyber Espionage Tools”. *Planet Express.* [En línea]. Disponible en. <https://walchko.github.io/posts/2015/12/cyber-espionage-tools/>. (Consulta 22/05/2017)

WALTZ, Kenneth. (2010). *Theory of International Politics.* EE.UU: Waveland Press.

WAQAS, Amir. (Octubre 18. 2013). “Israeli Think Tank Acknowledges Iran as Major Cyber Power, Iran Claims its 4th Biggest Cyber Army in World”. *Hack Read*. [En línea]. Disponible en: <https://www.hackread.com/iran-biggest-cyber-army-israel/>. (Consulta 22/05/2017)

WATSON, Ben. (Enero 12, 2017). “The Drones of ISIS”. *Defense One.* [En línea]. Disponible en: <http://www.defenseone.com/technology/2017/01/drones-isis/134542/>. (Consulta 25/08/2017)

WATTS, Barry D. (1996). *Clausewitzian Friction and Future War*. Institute for National Strategic Studies. National Defense University. [En línea]. Disponible en: <http://w ww.clausewitz.com/readings/Watts-Friction3.pdf>. Consulta (22/05/2016).

WATTS, Barry D. (2011). The Maturing the Revolution in Military Affairs. Estados Unidos: Center for strategic and Budgetary Assessments.

WEGE, Carl Anthony. (2015). “Iran’s Intelligence Establishment”. *Journal of U.S. Intelligence Studies*. Volumén 21, no. 2. [En línea]. Disponible en: <https://www.afio.com/publications/WEGE%20Iranian%20Intel%20Services%202015%20Sep%2001%20FINAL.pdf>. (Consulta 06/07/2017).

WENGER, Andreas. (2001). “The Internet and the Changing Face of International Relations and Security”. *Information & Security*. ProCon Ltd., Sofia, Bulgaria. [En línea]. Disponible en: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?i d=694&lng=en>. (Consulta 13/01/15).

WENTZ, L. K; C. L. Barry, y S. H. Starr (Eds.). (Julio, 2009). *Military Perspectives on Cyberpower*. Washington, DC: The Center for Technology and National Security Policy at the National Defense University, pp. 2-4. [En línea]. Disponible en: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA505424> (Consulta 22/11/2016)

WHEELER, Deborah. (2002). "Islam, Community, and the Internet: New possibilities in the digital age". Interface: *The Journal of Education, Community and Values.* [En línea]. Disponible en: <http://commons.pacifi cu.edu/cgi/viewcont ent.cgi?article=1010&context=inter02>. (Consulta 17/08/2017)

WILLIAMS, Phil. (*s.f.*). "Organized Crime and Cybercrime: Synergies, Trends, and Responses". [En línea]. Disponible: <http://www.crime-research.org/library/C ybercrime.htm>. (Consulta 29/05/2017)

WINTER, Michael y Kevin Johnson. (Agosto 19, 2014). "Video appears to show Islamic State beheading U.S. journalist". *USA TODAY*. [En línea]. Disponible en: <http://www.usatoday.com/story/news/world/2014/08/19/syria-isis-kidnap ped-journalist-beheaded/14306021/>. (Consulta 25/08/2017)

YENNE, Bill. (2017). *Drone Strike!: UCAVs and Unmanned Aerial Warfare in the 21st Century*. Reino Unido: Crécy Publishing Ltd.

ZETTER, Kim. (Noviembre 19, 2015). "Security Manual Reveals the OPSEC Advice ISIS Gives Recruits". Wired. [En línea]. Disponible en: <https://www.wired.co m/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-pro tocols/>. (Consulta 01/03/2017)