UCAM

UNIVERSIDAD CATÓLICA DE MURCIA

PROGRAMA DE DOCTORADO EN CIENCIAS SOCIALES

"Los nuevos conflictos bélicos del siglo XXI: las amenazas híbridas"

Autor:

D. José María Luque Juárez

Directores:

Dr. D. Cesar Augusto Giner Alegría
Dr. D. Claudio Augusto Payá Santos

Murcia octubre de 2019

UCAM

UNIVERSIDAD CATÓLICA
DE MURCIA

PROGRAMA DE DOCTORADO EN CIENCIAS SOCIALES

"Los nuevos conflictos bélicos del siglo XXI: las amenazas híbridas"

Autor:

D. José María Luque Juárez

Directores:

Dr. D. Cesar Augusto Giner Alegría
Dr. D. Claudio Augusto Paya Santos

Murcia octubre de 2019

UCAM
UNIVERSIDAD CATÓLICA
DE MURCIA

AUTORIZACIÓN DEL DIRECTOR DE LA TESIS PARA SU PRESENTACIÓN.

El Dr. D. Cesar Augusto Giner Alegría y el Dr. D Claudio Augusto Paya Santos, como directores de la Tesis Doctoral titulada "Los nuevos Conflictos bélicos del siglo XXI: Las amenazas híbridas" realizada por D José María Luque Juárez en el departamento de ciencias sociales, **autorizan su presentación a trámite** dado que reúne las condiciones necesarias para su defensa.

Lo que firmamos, para dar cumplimiento a los reales decretos 99/2011,1393/2007,56/2005 y 778/98, en Murcia a 30 de septiembre de 2019.

(1) Si la Tesis está dirigida por más de un Director tienen que constar y firmar ambos.

A mi Mujer y mis Hijos, mi Madre y mi Padre,

y a mis directores Dr. Cesar Augusto y
Dr. Claudio Augusto,

…...por ser el mejor ejemplo de esfuerzo y optimismo

…...con toda mi admiración, cariñó y agradecimiento.

AGRADECIMIENTOS.

No debo y así es mi deseo dejar pasar esta ocasión que se me brinda para agradecer mediante este trabajo a todas las personas que de algún modo han estado apoyándome es este proyecto y han estado presentes en la realización y consecución a buen puerto de mi trabajo de investigación.

Especialmente, quiero destacara el agradecimiento que les debo a mis dos directores de este Trabajo, Dr. Cesar Augusto Giner Alegría y el Dr. Claudio Paya Santos, por su dirección, cuidado y la atención que me han proporcionado durante estos tres años intensos. Queridos amigos, sabéis muy bien cuál ha sido vuestro papel tan necesario y sin el cual nunca hubiera conseguido mi propósito y el éxito del mismo, vuestros méritos, así como vuestros valores que justifican este agradecimiento.

De igual forma quiero agradecer Al consejo de Gobierno de la UCAM, en especial a su presidente D. José Luis Mendoza, así como a todos los profesores de las diferentes actividades, sin los cuales no hubiera podido superar las mismas con unas notas media de sobresaliente y que me han sido de una ayuda importantísima para la consecución del Trabajo.

También quiero agradecer a mis compañeros de trabajo de la Policía Local de Alcoy por su apoyo y tiempo, a mi compañero doctorando de UCAM, el Inspector jefe de Dolores D. Cristian Cañizares y en especial a mi Jefe Comisario D. David Lerma i Blasco por todos los consejos que me ha aportado para poder finalizar con éxito mi propósito.

Sería ingrato si no acabo este apartado con el agradecimiento enorme a toda mi familia. En primer lugar, a mis padres José y Ana ya que sin ellos nunca sería la persona que soy, dándome un gran ejemplo de cómo deber ser el ser humano como persona, siendo ellos el principal ejemplo que he seguido en mi vida. Igualmente agradecer a mi esposa Lirios su tiempo destinado en este proceso en el cuidado de mis hijos pequeños, Iñaki y Emma. Para finalizar con los agradecimientos mencionar a mí hermano Francisco que me ha aportado su apoyo en los momentos difíciles vividos estos tres años. No finalizare este punto

sin mencionar nuevamente a una persona que quiero como un hermano, unos de mis directores Dr. Claudio Paya Santos y a otro gran amigo D. José Luis Rus Garzón y a D. Juan José Delgado Moran, que han sido de vital ayuda e importancia para alcanzar mis objetivos.

Si de alguna forma no te identificas en estos agradecimientos, estas palabras son para ti, por tu amistad y buen hacer, y sobre todo por tus consejos que tanto me han servido y me han aportado a este objetivo que me plantee hace ya tres años.

Y agradecer a Dios por haberme permitido conocer a personas como vosotros y que habéis estado en mis pensamientos en la elaboración de estos agradecimientos.

INDICE

RESUMEN

El propósito de este trabajo es analizar la guerra asimétrica, compararla con la guerra convencional, y mostrar las medidas en que los países afectados pueden beneficiarse de los resultados de la investigación y elaborar al final un plan para hacer frente a cualquier agresión.

En esta investigación, se abordarán los diferentes tipos de guerra y métodos de lucha, y la definición de cada tipo o método de ellos, según diferentes escuelas de guerra. Seguidamente se presentará el desarrollo de estos métodos de combate hasta el día de hoy, centrándose en los conceptos y principios de la lucha en ambas guerras convencional y asimétrica, con una explicación exhaustiva de la guerra asimétrica y su evolución de generación en generación.

Se abordarán entonces las formas de enfrentar a las tácticas y métodos de combate formas que algunos Estados utilizaron para enfrentar a tales métodos, y las acciones que han tomado para superar este dilema.

Las Tecnologías de la Información y las Comunicaciones (TIC´s) han provocado el nacimiento de la llamada Sociedad de la Información y del Conocimiento. Actualmente, el ciberespacio se entiende como lugar de encuentro para millones de personas en el que todo está interconectado, lo que está provocando que la red no pare de aumentar, y que su repercusión para la sociedad tenga efectos extraordinarios, diciéndose que su aparición ha supuesto un antes y un después en la era de la información y la comunicación.

La revolución de las TIC´s, como concepto amplio, abierto y dinámico que recoge todos los elementos y sistemas empleados hoy en día para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, aún no ha finalizado ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio continuará expandiéndose y evolucionando en las décadas venideras.

En los últimos años se ha debatido mucho sobre la naturaleza y características de las amenazas híbridas, concepto ambiguo, innovador, dinámico y flexible que incluye casos tan diversos como los actos violentos perpetrados por civiles militarizados filo-rusos en el Este de Ucrania, o ciber-ataques contra estructuras críticas públicas en los Países Bálticos, o las masivas campañas de

fakenews y manipulación de las redes sociales durante el referéndum por el Brexit en el Reino Unido y las recientes elecciones presidenciales en Estados Unidos y Francia. El objetivo de esta tesis es analizar las diferentes aproximaciones que sobre dicho concepto se han generado, con el objetivo de hacer un primer estudio de los diversos modos de pensar estas nuevas dinámicas conflictuales que moldearán el mundo del futuro. Se intentará aportar aquí claridad conceptual sobre el tema, para afrontar los distintos desarrollos institucionales y de estrategia analítica operativa que se han ido generando a partir de la concienciación por parte de la comunidad internacional de la imperiosa necesidad de regular tan complejo fenómeno.

Keywords: Conflicto, Terrorismo, OTAN, Desarrollo tecnológico, Competitividad militar y, guerra convencional, guerra asimétrica, cibertaque, ciberespacio.

ABSTRACT

The purpose of this work is to analyze asymmetric warfare, to compare it with conventional warfare, and to show the measures in which affected countries can benefit from the results of the investigation and elaborate at the end a plan to deal with any aggression.

This research will address the different types of warfare and methods of fighting, and the definition of each type or method of them, according to different combat schools, as will be presented the development of these methods of combat to this day, focusing on the concepts and principles of the struggle in both conventional and asymmetric wars, with a thorough explanation of asymmetric warfare and its evolution from generation to generation.

It will address the ways as well to confront the asymmetric combat tactics and methods of the large traditional armies and will examine some of the ways some States used to confront such methods, and the actions they have taken to overcome this dilemma.

Information and Communication Technologies (TIC´s)) have caused the birth of the so-called Information and Knowledge Society. Currently, the cyberspace is understood as a meeting place for millions of people where everything is interconnected, which is causing the network to not increase, and that its impact on society has extraordinary effects, saying that its appearance has meant a before and after in the era of information and communication.

The TIC.s revolution, as a broad, they open and dynamic concept that includes all the elements and systems used today for the treatment of information, its exchange and communication in today's society, has not yet ended nor will it in a long time , which means that cybercriminality or crime associated with cyberspace will continue to expand and evolve in the coming decades.

In recent years there has been much debate about the nature and characteristics of hybrid threats, an ambiguous, innovative, dynamic and flexible concept that includes cases as diverse as violent acts perpetrated by militarized philo-Russian civilians in Eastern Ukraine, or cyberattacks against public critical

structures in the Baltic countries, or the massive campaigns of fake news and social media manipulation during the Brexit referendum in the United Kingdom and the recent presidential elections in the United States and France. This chapter aims to analyze the different approaches that have been generated on this concept, with the objective of making a first study of the different ways of thinking these new conflictive dynamics that will shape the future world. The chapter will attempt to provide conceptual clarity on the subject, to face the different institutional developments and operational analytical strategy that have been generated from the awareness on the part of the international community on the imperative need to regulate such a complex phenomenon.

Key words: Conflict, Terrorism, NATO, Technological development, Military competitiveness, Conventional warfare, asymmetric warfare, cyber attack, cyberspace.

-INTRODUCCIÓN -

I. INTRODUCCIÓN

1.1 APORTE ORIGINAL QUE SUPONDRÍA EN EL CAMPO CIENTÍFICO CORRESPONDIENTE E INTERÉS DEL PROYECTO.

La originalidad del proyecto está en encarar una temática novedosa como es la de las guerras híbridas, de muy poca producción bibliográfica en nuestro ámbito académico y relacionarla específicamente con la actividad del Estado Español.

De este modo, no sólo se logrará ofrecer un trabajo doctoral de importante valor académico, sino que también será útil referencia para el innovador debate que a nivel nacional y regional se incrementará en los próximos años sobre este fenómeno global. Esto implica no sólo actividades de campo, sino también el análisis de su influencia y atención por parte de los medios de comunicación, de los discursos políticos y sociales, del sector empresarial y de su proyección a otras áreas de la sociedad.

Dentro de estos fenómenos llevare a cabo un estudio profundo de las amenazas híbridas que están aumentando considerablemente en el ciberespacio con la utilización de las nuevas tecnologías. Otro fenómeno que está en aumento y que preocupa a la sociedad son los ataques terroristas con suicidas, lo conocidos como “lobos solitarios”.

La guerra es un fenómeno constante a lo largo de la historia de la humanidad, en su naturaleza constante, y también es un fenómeno cambiante en sus formas y medios en constante evolución. Las guerras crecen y evolucionan a lo largo de la historia en sus artes y métodos de gestión de generación en generación, como cualquier desarrollo natural que se produzca en diferentes aspectos de la vida, a pesar de las ideas avanzadas proporcionadas por el pensamiento humano para el establecimiento de sistemas para el propósito de la felicidad humana y la preservación de su dignidad en su patria y la renuncia a las guerras, y al logro del mayor nivel de seguridad. Todos estos se encuentran bajo valores y normas morales y éticas que garantizan todos sus derechos.

Durante las fases históricas que los pueblos han sufrido en sus conflictos, las sucesivas generaciones de guerras han evolucionado para satisfacer las crecientes necesidades de gestión de tales conflictos en todo el mundo. Generaciones de guerras se han movido a lo largo de los años de una etapa a otra en un desarrollo natural, que ha llevado ideas y visiones. Estos han llevado a la modernización de todo el sistema bélico, de la formación de los individuos a la calidad del arma utilizada, las teorías y los planes militares, pero la deficiencia humana está presionando para las soluciones violentas, de modo que los países del mundo se conviertan en campos de la lucha y de las guerras entre los seres humanos.

Esta evolución de los conceptos y principios de las operaciones ha sido una tendencia de dos vías, donde tenían lugar movimientos revolucionarios y liberales en algunos Estados y grupos armados y terroristas, que han adoptado los principios de la guerra de guerrillas frente a fuertes ejércitos regulares. Más tarde se han llamado guerras asimétricas, y como esos movimientos los han seguido algunos estados militarmente débiles, los mismos principios han sido adoptado por ellos frente a Estados poderosos, y estas se han llamado guerras desequilibradas.

Por otro lado, las grandes potencias, que poseen enormes poderes militares, han hecho cambios en sus doctrinas de operaciones, para que puedan enfrentar la guerra asimétrica, donde los Estados Unidos han ideado y adoptado una manera de confrontar a los grupos que adoptan tácticas no beligerantes asimétricas y poco convencionales. Entonces, la calificaron de "guerras irregulares", y desarrollaron principios y conceptos que se adoptaron en algunas unidades sin descuidar los principios convencionales de la guerra que permanecieron en otras unidades, y que son indispensables para cualquier conflicto convencional cuando enfrentarse a ejércitos regulares.

En definitiva, lo que pretendemos a través de la realización de la Tesis doctoral es poder demostrar que:

- Nos encontramos en un tipo de conflicto bélico complejo con la utilización simultanea de medios convencionales e irregulares y por tanto una guerra

asimétrica o por el contrario no existe cambio alguno a los conflictos existentes antes de Siglo XXI

- En un contexto mundial líquido y de revolución tecnológica, las amenazas híbridas representan el más innovador y desafiante escenario para los expertos en Seguridad y Geopolítica.

- Las guerras ya no se declaran, y las batallas se producen cada vez más en el espacio informativo.

- Rusia con toda su maquinaria intenta debilitar tanto la UE como otras zonas de interés estratégico para ellos.

Para el estudio de esta tesis doctoral definiremos la guerra como un acto político, un acto violento y un acto de voluntad.

Esta decisión de emplear las armas corresponde al poder político. Una vez que este poder decide entrar en acción hay que tener en cuenta tres cuestiones muy importantes, en primer lugar el fin que se pretende alcanzar con la misma, en segundo lugar el modo y las armas que se van a utilizar para poder alcanzar el fin que se persigue y por último que medios tanto humanos como técnicos han de emplearse.

Una de las definiciones más exactas, según mi punto de vista fue la llevada a cabo por Hoffman que define la amenaza híbrida como "cualquier adversario que de manera simultánea y adaptativa emplea una mezcla de armas convencionales, tácticas irregulares, terrorismo y comportamiento criminal en el espacio de la batalla para alcanzar sus objetivos políticos.[1]"

Se trato de una definición muy interesante en ese momento porque a partir del mismo se extraen una serie de consecuencias estratégicas y de innovación militar a la hora de hacer frente a otros enemigos otorgando un plus de capacidad para la batalla.

---

[1] Hoffman, FRANK G. (2007) Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies.

Esta definición cobro más fuerza cuando un año después Hizbollad demostró en un estudio que podía alternar tácticas irregulares propias de una insurgencia con capacidades militares y tecnológicas avanzadas propias de un ejército como por ejemplo los drones y varios tipos de misiles.

Estos autores ya ponían de manifiesto el poderío que poseen actores estatales como el nortecoreano, motivando con ello a otros actores, tanto estatales como no estatales, a buscar nuevos mecanismos de tipo tecnológico y nuevas estrategias tendentes a obtener ventajas sobre el enemigo. Con ello se pretende llevar el conflicto lo más alejados de las fronteras, hecho que se produce cuando a la presencia de grupos estatales se reincorporan otros grupos no oficiales o no estatales, consiguiendo con ello que el impacto sobre su territorio afecte el menos posible desde todos los puntos de vistas, principalmente los económicos o sociales.

Otro de los problemas principales que existen con estos grupos no estatales se fundamenta en su campo de actuación donde operan al margen de la ley es la responsabilidad de sus actos. El primero de los problemas es la dificultad para identificarlos, sobre todos a sus líderes. Es evidente que si se tratara de grupos estatales, estos serían juzgados por las leyes internacionales como posibles autores de Crímenes de guerra con la humanidad ante la Corte Penal Internacional, mientras a que a los otros grupos, como terrorismo, el castigo es mas de carácter de exclusión social y por tanto con mayor supervivencia en el tiempo.

Lo que pretenden estos grupos no oficiales no es el exterminio del enemigo sino debilitarlo con fuertes y sorpresivos ataques, consiguiendo con ello condicionar las actuaciones de los estados y sembrar el terror en la población, deslegitimar su lucha haciéndolos actuar de modo irregular o haciendo creer a la opinión pública que están en contra de las normas internacionales, siendo conscientes de que en un enfrentamiento bélico regular no existe ninguna posibilidad de éxito.

Otra definición a tener en cuenta fue la elaborada por el español Calvo Albero que define a la guerra híbrida "como aquella en la que al menos uno de los adversarios recurre a una combinación de operaciones convencionales y guerra

irregular, mezclada esta últimas con acciones terroristas y conexiones con el crimen organizado.[2]"

Del análisis de estas definiciones, según mi opinión podemos definir la "guerra híbrida" como aquella que está concebida para que se tenga en cuenta un nuevo tipo de conflicto en el cual parecen estar presentes el empleo de miedos convencionales e irregulares, idea que está recibiendo una gran atención desde el punto de vista militar y académica, a pesar de que está generando muchas controversias en los expertos.

Como se menciona en el punto anterior, es importante destacar que el término de Guerra Híbrida no es compartido por todos los expertos o estudiosos de la materia generándose un importante debate entre el termino de "Guerra Híbrida" con otros como "Guerra compuesta", "Guerra combinada", "Amenaza híbrida", "Conflicto Híbrido " etc.

Este tipo de conflictos que van a ser objeto de estudio y que son característicos del mundo globalizado, son analizados por los estudiosos en mayor proporción en asuntos de carácter militar y hace referencia al análisis por una parte de los actores involucrado, entre los que formaría por una parte los Estados unidos, los grupos guerrilleros y terroristas, las redes criminales o los contratistas militares privados, y por otra parte de los medios utilizados entre los que destacan el armamento sencillo y asequible utilizado de forma novedosa, los sistemas de armas altamente sofisticadas y las nuevas tecnologías, y por último las tácticas empleadas , acciones convencionales limitadas, actos terroristas, operaciones de información, lobos solitarios, operaciones de información , sistemas de posicionamiento y geolocalización, redes sociales, redes de información y sobre todos el uso de las comunicaciones más avanzadas que permite el uso de Internet.

---

[2] Calvo Albero, JOSÉ LUIS. (2009) La Evolución de las Insurgencias y el concepto de Guerra Híbrida. Revista Ejército Nro. vol. 822, p. 6-13.

Sería un grave error no añadir a este tipo moderno de conflicto la financiación y la estrecha colaboración que puede existir con el crimen organizado. Una diferencia muy importante, si la comparamos con las guerras convencionales, la encontramos en el tipo de guerra que en muchos de sus casos va dirigida a sector determinado de la población y el agresor suele recurrir a actuaciones clandestinas y con ello no asume la responsabilidad y con ello las posibles represalias.

Cabe destacar, en referencia al campo de batalla que en este tipo de Guerras híbridas se integran una serie de componentes importantes de los cuales destacaremos:

1.- La disposición de armas balísticas. Este componente se caracteriza por su bajo coste, por su simplicidad técnica a la hora de su uso y por la facilidad con que penetran en los territorios enemigos, destacando que en alguno de ellos este uso de armas está legalizado. A esta facilidad hay que añadir la dificultad que se planeta a la hora de prevenir ataques y la localización de los atacantes. En este componente cabe destacar que en la actualidad el uso de cohetes y misiles son muy importante por sus efectos disuasorio y el desgaste que produce.

2.- El uso de las armas y métodos de operaciones que dan lugar a un número alto de víctimas y combatientes. En este punto destacaremos los ataques terroristas suicidas y uso de artefactos explosivos improvisados. El atentado terrorista es el eje central de una guerra asimétrica. En el contexto de guerra asimétrica no es tan importante causar bajas en el enemigo, sino condicionar los comportamientos políticos de grandes audiencias a través de sembrar el miedo y la intimidación en la población, trasladado la sensación de fracaso en la misma.

3.- La utilización de los medios de comunicación y los esfuerzos de propaganda destinados a todos los ámbitos, tanto al adversario como a la población local y la comunidad internacional. Lo que se pretende con este componente el legitimar al oponente para el uso de las fuerzas militares.

4.- Mejorar la capacidad de supervivencia. Esta mejora se logra fundamentalmente con los medios de protección, sobre todo utilizando medios de camuflaje o engaño que dispersan las fuerzas militares, creando una confusión deliberada de las instalaciones militares y civiles, llevando el conflicto a un

entorno urbano, donde encuentra por un lado una mayor densidad de población y por otro lado la existencia abundante de los medios de comunicación, que como se ha mencionado en el punto anterior en un componente muy importante.

Todas estas características demuestran una evidente diferencia de las guerras del siglo XXI con las guerras más importante de la Época Moderna y Contemporánea, En estos tipos de guerras los ejércitos se enfrentaban a conflictos convencionales y simétricos claramente definidos.

Ante la imposibilidad de combatir con las técnicas convencionales, el enemigo suele atacar con ataque muy limitados, emboscadas y principalmente acciones terroristas donde últimamente destacan los conocidos como Lobos Solitarios, atentados terroristas donde en atacante es una sola persona o un grupo muy reducido que hace uso de medios muy económicos y la utilización de las redes sociales donde la comunicación es rápida y prácticamente sin coste.

Este tipo de conflictos también ha afectado a las fuerzas armadas de nuestro país, principalmente al ejército de tierra. Es evidente que no se plantea de igual forma una misión bélica si nos encontramos en un escenario donde persiste o hay riesgo de la existencia de una guerra irregular de baja intensidad, que si por el contrario el escenario puede dar lugar a un riego elevado de guerra híbrida donde aumenta considerablemente dicha intensidad.

Para finalizar con esta breve introducción del tema de mi proyecto de tesis, destacar que el pasado 06 de abril de 2016 La Comisión Europea y la Alta Representante adoptaron un marco común para luchar contra las amenazas híbridas y fomentar la resiliencia de la UE, de sus Estados miembros y de los países socios, al tiempo que intensifican la cooperación con la OTAN en la lucha contra esas amenazas.

Este documento definía las amenazas híbridas como:

"Una mezcla de actividades que suelen combinar métodos convencionales y no convencionales y pueden ser utilizadas de forma coordinada por agentes estatales o no estatales, manteniéndose por debajo del umbral de una guerra

declarada oficialmente. Su objetivo no es solo causar daños directos y aprovechar las vulnerabilidades, sino también desestabilizar las sociedades y crear ambigüedades que dificulten la toma de decisiones[3]".

La Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, Federica Mogherini, ha hecho las declaraciones siguientes:

"En los últimos años, el panorama de la seguridad ha cambiado radicalmente. Hemos visto el aumento de las amenazas híbridas en las fronteras de la UE. Se ha instado enérgicamente a la UE a adaptar e incrementar sus capacidades de proveedor de seguridad. Debe seguir reforzándose la relación entre seguridad interior y exterior. Con estas nuevas propuestas, deseamos reforzar nuestra capacidad de lucha contra las amenazas de naturaleza híbrida. En este empeño, intensificaremos asimismo la cooperación y coordinación con la OTAN[4]".

Igualmente, Elżbieta Bieńkowska, Comisaria de Mercado Interior, Industria, Emprendimiento y Pymes, ha señalado lo siguiente:

"La UE debe pasar a ser un proveedor de seguridad capaz de adaptarse y anticiparse y de reaccionar ante la naturaleza cambiante de las amenazas a las que nos enfrentamos. Ello implica reforzar desde dentro nuestra capacidad de resiliencia y nuestra seguridad y aumentar a su vez nuestra capacidad de lucha contra las nuevas amenazas externas. Con este marco, actuamos al unísono para luchar contra las amenazas híbridas comunes. Presentamos propuestas concretas para que la Unión y los Estados miembros aumenten la cooperación en materia de seguridad y defensa, mejoren la resiliencia, solventen las vulnerabilidades estratégicas y preparen una respuesta coordinada[5]".

---

[3] Nota de prensa de la Comisión Europea de seguridad (2016): La UE refuerza su respuesta a las amenazas Híbridas, Bruselas.

[4] Federica Moggherini, (2016) Alta Representante de la Unión Europea en asuntos Exteriores y Política de Seguridad

[5] Elzbieta Bienkowska, (2016) Comisaria de Mercado Interior, Industria, emprendimiento y Pymes.

Lo que se pretende en esta comisión europea es de dar una respuesta en común a las amenazas híbridas, respuesta que sea más eficiente y rápida ante las últimas amenazas y atentados que van cada vez más en aumento con mayor intensidad y produciendo un gran impacto sobre la sociedad.

1.2 ESTADO ACTUAL.

Tras el análisis y revisión literaria, encontramos el término de "Guerra Híbrida" en los años 2002 para advertir de las tácticas que se emplearon por parte de la insurgencia chechena contra el ejército ruso. No obstante, este término fue empleado por primera vez de manera oficial en el año 2005 por el ministerio de defensa de los Estados Unidos con el cual se explicaba la combinación existente entre dos o más amenazas de tipo tradicional, irregular, catastrófico o disruptivo.

La denominación de guerra híbrida aparece por primera vez en un artículo publicado en la prestigiosa revista Proceedings, en el año 2005 por Mattis y Hoffman en su obra "Future Warfare: The Rise of Hybrid Wars" donde destacaban una superioridad de los Estados Unidos y advertían que dicha superioridad crearía una lógica que impulsaría a los actores estatales y no estatales a abandonar el modo tradicional de hacer la guerra y buscar una capacidad o algún tipo de combinación de las nuevas tecnologías con tácticas que les permitiera obtener alguna ventaja sobre su adversario.

No obstante, hasta un año después no aparece en un artículo científico, "La guerra del futuro: la llegada del conflicto híbrido", del General James Mattis y el Teniente Coronel Frank G. Hoffan los cuales acuñaron este término hasta la actualidad, y advertían que la superioridad de Estados Unidos crearía una lógica que impulsaría a los actores estatales y no estatales a abandonar el modo tradicional de hacer la guerra y a buscar una capacidad combinando muevas tácticas y métodos de ataque y defensa.

Este concepto de guerra híbrida se ha ido ampliado en otros ámbitos importantes, abarcando múltiples aspectos del panorama de la seguridad internacional y de las políticas criminales. Dentro del ámbito internacional podemos encontrar la desinformación en el ciberespacio por parte de Rusia, carteles de drogas, la construcción de islotes artificiales por parte de china, ciber

ataques por parte de corea del norte, la radicalización y el terrorismo yihadista, siendo este último el más habitual en la actualidad.

Uno de los ejemplos más importantes referente a la guerra híbrida lo encontramos en la agenda de trabajo del centro Europea de Excelencia de Amenazas Híbridas con sede en Finlandia.

Su primera manifestación practica fue llevada a cabo en la guerra del verano de 2006 entre Israel y Hezbolah en la presentación del ensayo "El conflicto en el siglo XXI: el advenimiento de la guerra híbrida.[6]"Tras la definición llevada a cabo a raíz de la mencionado guerra de 2006, el termino de guerra híbrida se ha popularizado entre la comunidad estratégica para llevar a cabo las explicaciones de las tácticas, de los métodos y sobre todo de los medios que se han utilizado por parte de las insurgencias iraquís y afganas, la oposición por parte de siria o el Estado Islámico en Iraq y Rusia, integrándose por una parte en la terminología empleada por los Estados Unidos así como por la parte aliada para llevar a cabo una explicación de la complejidad de este tipo novedoso de guerras del siglo XXI.

No obstante, a pesar de haberse formalizado entre la comunidad de expertos, de ser llevada a cabo la consolidación en la jerga militar y haberse utilizado en muchos documentos estadounidenses y aliado, el concepto de "Guerra Híbrida" no es el único utilizado para definir este tipo de conflicto bélico.

Otro ejemplo de este tipo de guerras lo podemos encontrar en la denominada segunda guerra del Líbano en la cual hubo un enfrentamiento entre las Fuerzas de defensa de Israel contra los objetivos de la agrupación chiita libanesa Hezbolá. En ella hubo la intervención de ejércitos paramilitares que estaban ocupados en el sur del Líbano, dando lugar a una guerra irregular y sorpresiva que debilitaba al otro bando, una guerra poca tradicional donde no se puede definir claramente al enemigo. Estos ataques se llevan a cabo en zonas densamente pobladas donde se usan a la población civil como escudos humanos, siendo estas otras de las características de una guerra Híbrida.

---

[6] Hoffman, FRANK G. (2007) Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies.

Más ejemplos lo encontramos ya en 2008-2009 donde el ejército israelí sufrió un duro golpe durante las guerras contra Hamás en la franja de Gaza (2008) Plomo fundido, 2012 (Pilar Defensivo) y 2014 (Margen Protector).

Como documento más reciente en referencia a las amenazas híbridas encontramos la comisión europea de 06 de abril de 2016, en un comunicado de prensa "Seguridad: La UE refuerza su respuesta a las amenazas híbridas[7]".

En dicho documento, hace referencia a las amenazas híbridas donde destaca que cada vez están más expuestos todos los países miembros y que incluyen una serie actuaciones hostiles destinadas principalmente a desestabilizar un Estado o Región. Lo que se pretende con este documento es dar una respuesta en común intensificando la cooperación de todos los países miembros. Son consciente de que en común se dará una mejor respuesta, siempre una respuesta en conjunto es más fuerte que de forma individual. En consecuencia, La UE debe dar una respuesta conjunta a los retos que se nos avecinas ante estas amenazas o guerras híbridas.

La UE entiende que en gran medida se trata de asunto de competencia nacional, y que la responsabilidad radica en cada uno de los estados miembros. No obstante, en este marco común se pretende ayudar a todos los estados miembros y a sus socios para poder combatir estas amenazas híbridas y mejorar la resiliencia, combinado instrumentos europeos y nacionales para una mejor eficacia y una mejor directriz para llevar a cabo políticas criminales.

La OTAN también ha dado la importancia que se merece estas nuevas amenazas intentando adaptarse a ellas, siendo uno de los retos del recién acreditado Centro de Excelencia de la OTAN de «Strategic Communications» localizado en Riga (Letonia) -el emplazamiento no es baladí-.

Esta institución fue reconocida en la última cumbre de Gales con una declaración final que incluía en su punto 13 la necesidad de afrontar de modo solvente el desafío de la guerra híbrida. De nuevo con Rusia en el horizonte.

---

[7] Nota de prensa de la Comisión Europea de seguridad (2016): La UE refuerza su respuesta a las amenazas Híbridas, en Bruselas.

1.3 METODOLOGÍA DE LA INVESTIGACIÓN.

La investigación doctoral que aquí se presenta se inserta dentro de los estudios en al ámbito de las ciencias sociales referentes a las amenazas a nivel global, concretamente la Seguridad Internacional. Teniendo en cuenta la naturaleza compleja y dinámica de este tipo de amenazas para la seguridad, principalmente el terrorismo islámico y la ciberseguridad como fenómeno objeto de estudio, la investigación se articula en torno a un método de análisis cualitativo.

Teniendo en cuenta el método descriptivo que consiste en realizar una exposición narrativa, numérica y/o gráfica, lo más detallada y exhaustiva posible de la realidad que se investiga.[8], Dicho método es utilizado en la presente investigación doctoral para exponer la naturaleza de las nuevas amenazas a la seguridad y utilizadas en los conflictos bélicos como realidad y objeto de estudio principal.

El método descriptivo es utilizado junto al método teórico-jurídico en el inicio de todas las fases y capítulos de esta tesis doctoral debido a que ambos permiten obtener una visión plural y poliédrica del objeto de estudio y su evolución histórica.

Teniendo en cuenta que el método comparativo "realiza una contrastación entre los principales elementos de la realidad que se investiga con las otras realidades similares ya conocidas[9]", éste se ha puesto en práctica a lo largo de la investigación para exponer las diferencias y las similitudes de los conflictos bélicos y las amenazas a lo largo de la historia.

---

[8] Calduch, R. (1988) Métodos y técnicas de investigación internacional. Madrid: Universidad Complutense de Madrid

[9] Idem

La combinación de estos tres métodos citados nos permite dar respuesta a las preguntas formuladas que se investigan y verificar las hipótesis de la investigación en relación con las nuevas amenazas en los conflictos bélicos actuales.

Las técnicas de investigación utilizadas en esta tesis son de carácter directo e indirecto. La investigación directa hace referencia a la realidad de los actuales conflictos bélicos que se presentan, por un lado, por las organizaciones terrorista y, por otro lado, por las informaciones referentes a los ataques utilizados por las nuevas tecnologías. Dentro de este marco se cumple un amplio abanico de formatos en los que se destacan las revistas, videos, audios, inforgrafias y programas informáticos. Conjuntamente a ello se tiene entrevistas con expertos en materia de ciberseguridad, concretamente con peritos informáticos.

La investigación indirecta se lleva a cabo a través de una revisión bibliográfica y de todo tipo de fuentes documentales. Se realiza una busca en Plataformas webs bibliográficas como: ISI Web of Science, Scopus, Web of Knowledge. ISI Current y ISI Essencial Science Indicators.

Conjuntamente se lleva a cabo una búsqueda en las bibliotecas nacionales, entre las que destacaremos los libros del Instituto español de Estudios Superiores, y de diferentes países destacando Estados Unidos, Republica dominicana, Líbano, Colombia y Egipto.

Las palabras claves más utilizadas son, en un primer lugar “Dáesh”, “terrorist magazine”, “go zones” y " lonely wolf. En segundo lugar y referente a la amenaza con el uso de las nuevas tecnologías, “Cyber”, “cyberattack”, “cyber threat”, “hybrid conflict” y “hybrid threat”.

El alcance de nuestra investigación será caracterizado como exploratorio, que conceptualizará el fenómeno y ayudará al lector a posicionarse ante el mismo, dados los objetivos de la tesis y la poca literatura al respecto. Acudiremos a fuentes de información que se caracterizan por ser de tipo no experimental pero que nos aportara conocimiento concreto del fenómeno de la inteligencia.

La inducción a partir de los fenómenos estudiados nos será de gran ayuda para responder a las preguntas e hipótesis planteadas. Para establecer relaciones e interrelaciones entre los datos analizados, las categorías y los conceptos

acudiremos al método trasversal para triangular los datos y acomodarlos al índice y objetivos propuestos.

El proceso de investigación comenzara con una exploración bibliográfica sobre los distintos acercamientos al objeto de la tesis para deslindar lo que consideraremos o no como "Guerra Híbrida".

Las principales técnicas empleadas para la recolección de información serán:

- Consulta de la literatura científica al efecto.
- Consulta de textos y publicaciones sobre estudios relativos a Seguridad y su gestión nacional e internacional.
- Análisis Jurídico en materia desarrollo democrático y buen gobierno.
- Dentro de las técnicas metodológicas que vamos a utilizar, destaca la observación documental a través de:
- Metaanálisis: búsqueda documental y tratamiento de datos.
- El análisis de contenidos: unidades de análisis, categorización, codificación y cuantificación.
- El análisis secundario: fuentes de datos, análisis e interpretación.

1.4 OBJETIVOS CIENTÍFICOS.

1. Estudiar empíricamente los procedimientos regulares e irregulares utilizados en los conflictos del Siglo XXI, los medios convencionales y no convencionales.

2. Analizar las nuevas amenazas híbridas en los conflictos del Siglo XXI.

3. Indagar acerca de la revolución tecnológica que influye en el conflicto bélico híbrido, llevando a cabo un profundo estudio de la ciberseguridad como forma de ataque las infraestructuras críticas y de primera necesidad como son la energía y el transporten.

4. Describir los sistemas financieros y su influencia dentro de los conflictos bélicos híbridos

5. Examinar las políticas de protección de la seguridad y la salud pública, mediante un análisis empírico de los planes de prevención tendentes a evitar la radicalización y los actos de extremismo violento.

6. Detallar los componentes y los factores que están implicados en este tipo de conflicto bélico, "las amenazas híbridas".

7. Establecer empíricamente la relación existente entre la Unión Europea y los estados miembros en materia de políticas criminales. Dicho estudio llevado a cabo todos los niveles, tanto dentro de la UE como los estados miembros y todas sus administraciones públicas u órganos de gobierno.

8. Explicar la influencia que llevan a cabo de los medios de comunicación en este tipo de conflictos.

9. Poner en claro los efectos que consigue Rusia cuando pone en marcha toda su maquinaria como amenazas híbridas con la intención de debilitar tanto la U.E. con otros puntos estratégicos.

10. Comparar la efectividad de los mecanismos específicos existentes para un intercambio real y rápido de la información entre todos los estados implicados y la mayor coordinación para llevar a cabo una mejor defensa y prevención ante las amenazas híbridas.

-DEFICINCIÓN Y CARACTERISTICAS DE LAS AMENAZAS HIBRIDAS-

II DEFINICION Y CARACTERISTICAS DE LAS AMENAZAS HIBRIDAS.

2.1 INTRODUCCIÓN: TIPOS DE GUERRA Y SU DEFINICIÓN.

Antes de investigar la evolución de la guerra y los conceptos de lucha, es necesario definir los tipos de guerra, para llegar a un enfoque puramente científico, basado en principios realistas, que nos permite sacar verdaderos resultados. La guerra se definió y discutió en muchos contextos, algunos de los cuales lo definieron como una expresión de la naturaleza del hombre, su entorno y las ideas sobre las que se originaron, pero otros, dijeron que reflejaba las relaciones entre los grupos humanos y podían caer entre las capas y facciones rivales de la sociedad y convertirse en un mecanismo para reequilibrar a toda la comunidad mundial.

Carl Von Clausewitz[10] definió la guerra como un "subconjunto de la teoría de un conflicto mayor". Lo definió como un "esgrima en una escala más amplia", "una obra de fuerza para forzar a nuestro enemigo ", "la continuación de la política por otros medios", y "la guerra es una lucha violenta de la voluntad". Sun Tzu[11] lo define como un "tema vital para el estado, boicoteando la vida o la muerte, la manera de sobrevivir o arruinar", y para evaluar sus fundamentos, se propone emprender un análisis de cinco factores clave: la influencia moral, el clima, el terreno, el liderazgo y la doctrina. Afirma además que "lo que es de suma importancia en la guerra es atacar la estrategia del enemigo".

---

[10] Carl von Clausewitz, general e historiador del ejército bruso, nació en 1780 en Magdeburgo, y murió en 1831 en Breslau, uno de sus escritos más importantes, "De la guerra", sus escritos sobre filosofía, táctica y estrategia tuvieron un profundo impacto en el campo militar en los países occidentales.

[11] Sun Tzu,general chino, experto militar y filósofo, nació en 551 A.C. y murió en 496 A.C., se hizo conocido debido a su famoso genio militar, escribió una serie de ensayos estratégicos militares, llevando el nombre del libro "Arte de la guerra".

La doctrina de las fuerzas armadas de los Estados Unidos "Joint Publication" definió el concepto de guerra como "una sucesión social de la violencia con fines políticos", y "podría resultar del fracaso de los Estados para resolver sus disputas por medios diplomáticos", y afirmó que la guerra clásica incluía históricamente nueve principios, conocidos como los principios de la guerra (que se explicará más adelante), y "la naturaleza fundamental de la guerra son inmutables, aunque la guerra está en constante evolución". El ejército estadounidense confía en dos formas básicas de guerra: convencionales e irregulares.

El concepto Marxista-Leninista distinguió en la definición de guerra y dijo: "la guerra es el producto del conflicto de estratos", pero la enciclopedia árabe mundial explicó el concepto de guerra, "la guerra es un conjunto de procesos sociales negativos, caracterizado por el violento conflicto destructivo. Es un conflicto donde se utiliza la fuerza armada usando grupos armados organizados llamados ejércitos regulares, o usando grupos paramilitares o milicias, y usando todos los medios para infligir daño al otro lado, tanto en sus capacidades militares como civiles obligándolo a retirarse sin alcanzar sus objetivos". Finalmente, la guerra se conoció como "operaciones militares entre enemigos, o una actividad de una unidad política para debilitar o destruir otra, o un conflicto entre enemigos rivales".

2.1.1 La Guerra convencional.

Esta forma de guerra es clasificada como un conflicto entre dos estados o dos partes conflictivas, y cada parte puede ser una coalición de varios estados nacionales. Este modelo se llama convencional porque es la forma prominente de la guerra, en la cual el estado nación solamente se reserva el derecho de monopolizar el uso legítimo de la fuerza, y el propósito estratégico de la guerra convencional es imponer la voluntad de un estado hostil en un estado nacional o prevenir la imposición de la voluntad de un estado agresor en otro estado. Esta es la forma de la mayoría de las guerras que se han producido a lo largo de la historia.

La guerra convencional es una guerra oficialmente proclamada, en la que los Estados nación luchan entre sí por múltiples razones que colectivamente representan sus intereses nacionales. Es una lucha violenta por la hegemonía

entre coaliciones de Estados-nación, y también incluyen actores no estatales, que utilizan capacidades y métodos militares convencionales al servicio de los mecanismos tradicionales de la victoria de la guerra, y estas guerras se caracterizan por la magnitud de las víctimas humanas resultantes.

La guerra convencional involucra operaciones militares basadas en el uso de la fuerza, en la que los adversarios utilizan una variedad de fuerzas convencionales y fuerzas de operaciones especiales que luchan entre sí en todas las áreas materiales, así como el entorno de información (que incluye el ciberespacio). Las tácticas de esta guerra se caracterizan por una serie de operaciones ofensivas, defensivas y de estabilización que se llevan a cabo contra los centros de gravedad del enemigo.

Clausewitz cree que la guerra se caracteriza por la interacción cambiante de tres potencias: la emoción (ilógica), la coincidencia (lógica) y la razón (racional), con las que se asocian actores principales clave, formados por tres fuerzas comunitarias, que son el pueblo, el ejército y el gobierno. Estas variables a menudo se combinan para causar una "niebla de guerra", y estas observaciones siguen siendo válidas hasta el día de hoy y colocan una carga sobre el líder para seguir adaptativo a crear y aprovechar oportunidades[12].

Las operaciones militares en la guerra convencional se centran generalmente en las fuerzas armadas del enemigo hasta poder influenciar su gobierno. Los mecanismos de la victoria en la guerra convencional incluyen la derrota de las fuerzas armadas enemigas, la destrucción de su capacidad, o el asimiento y la retención de la tierra. La guerra convencional asume generalmente que la población en el área de operaciones no es parte del conflicto, estará sujeta a cualquier resultado político que se impone o se negocia, y el objetivo primario sigue siendo la reducción de interferencia civil en operaciones militares para evitar sus efectos destructivos.

[12] Von Clausewitz, K. (1980): De la guerra, traducido por Akram Deere y Haitham al Ayoubi, Fundación árabe para los estudios y la publicación, Beirut, 312 páginas.

Los principios a destacar en este tipo de guerras convencionales son:

- El objetivo: Consistente en dirigir todas las operaciones militares hacía un objetivo claro, específico y alcanzable.

- El ataque: Conocido por el control, la propiedad y la toma de decisiones. Se considera como uno de los principios más importante de este tipo de guerra convencional proporcionando libertad de movimientos a nivel táctico.

- Unidad de Mando: Se trata de uno de los principios más importantes sobre lo que se basan los ejércitos regulares dada su estructura jerárquica, disciplina y organizativa típico de este tipo de guerras.

- Multitud y aglomeración: el principio va referido a la concentración de la capacidad de combate en un momento y lugar concreto. Es decir, en los niveles tácticos y operativos que generalmente son evitados por grupos armados irregulares. Se requiere una superioridad numérica y una gran potencia de fuego teniendo un alto coste tanto financiero como logístico.

- Maniobra. Se basa en la flexibilidad, velocidad de movimiento y fácil comunicación entre las tropas, y permite al liderazgo para hacer cumplir las condiciones de la batalla, aplicada por todos los ejércitos regulares

- Sorpresa. Es un multiplicador en las posibilidades de ganar la batalla y lograr el objetivo deseado golpeando al enemigo en un lugar o tiempo que no está esperando, y permitiendo el éxito por encima del nivel de esfuerzo. Sin embargo, el rápido progreso en la tecnología de reconocimiento, vigilancia y comunicaciones dificultó la ocultación de grandes capacidades de combate, por lo que no es necesario sorprender al enemigo por completo, sino retrasar su percepción de lo que está sucediendo, y su reacción vendrá ineficaz.

- Economía de fuerza. Consiste en la cantidad mínima de fuerza de combate se asigna para lograr los beneficios requeridos. Esto contradice la teoría de la proliferación expandida de fuerzas, causando confusión en el campo de batalla.

- Precaución. Se manifiesta al impedir que el enemigo adquiera la ventaja inesperada de las compensaciones y evitar que se invierta en debilidades o lagunas en la estructura de las fuerzas armadas o los ejércitos amistosos.

- Simplicidad. Manifestado a través de una planificación simple, fácil y sencilla, los órdenes claros y fáciles de entender, y la sencillez de los planes permiten una comprensión más profunda de los deberes y un mejor comando de las fuerzas.

Dentro de este tipo de guerra convencional encontramos el modelo conocido como guerra convencional desequilibrada,

El desarrollo tecnológico ha impactado significativamente en la forma de la guerra haciéndola más compleja, y ha llevado a la superioridad militar en los ejércitos de ciertos Estados, lo que ha impuesto una realidad del desequilibrio militar en su interés contra ejércitos regulares de otros Estados, que carecen de un arma cualitativa y tecnológica sofisticada, como resultado de su débil capacidad económica o el resultado de las restricciones internacionales impuestas a ellos, lo que los situó en una desventaja en el logro del equilibrio militar, recurriendo a tácticas no convencionales con la esperanza de la victoria.

El general británico Rupert Smith[13] describió la guerra desequilibrada como una "guerra convencional entre dos ejércitos, con una superioridad militar diferente entre sí". Mientras que en la guerra convencional cada equipo buscó superar las capacidades de la otra, utilizando armas superiores modernas, o aprovechando las debilidades del oponente y destruyendo sus fortalezas con el fin de destruirlo, buscó en la guerra desequilibrada controlar su voluntad y opciones. El curso de la guerra ha cambiado de "campo de batalla" a la guerra en medio de los pueblos[14].

La definición anterior de una guerra convencional desequilibrada muestra su realidad tradicional y su respeto por los principios de la guerra convencional. El escenario de guerra suele ser un comienzo recurrente de las operaciones de combate, bombardeo aéreo, artillería y cohetes, confrontación real con unidades de infantería entrenadas y unidades blindadas, compuestas de números y

[13] Rupert Anthony Smith, nacido en 1943, oficial retirado del ejército británico y autor de "La utilidad del poder y el arte de la guerra en el mundo contemporáneo".

[14] Shakhtourra, R. (2014): "Guerra asimétrica: El arma más débil también puede ser utilizado por el poderoso", pp. 6-12.

formaciones regulares, apoyados por líneas de suministro y apoyo logístico como telón de fondo, enfrentándose a sus contrapartes de las fuerzas opuestas. También son apoyados por la artillería necesaria y el fuego de la aviación, con la diferencia de que el equilibrio militar entre estos ejércitos regulares opuestos es diferente, y por lo tanto los principios de esta guerra no son diferentes de los de la guerra convencional, pero corresponden exactamente a ellos.

La guerra desequilibrada depende de la tecnología, como bloquear las redes, y el acceso a Internet para detener el sistema informático militar, y utilizar esta red para comunicar y transferir fondos.

Los sistemas tecnológicos, a pesar de sus características positivas, tienen la desventaja de ser técnicamente susceptibles de manipulación y de perjudicar sus capacidades atacando infraestructuras vitales a través de Internet.

Igor Koruchenko[15], miembro del Consejo Social del Ministerio de Defensa de Rusia, considera que el ejército georgiano es "una fuerza significativa", porque sus miembros fueron entrenados por consultores occidentales y equipados más allá del equipamiento del ejército ruso, con respecto a los prismáticos de visión nocturna y el material individual. Sin embargo, a pesar del apoyo de Ucrania a Georgia con armas, el ejército ruso permaneció militarmente superior y mantuvo un control aéreo casi absoluto en el campo de batalla[16].

2.1.2 La Guerra Asimétrica.

Es una guerra entre dos partes o más de un conflicto, con capacidades militares muy variables entre cada uno de ellos, y uno al menos de ellos debe ser un actor no estatal. Los pensadores militares lo amplían para incluir la disparidad en la planificación y la estrategia, en este tipo de conflicto se mezcla la estrategia y la táctica de la guerra no convencional y la guerra de guerrillas, el equipo débil "ostensiblemente" trata de superar la superioridad cuantitativa y cualitativa del

[15] Igor Koruchenko, experto militar y miembro del Consejo Social del Ministerio de defensa de Rusia, redactor jefe de la revista de defensa nacional de Rusia.

[16] Zaid Al-Marhoun, A. (2008): "La guerra desequilibrada del Cáucaso", Al Riyadh, La Fundación Al Yamamah, (14662), pp. 48-56.

oponente, y a menudo hace que las ventajas de sus fuerzas se vuelven negativamente sobre él.

Este tipo de guerra asimétrica se produce entre un ejército regular y grupos no gubernamentales, no sólo apuntando y destruyendo instalaciones militares y combatientes, como en la guerra convencional, sino que abarca una amplia gama de objetivos políticos, económicos y sociales. Estos ataques son más frecuentes, creativos y dañinos a medida que se dirigen a las vulnerabilidades del oponente, el objetivo está el poder político y la población, mientras que la guerra convencional está dirigida al ejército y a la autoridad gobernante.

La guerra asimétrica es la guerra librada por la parte más débil para lograr un objetivo político que se puede lograr sólo causando muchas bajas a la parte más fuerte, e informando a la comunidad internacional que la situación es caliente y no puede ser olvidada, pero utiliza métodos asimétricos de lucha para cubrir la diferencia de fuerza y para evitar que la poderosa parte gane la guerra.

El Dr. David Buffalo definió la guerra asimétrica como una "guerra no tradicional centrada en la población que se libró entre una fuerza superior militar y uno o más de los poderes inferiores que incluye la evaluación y la derrota de la amenaza asimétrica, la realización de operaciones asimétricas, y la comprensión de la disparidad cultural y la evaluación asimétrica de costos"(Buffalo, 2006), el objetivo estratégico de la guerra asimétrica es ganar la voluntad de los civiles y la voluntad de sus líderes (Al-Asali, 2009), mientras que la guerra asimétrica se caracteriza por una de sus partes no estatales (Dixit, 2010).[17]

El término también se utiliza con frecuencia para describir lo que también se llama "guerra de guerrillas", "insurgencia", "contrainsurgencia", "rebelión", "terrorismo", y "contraterrorismo", conflicto esencialmente violento entre un militar formal y un informal, menos equipado y apoyado, poco tripulado pero resistente y motivado oponente.

[17] Anexo A: Comparison between traditional and asymmetric warfare.

Apareció en las enseñanzas de Sun Tzu: "Todas las guerras son asimétricas porque uno explota los puntos fuertes del enemigo mientras ataca sus debilidades". La guerra asimétrica se definió según Antonio Echevarría[18] como "esas guerras que dependen del tipo de rebelión en lo que las fuerzas utilizan todos los medios tecnológicos, políticos, económicos y sociales para obligar al enemigo, que es una fuerza regular, a abandonar su política y sus objetivos estratégicos".

Principios de la guerra asimétrica

La guerra asimétrica se ha convertido en una estrategia de elección para disidentes y grupos políticos extremistas, y probablemente representará la mayor amenaza para la seguridad nacional e internacional en el siglo XXI (Long, 2008), ya que no se basa en los principios de la guerra convencional que hemos mencionado anteriormente, algunos de estos principios fueron adoptados y otros fueron inventados. Estos principios giran en torno a varias características que ilustran las cualidades que caracterizan a estas guerras:

- Flexibilidad: La flexibilidad de las operaciones de combate es a todos los niveles, lo que significa la flexibilidad de los frentes, la flexibilidad del despliegue, la flexibilidad de los planes cambiantes, la flexibilidad del liderazgo y la capacidad de adaptarse rápidamente para combatir los métodos de los oponentes, y encontrar contramedidas inmediatas y efectivas.

- Conocimiento del terreno y su naturaleza. Proporciona un control de campo natural de las fuerzas que existen en una ubicación geográfica particular, independientemente de su afiliación y tipo.

- Unidad de esfuerzo: Empleo de todas las energías y capacidades disponibles en el momento y lugar adecuados para alcanzar el objetivo deseado y explotar las vulnerabilidades del enemigo, en términos de emboscadas, allanamiento, francotiradores y uso de armas según su calidad, invirtiendo los poderes y medios mínimos.

[18] Echevarría, A. (2005): Cuarta generación de la guerra y otras leyendas, pág. 34

- Evitación del acoplamiento directo. Evita el choque directo con el enemigo, para privarlo del uso de su potencia de fuego superior, para elegir los lugares y los tiempos correctos, para confrontarlo, y para atacarlo en sus peores casos además de aprovecharse de la naturaleza de la tierra en todos los casos .

- Adopción del concepto de espacio de guerra abierta. La guerra asimétrica se basa en el concepto de "sin planes, sin trincheras, sin líneas, sin fortificaciones y sin multitudes", golpeando al luchador donde quiera, la hora que quiera, y los medios para lograr el objetivo deseado. Esta realidad contradice las artes marciales adoptadas por los ejércitos y Estados regulares.

- Práctica de la guerra de los medios por todos los medios. Los medios de comunicación desempeñan un papel importante en la guerra, con la alta moral que proporciona a los vencedores, o en el que atrae el apoyo moral internacional o interno. En la guerra asimétrica, se basa en todos los medios antiguos, primitivos y modernos, para lograr varios objetivos, incluyendo difundir el terror, crear confusión y socavar la moral pública, ganando apoyo popular para sus posiciones, influyendo en la opinión pública apoyando al oponente, distrayendo Sus posiciones, creando opiniones contra la decisión política o militar.

- Proporción del entorno envolvedor de la población. La base de este principio es la necesidad de apoyo popular por parte de los grupos armados para compensar la superioridad material, que, además de la posibilidad de la infiltración y el oculto dentro de la población local, permite la obtención de los suministros necesarios para continuar .

- Práctica de la guerra de los medios por todos los medios. Los medios de comunicación desempeñan un papel importante en la guerra, con la alta moral que proporciona a los vencedores, o en el que atrae el apoyo moral internacional o interno. En la guerra asimétrica, se basa en todos los medios antiguos, primitivos y modernos, para lograr varios objetivos, incluyendo difundir el terror, crear confusión y socavar la moral pública, ganando apoyo popular para sus posiciones, influyendo en la opinión pública apoyando al oponente, distrayendo Sus posiciones, creando opiniones contra la decisión política o militar.

• Adopción de una guerra psicológica. El objetivo de la guerra psicológica es difundir el terror y la intimidación psicológica temprana en las almas de los pueblos, extendiendo algunas ideas, opiniones o creencias, para debilitar la capacidad de combate del oponente, para reducir su moral, para cuestionar la equidad de su caso, y a cambio de elevar el estado moral del partido librando la guerra psicológica. El objetivo principal de este proceso es persuadir al adversario de que no tiene sentido continuar la guerra.

• Utilización de comunicaciones multimedia modernas y antiguas. Los medios de comunicación, especialmente los antiguos con cables desempeñan un papel importante y eficaz en el suministro de una comunicación segura a los grupos armados, ya que es difícil ponerlos bajo vigilancia o el jamming.

• Utilización del bombardeo y del secuestro. El bombardeo se considera uno de los métodos más importantes y efectivos en los países democráticos, por lo que la opinión popular tiene influencia en las decisiones de la autoridad política y militar, y el bombardeo tiene como objetivo confundir y distraer al oponente. Por otro lado, el secuestro es también importante y entonces la negociación para los detenidos y los secuestrados.

Objetivos y ventajas de la guerra asimétrica.

La guerra asimétrica no está destinada a destruir la institución militar ni a eliminar la capacidad del Estado, sino que está destinada a agotar el poder del Estado hostil y la erosión lenta en su voluntad para obligarlo a llevar a cabo lo que la fuerza que utiliza este tipo de guerra quiere. También pretende frustrar el Estado en que una parte del territorio de ese estado está fuera de su control, facilitando así el control de los grupos terroristas en esta área, utilizándola para lanzar operaciones terroristas para atacar instalaciones económicas, líneas de transporte e instituciones vitales y debilitar el poder del Estado.

Puesto que la situación de seguridad en un país tiene una influencia directa en la capacidad del Estado para obtener préstamos, lo que da a estas guerras diferentes formas de influir en la posición del Estado, y un acto preliminar es suficiente para influir en la situación financiera del Estado objetivo y alentarlo a negociar, y el objetivo es crear una situación de parálisis en el proceso político del Estado objetivo. Las organizaciones que utilizan tales guerras pretenden lograr un éxito político y no militar, y centrarse en cambiar las mentes, opiniones y políticas

de los tomadores de decisiones en la dirección que deseen, a través de la presión psicológica y de los medios de comunicación o a través de organizaciones internacionales.

La guerra asimétrica se caracteriza por una serie de características y cualidades que lo distinguen de la guerra convencional o sistémica, tanto en términos de objetivos, medios y herramientas, como en términos de teatro de operaciones y período de tiempo. Sun Tzu describió las técnicas básicas de los enfoques indirectos a seguir y dio su consejo en la escritura de "El Arte De La Guerra", el más importante de los cuales es "evitar la fuerza y atacar la debilidad en el oponente"[19]

Los adversarios menos poderosos en la guerra asimétrica favorecen el uso de métodos desiguales y evitan la confrontación directa con fuerzas militares superiores atacando objetivos no militares para influir o controlar a la población local, sin perder de vista los métodos diplomáticos, informativos y económicos.

Lawrence de Arabia[20] fue uno de los pensadores militares que trataron en la escritura de los "7 Pilares De La Sabiduría" el concepto de la guerra asimétrica, sugiriendo que la ventaja militar estricta puede no ser la forma más rápida de la victoria, y muestra que la lucha en un entorno asimétrico entra en vigor los objetivos de largo plazo, y así se realiza un progreso intangible, resultante de la forma en que se combate la guerra, que supera el progreso militar tradicional de la campaña.

En 1999, dos oficiales de la República Popular de China, los coroneles Qiao Liang y Wang Xiangsui[21] escribieron un libro titulado "La Guerra Sin Restricciones: El Principal Plan De China Para Destruir América", afirmando que "el terrorismo es sólo uno de los muchos instrumentos en manos de algunos Estados y sus aliados terroristas para librar una guerra total contra los Estados Unidos". Han anticipado eventos similares a los que ocurrieron dos años más

[19] Tzu, S. (2004): Arte de la Guerra, siglo VI

[20] Thomas Edward Lawrence, el famoso Lawrence de Arabia (1888 – 1935), pág. 44

[21] Liang Q. y W. Xiangsui (1999): Guerra sin restricciones: plan maestro de China para destruir América, pág. 4

tarde en 11 de septiembre, este libro causó pánico en la comunidad de defensa e inteligencia en los Estados Unidos, y condujo a la atención a muchos conceptos que no fueron tomados previamente en cuenta en el campo de la guerra, y cambiar el pensamiento hasta el punto de imaginar cada acto de poder nacional como un acto de guerra.

Los ataques del 11 de septiembre han cambiado muchos conceptos y han mostrado a Occidente que su nuevo enemigo no respeta ninguna regla o frontera nacional, y aunque no posee tecnología avanzada, ha logrado causar destrucción y pérdidas a los estadounidenses en el suelo de Estados Unidos. Estos ataques también han demostrado que el ejército ya no puede garantizar la protección total y servir como una barrera entre el enemigo y su gobierno o población. Este trauma psicológico provocó gran parte del debate que ya se reflejaba en el concepto de percepciones asimétricas de estrategia y tácticas de guerra.

Desde el punto de vista de los posibles atributos de este tipo de guerra, esta se caracteriza por la existencia de grupos e individuos que no están directamente asociados con el Estado y que operan dentro del Estado hostil objetivo y son difíciles de detectar, dispersos en todo el territorio del Estado hostil. La guerra asimétrica se lleva a cabo dentro de un rango amplio y no limitado en área geográfica, en contraste con las guerras tradicionales en las que el teatro de operaciones es conocido y definido para las dos partes, que son ejércitos regulares.

El uso de medios tecnológicos, intelectuales y económicos en la guerra asimétrica es utilizado por la parte más débil para resolver la guerra a su favor, en contraste con la guerra convencional en la que se utilizan las armas convencionales y de manera directa.

La guerra asimétrica toma largos periodos de tiempo debido a su dependencia de las tácticas de las guerras de guerrillas, mientras que la guerra convencional o sistémica no toma un período abierto, pero sus resultados a menudo se resuelven rápidamente o dentro de un cierto período de tiempo, que van desde corto a mediano. La guerra asimétrica por lo general persiste durante décadas porque se articula al factor de desgaste a largo plazo, el ejemplo más prominente es la guerra internacional contra el terrorismo liderada por los

Estados Unidos, ya que este último se niega a determinar el tiempo necesario para la guerra y dice que esta guerra está abierta e infinita[22].

Las características sociales de la guerra asimétrica son el deterioro de la idea estatal y el creciente estado de lealtad a ciertas culturas en el mundo, que socava la homogeneidad de la sociedad, termina el monopolio estatal de la guerra y explota la responsabilidad política de los Estados hacia sus ciudadanos para desarrollar estrategias que les obligan a adoptar cierto comportamiento político, que la cae en el tabú, y fomentan la aparición de entidades no estatales como tribus o grupos étnicos, religiosos o confesionales.

La globalización ha desempeñado un papel importante en la influencia de estas guerras al ayudar a difundir grupos terroristas a gran escala y utilizar métodos no tradicionales para enfrentar la paz y la seguridad internacionales, y se ha beneficiado del uso de los instrumentos que han resultado de la globalización, especialmente en el área de progreso de tecnología, y se basó en la provisión de redes de Internet para facilitar la comunicación entre ellos. También utilizan varios medios de comunicación para promover sus ideas y para lanzar la guerra psicológica contra las personas en áreas específicas como la publicación de vídeos en youtube, sitios de redes sociales o un sitio web para grupos terroristas en Internet[23]

Contradicciones entre la lucha convencional y la lucha asimétrica.

Los grandes ejércitos, que fueron superiores en el campo de batalla en anteriores guerras convencionales, han llegado a una necesidad urgente de desarrollar los conceptos de lucha, para poder enfrentar los grupos pequeños, organizados o no organizados, que utilicen métodos de lucha "asimétricos" que contradigan la manera en que se llevaron a cabo con los principios y conceptos establecidos de la guerra convencional, para los que estos ejércitos fueron

[22] Metz, S. y D. Johnson. II (2014): Asymmetry and U.S. Military Strategy: Definition, background and strategic concepts, Instituto de Estudios Estratégicos del ejército de EE. UU.

[23] Smith, R. (2008): La utilidad del poder y el arte de la guerra en el mundo contemporáneo, Casa Árabe de las Ciencias, Beirut

fundados y entrenados para respetarlos y adoptarlos en el transcurso de sus implementación de todas las operaciones de combate.

Desde el punto de vista de metas y objetivos, El objetivo principal de las partes en la guerra, en la lucha convencional, es el éxito militar y la destrucción de la voluntad del enemigo, pero el logro de este objetivo en la guerra asimétrica parece ser una tarea muy difícil, porque el lado débil no puede lograr la victoria militar debido a su falta de factores de fuerza, y su objetivo sería esencialmente el éxito político, la victoria de la voluntad de los civiles y la voluntad de sus líderes, y no el éxito militar. Intenta prolongar la guerra para drenar al enemigo y obligarlo a reconocer sus derechos políticos, pero la parte fuerte, y a pesar de tener los elementos del poder que la califica para lograr la victoria militar, pero es incapaz de explotar esta superioridad y emplearla en su ventaja, porque el enemigo consiste en pequeñas células distribuidas en lugares desconocidos, donde no pueden ser golpeadas y destruidas definitivamente en una sola operación militar.

En referencia a los medios y herramientas empleadas, En la guerra convencional, los beligerantes recurren a medios y herramientas bien conocidos como artillería, cohetes y aviones de combate de todo tipo, con grandes unidades militares estacionadas en puntos y lugares específicos. En la guerra asimétrica, los medios, métodos, herramientas y tácticas usadas son numerosas y están cambiando constantemente de un ataque a otro. En la guerra convencional, el campo de batalla y los sitios de confrontación eran conocidos, dentro de marcos específicos y áreas geográficos definidos. Sin embargo, la situación es diferente en la guerra asimétrica, donde no hay terreno en lo que los beligerantes se encuentren, pero el teatro de operaciones es abierto y no específico a un área geográfico en particular. En algunos casos, como las confrontaciones entre Al-Qaeda, Estados Unidos y los países occidentales, puede extenderse a todas las regiones del mundo, y los teatros de operación se han ampliado para llegar a los civiles.

2.1.3 La Guerra Hibrida.

Para finalizar con el capítulo, haremos referencia a la Guerra híbrida, siendo este el principal tema de mi investigación y trabajo doctoral.

La guerra híbrida es una mezcla de guerra convencional y guerra asimétrica, caracterizada por el uso de la tecnología moderna, que no está sujeta a reglas constantes desde el mando a las operaciones militares, y tiene como objetivo destruir el poder del enemigo y neutralizar sus capacidades, e infligir las mayores pérdidas. La guerra híbrida contraviene totalmente las reglas conocidas en las guerras, es una estrategia militar que combina las guerras convencionales y asimétricas con la ciberguerra, con otros métodos influyentes como las fakenews y la diplomacia, y que combina operaciones cinéticas con esfuerzos de subversión.

La naturaleza de los conflictos de hoy ha asumido formas más complejas que en el pasado como resultado de las revoluciones tecnológicas e informativas que crearon nuevos medios y áreas de confrontación que no estaban previamente disponibles. Internet y los teléfonos móviles han proporcionado medios de comunicación potentes a nivel local e internacional, El desarrollo de la química también ha conducido a la aparición de varios tipos de explosivos que se preparan fácilmente localmente, además de las armas avanzadas y efectivas proporcionadas por el mercado negro, lo que conduce a la aparición de una nueva generación luchando en formas tradicionales y no convencionales que los integra, una forma sofisticada de la guerra, usando sus tácticas y, al mismo tiempo, usando armamento sofisticado, los estudios americanos la definen como guerra híbrida[24].

Los combates híbridos no siguen los principios tradicionales de combate que forman la base intelectual de la mayoría de los ejércitos del mundo, una forma diferente de lucha, una mezcla de la brutalidad de la guerra convencional librada por los ejércitos regulares con el fundamentalismo de guerra asimétrico adoptado por los grupos armados. Los grupos organizados, entrenados y bien

[24] Kahwagi, R. (2016): "Guerra híbrida: la evolución de las tácticas guerrilleras y la guerra revolucionaria en la era de la digitalis".

armados, con una capacidad de afrontamiento directa, y golpeando la profundidad del enemigo con cohetes, naves, aeronaves, capacidades de vigilancia aérea o guerra cibernética, no se clasifican sus tácticas de combate como "asimétricos", pero se clasifican como híbridos.

Varias guerras fueron clasificadas como "híbridas" según los análisis y estudios norteamericanos de la guerra moderna, guerras que evolucionaron de "asimétrica" a "híbrida", incluyendo la guerra de Afganistán, la guerra de Somalia, la guerra de Sudán, la guerra de Palestina en Gaza, la guerra de Libia, la guerra de Siria, y la guerra libanesa (experiencia de resistencia en agresión julio 2006). Hezbolá libanés es uno de los ejemplos más exitosos, que aplicó con éxito la guerra híbrida en la guerra de julio de 2006[25], donde sus combatientes adoptaron tácticas guerrilleras, usando cohetes anti blindaje y naves con un éxito impresionante, y sus cohetes fueron capaces de amenazar la retaguardia del enemigo, y sus herramientas y los medios de comunicación tuvieron éxito y han podido lograr una victoria moral sobre el enemigo israelí, penetrar en su aparato de comunicaciones, espiar a su movimiento, y evitar que penetre en sus filas, lo que causó que el ejército del enemigo israelí fue en un estado de gran pérdida y lo que condujo a su derrota en el suelo.

[25] Kahwagi, R. (2016): "Guerra híbrida: la evolución de las tácticas guerrilleras y la guerra revolucionaria en la era de la digitalis".

-APROXIMACION AL CONCEPTO DE AMENAZAS HIBRIDAS-

III APROXIMACION AL CONCEPTO DE AMENZAS HIBRIDAS.

3.1 PERSPECTIVAS DESDE OTAN, UE Y PESCO.

Después de la Cumbre de OTAN en Gales en septiembre de 2004,[26] la organización del Atlántico Norte expresó la necesidad de luchar contra las «amenazas de guerra híbrida» y las «amenazas híbridas» con herramientas y procedimientos nuevos y necesarios para disuadir y responder eficazmente a estas amenazas, así como las capacidades para garantizar las fuerzas de cada nación (Hoffman, Frank G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars) . Sin embargo, entre los miembros de la OTAN, no existe una definición acordada de términos relacionados con la guerra híbrida y, por lo tanto, es difícil tener una estrategia militar específica.[27]

Sin embargo, el analista del Centro para la Nueva Seguridad Estadounidense y miembro del Instituto Kennan del Wilson Center Michael Kofman, cree que «Occidente se ha estado aterrorizando a sí mismo con espectros de guerra híbrida hasta el punto de calificar como una de las mejores operaciones de desinformación de la historia, incluso si fue completamente involuntario. El problema es más pronunciado para los aliados europeos que están experimentando una versión moderna del "susto rojo" de los Estados Unidos desde la década de 1940 y 50. Algún día, podemos mirar hacia atrás en esta ocasión en Europa y llamarlo el "susto" de la guerra híbrida. La influencia y la subversión rusas son reales en gran parte de Europa, pero los temores de esta mística guerra híbrida han llevado a los funcionarios europeos a ver a los agentes del Kre- mlin detrás de cada esquina.

En la misma línea, Chris Tuck, (Hybrid War: The Perfect enemy, 2017), recuerda que «intelectualmente, el concepto de guerra híbrida dice más sobre nuestros temores que sobre cualquier modelo de guerra genuinamente nuevo. Esto no quiere decir que el entorno de seguridad actual no sea difícil y peligroso.

---

[26] Wales Summit Declaration, Press Release, (2014), p. 13 – 104.

[27] Hoffman, Frank G, (2010), « "Hybrid threats": Neither Omnipotent Nor Unbeatable, volumen 4 p 441-445.

Sin embargo, si dejamos de conectar todas nuestras dificultades, multiplicándolas por la suposición de adversarios superiores y luego etiquetándolas como guerra híbrida, podríamos encontrar que estos desafíos son más fáciles de abordar.

En este sentido, nos hacemos cargo que la «amenaza» híbrida no es un espectro, sino un hecho real. En este contexto, por ejemplo, Rusia ha violado el espacio aéreo aliado y continúa con su prueba de misiles y las fuerzas nucleares de rango intermedio o redes neutralizadas como parte de los ataques híbridos Occidente, diseñados para lograr cualquier cantidad de objetivos a través de acciones hibridas. En respuesta, la estrategia occidental sigue siendo en su mayoría opaca, o al menos no explícita, pero incluyen dinámicas y factores internos y políticos.

Según John R. Deni[28], la guerra debe considerarse como siempre: un conjunto complejo de amenazas interconectadas y medios contundentes impulsados por motivos políticos adicionales. La guerra híbrida tiene una gran cantidad de capacidades que confieren a la brutalidad, desorden de seguridad y ataques terroristas. Esta nueva cara de la guerra podría ser intemporal sin límites ya que puede utilizar tácticas irregulares y convencionales, ciberataques que rompen la ciberseguridad, procedimientos criminales y terroristas, crimen organizado, operaciones encubiertas, disputas marítimas, satélites, control de los recursos energéticos y así, una amalgama multiforme de espectro impredecible[29].

Esta «nueva forma» de hacer la guerra se puede hacer dentro de una estructura perfecta con unidades dispersas equipadas con IED, UAV, misiles y municiones de última generación, alta tecnología como guerra cibernética contra

---

[28] Profesor de Estudios de Seguridad y director asociado de Investigación en el Instituto de Estudios de Seguridad Nacional de la Universidad de Texas. Profesor adjunto de la Escuela de Servicio Internacional de la Universidad Estadounidense, el Instituto de Estudios Estratégicos del US Army War College. desarrollando estrategias basadas en desafíos «híbridos»,

[29] Deni, John. R.: «More of the Same in Response to Russia?», Carnegie Europe, Judy Dempsey's Strategic Europe, 23 november 2017. http://carnegieeurope.eu/ strategiceurope/74811¨ [consultado 24 febrero 2018]

infraestructuras clave, capaces de combinar todo tipo de capacidades – convencionales o no, para perseguir la interrupción y el desorden de su oponente. Esta guerra es irregular y difícil de enfrentar, no por sus capacidades sino por la filosofía de la respuesta convencional.

Las operaciones asimétricas, híbridas y de contrainsurgencia enmarcarán los futuros conflictos armados cambiando los paradigmas reales de las formas de hacer la guerra. La Alianza del Atlántico Norte y la Unión Europea tienen una oportunidad para disuadir la guerra híbrida y la única forma de tener éxito en este propósito es trabajando juntos. La OTAN y la Unión Europea deben estar preparadas para la «nueva generación de guerras» con armas especiales, hardware apropiado, recursos suficientes y atuendo específico de combate. Por el contrario, la OTAN y la UE pueden fracasar y perder la oportunidad de detener las amenazas no convencionales, las guerrillas, los terroristas y los mercenarios criminales. Por lo tanto, es un buen momento para que la OTAN y la UE cooperen como hermanos de armas. En palabras del Secretario General de la OTAN Jens Stoltenberg: «Rusia ha utilizado soldados sustitutos, Fuerzas especiales no marcadas, intimidación y propaganda, todo para crear una espesa niebla de confusión; para ocultar su verdadero propósito en Ucrania; e intentar la negación. Por lo tanto, la OTAN debe estar preparada para tratar cada aspecto de esta nueva realidad desde cualquier lugar. Y eso significa que debemos mirar de cerca cómo nos preparamos; desalentar; y si es necesario, defendernos contra la guerra híbrida»[30].

«Uno de los grandes pasos ya dados es la Estrategia Global de la UE para Política Exterior y de Seguridad (EUGS) que inició un proceso de

«Cooperación más estrecha en seguridad y defensa». Los Estados miembros acordaron intensificar el trabajo de la Unión Europea en este ámbito y reconocieron que se debe mejorar la coordinación, aumentar la inversión en

[30] NATO (2015) keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar, Washington, DC. https://www.nato.int/cps/en/natohq/opinions_118435.htm?selectedLocale=en [consultado 2 Marzo 2018]

defensa y la cooperación en el desarrollo de capacidades de defensa. Estos son parte de los requisitos clave para lograr. Este es el objetivo principal de una Cooperación estructurada permanente en materia de seguridad y defensa (PESCO), tal como se establece en el Tratado de la UE, los artículos 42 y 46, así como el Protocolo 10. A través del PESCO, los Estados miembros aumentan su eficacia en abordar los desafíos de seguridad y avanzar hacia una mayor integración y fortalecimiento de la cooperación en defensa dentro del marco de la UE»[31].

3.1.1 Toma de decisiones.

Es esencial que la Alianza posea las herramientas y los procedimientos necesarios para disuadir y responder eficazmente a las amenazas de guerra híbrida y las capacidades para reforzar las fuerzas nacionales. Esto también incluirá la mejora de las comunicaciones estratégicas, el desarrollo de la OTAN y otras organizaciones, en línea con las decisiones pertinentes tomadas, con miras a mejorar el intercambio de información, las consultas políticas y la coordinación entre el personal[32]. En este sentido el establecimiento del Centro de Excelencia de Comunicaciones Estratégicas acreditado por la OTAN en Letonia como una contribución significativa a los esfuerzos de la OTAN en esta área[33].

En la ceremonia de apertura de la cumbre de la OTAN, el Secretario de Estado del Ministerio de Relaciones Exteriores de Letonia Andrejs Pildego- vičs dijo: «[…] Debemos ser capaces de responder a los desafíos emergentes. Uno de

---

[31] Permanent Structured Cooperation, PESCO, (2017) «Deeping Defense Cooperation among UE Members States», European External Action Service. 2017 https://eeas.europa.eu/sites/eeas/files/pesco_factsheet_14-11-2017.pdf [consultado 25 marzo 2018]

[32] NATO, Wales Summit Declaration, op. cit. 13th point. https://www.nato.int/cps/en/natohq/official_texts_112964.htm [consultado 25 marzo 2018]

[33] Hunter, Eve y Pernik, Piret (2015): The challenges of Hybrid Warfare, Tallinn, Estonia, International Centre for Defense and Security (ICDS), pág. 3. https://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf [consultado 25 marzo 2018]

esos desafíos es el espacio de información y la comunicación, que adquieren una importancia cada vez mayor en cualquier situación de crisis. Al unir sus esfuerzos, los miembros de la OTAN tienen un gran potencial para desarrollar el sector, y Letonia está decidida a contribuir considerablemente para lograr ese objetivo[34]». Esta fue una declaración crucial de advertencia para todos los miembros de la OTAN para fortalecer el vínculo entre Europa y América del Norte y enfrentar los desafíos del siglo XXI. Después de la reunión del Consejo del Atlántico Norte en Varsovia (julio de 2016), los jefes de Estado y de Gobierno acordaron adaptar la postura defensiva y de disuasión para responder a las amenazas y desafíos, aumentar la inversión en capacidades y el desarrollo de fuerzas altamente aptas y desplegables.

El Compromiso de inversión en defensa acordado en la Cumbre de Gales (septiembre de 2014) fue un paso importante en esta dirección y el Jefe de Estado y Gobierno de la OTAN reafirmó su importancia. En la cumbre de la OTAN en Varsovia, los miembros recordaron de acuerdo con el Paquete de medidas para la implementación de los acuerdos de Minsk el 15 de febrero de 2015[35].

Según diferentes fuentes, la estrategia adoptada y los planes de implementación accionables de la OTAN en la lucha contra la guerra híbrida no fueron lo suficientemente efectivos, aunque la OTAN está preparada para ayudar a un aliado en cualquier etapa de una campaña híbrida y como parte de la defensa colectiva incluida cuando el Consejo invoca el Artículo 5 del Tratado de Washington[36], donde la Alianza está comprometida en la cooperación y coordinación efectiva entre sus socios y las organizaciones internacionales

---

[34] Latvia Ministry of Foreign Affairs (2014): NATO Center of Excellence for Strategic Communication in Latvia. http://www.latvia.lv/news/nato-centre-excellence- strategic-communication-latvia [consultado 27 marzo 2018]

[35] NATO, Joint statement of the NATO (2016)-Ukraine Commission at the level of Heads of State and Government https://www.nato.int/cps/en/natohq/ ofçficial_texts_133173.htm?selectedLocale=en[consultado 27 marzo 2018]

[36] NATO, (1949): The North Atlantic Treaty, Article V. https://www.nato.int/cps/en/ natohq/official_texts_17120.htm[consultado 27 marzo 2018]

relevantes, en particular la UE, según lo acordado, en los esfuerzos para contrarrestar guerra híbrida. Los deseos e intenciones son claros, así como el mensaje de que el trabajo debe hacerse como un agujero dentro de la Alianza. La OTAN tiene el desafío de lidiar con los nuevos procedimientos para defender a sus miembros de ataques no convencionales que cambian el patrón de Estado contra Estado.

El Artículo 5 del Tratado del Atlántico Norte dice:

«Las Partes acuerdan que un ataque armado contra uno o más de entre sus miembros en Europa o América del Norte se considerará un ataque contra todos ellos y, en consecuencia, acuerdan que, si se produce un ataque armado, cada uno de ellos, en ejercicio del derecho de legítima defensa individual o colectiva reconocido en el Artículo 51 de la Carta de las Naciones Unidas, asistirá a la Parte o Partes atacadas tomando inmediatamente, individualmente y en concierto con las demás Partes, las medidas que considere necesarias, incluido el uso de la fuerza armada, para restablecer y mantener la seguridad del área del Atlántico Norte. Todo ataque armado de ese tipo y todas las medidas que se tomen como consecuencia de este deberán ser informados al Consejo de Seguridad. Tales medidas terminarán cuando el Consejo de Seguridad haya tomado las medidas necesarias para restablecer y mantener la paz y la seguridad internacionales».

En este sentido, cuando la Alianza invocó el principio del Artículo V del Tratado de Washington el 12 de septiembre, esta declaró que necesitaba saber si tales acciones se habían llevado a cabo desde el exterior antes de que el Artículo pudiera entrar en pleno funcionamiento. Algunos analistas piensan que el Artículo V de la OTAN necesitaba ser revisado. La ambigüedad del Artículo V de la OTAN concerniente a las operaciones en Afganistán dejó atrás el deseo de los Estados Unidos de dar una respuesta contundente al terrorismo. Sin embargo, las cosas sucedieron de manera diferente.

En ese momento, el Secretario General de la OTAN Lord George Robertson explicó que «era prematuro especular sobre qué acción militar tomaría la Alianza, ya fuere individual o colectiva».

La decisión de la OTAN hizo que Estados Unidos diera una respuesta unilateral al régimen talibán en Afganistán, enviando operaciones expedicionarias de fuerzas especiales de manera fácil y rápida para ser

desplegadas y sin necesidad de una estructura militar tradicional. El presidente de Estados Unidos, George W. Bush, y el Jefe de Defensa estaban listos para comenzar una guerra asimétrica con herramientas híbridas contra todas las posibles amenazas.

La respuesta a una nueva generación sobre el combate híbrido de los Estados Unidos fue una campaña de siete semanas para derrocar a los talibanes en Afganistán. Después del final de esa campaña contra los talibanes, Donald Rumsfeld, el Secretario de Defensa y el presidente George W. Bush, participaron en una campaña transformadora que básicamente cambió las reglas de guerra enfocadas en el uso de Fuerzas de Operaciones Especia- les (SOF) pequeñas y livianas terrestres y respaldadas por un poder aéreo de precisión y que según Rumsfeld fue «la receta para el éxito»[37], y donde también fue crucial para derrotar a los talibanes, el rol jugado por el general Tommy Franks, comandante del Comando Central de EE. UU. Y responsable de la Fuerza, Inteligencia, Vigilancia y Reconocimiento (ISR) proveniente de sistemas basados en el espacio con sistemas aéreos no tripulados.

A partir de ese momento el conflicto combinará operaciones militares encubiertas y abiertas con escuadrones paramilitares o mercenarios como fuerza de tarea principal con actores no estatales, lo que incluye la necesidad de actualizar los procedimientos de combate y garantizar la capacidad de abordar eficazmente los desafíos planteados por la guerra híbrida donde las reglas de enfrentamiento difieren de las de una guerra convencional.

La declaración final hecha en la cumbre de la OTAN en Varsovia (julio de 2016) por los jefes de Estado y Gobierno de los países miembros de la Alianza del Atlántico Norte fue clara cuando reconocieron que «existe un arco de inseguridad e inestabilidad en la periferia de la OTAN y más allá» La Alianza se enfrenta a una gama de desafíos y amenazas de seguridad que se originan tanto en el este como en el sur; de actores estatales y no estatales; de las fuerzas militares y de

[37] H. A. S. C. (2000): Counter-insurgency an irregular warfare: issues and lessons learned, Hearing Held May 7, 2009, Committee on Armed Services, House of Representatives No. 111-55, US Government Printing Office, Washington.

ataques terroristas, cibernéticos o híbridos. Las acciones agresivas por ejemplo de Rusia, incluidas actividades militares provocadoras en la periferia del territorio de la OTAN y su demostrada voluntad de alcanzar objetivos políticos mediante la amenaza y el uso de la fuerza son una fuente de inestabilidad regional, y desafían fundamentalmente a la Alianza, dañando la seguridad euroatlántica y amenazando a Europa.

Nuestra seguridad también está profundamente afectada por la situación de inseguridad en Medio Oriente y África del Norte, que se ha deteriorado significativamente en toda la región. El terrorismo, particularmente perpetrado por el llamado Estado Islámico de Iraq y el Levante (EIIL)/ Da'esh, ha alcanzado un nivel de intensidad sin precedentes, alcanza a todo el territorio aliado y ahora representa una amenaza inmediata y directa para nuestras naciones y la comunidad internacional. La inestabilidad en Medio Oriente y África del Norte también contribuye a la crisis de refugiados y migrantes[38].

En la próxima cumbre de la OTAN, que tendrá lugar en julio de 2018 en Bruselas, los miembros deben dar un paso adelante en la evolución de las amenazas y reforzar su defensa colectiva. El secretario general de la OTAN dijo que «nuestros grupos de combate multinacionales en el este de la Alianza ahora están en pleno funcionamiento y estamos fortaleciendo nuestra presencia en la región del Mar Negro. También estamos intensificando nuestros esfuerzos contra los ciberataques y las amenazas híbridas»[39].

Jens Stoltenberg dijo que la OTAN basará su trabajo con naciones y organizaciones asociadas para luchar contra el terrorismo y mantener estable nuestro vecindario, impulsando nuestra misión de capacitar, asesorar y ayudar a las fuerzas locales para garantizar que su país nunca vuelva a ser un refugio seguro para los terroristas internacionales.

Como vemos, la guerra no convencional se está convirtiendo en una amenaza mundial y tenemos que enfrentarla y combatirla con todas nuestras

---

[38] NATO Warsaw Summit Communiqué, op. cit. 13th Point. https://www.nato.int/cps/en/natohq/official_texts_133169.htm [consultado 29 marzo 2018]

[39] NATO (2017) Secretary General statement. 20 October 2017

capacidades, y así se hace actualmente en una serie de áreas como Somalia, Yemen, etc., donde la solución establecida para cada uno de esos problemas no generalmente debe ser convencional pues necesariamente debe ser diferente.

David J. Kilcullen considera que «la contrainsurgencia es factible, aunque definitivamente no es la preferida en el entorno estratégico actual. Pero si necesitamos involucrarnos en él, especialmente en las sociedades tribales tradicionales, haciendo énfasis en las asociaciones locales y las fuerzas de seguridad locales, para que estas protejan a sus comunidades contra la presencia extremista como componente esencial de dicha campaña. En un nivel más estratégico, tales alianzas locales también son un componente clave para hacer frente a la amenaza del terrorismo takfir transnacional»[40].

Ahora que hemos identificado el problema, la forma y los medios con los que lucha, la preocupación de las organizaciones internacionales es cómo maniobrar. Como dicen Qiao Liang y Wang Xiangsui, «en la guerra y la guerra no militar, que es principalmente nacional y supranacional, no hay territorio que no pueda ser superado; no hay medios que no puedan usarse y no hay territorio y método que no puedan usarse en combinación»[41]

3.2 DE LA GUERRA HÍBRIDA EN ÁMBITO MILITAR A LAS AMENAZAS HÍBRIDAS EN ÁMBITO SOCIAL.

Fue en el ámbito militar donde surgieron los primeros debates acerca de las guerras híbridas y los conflictos híbridos, que desde su inicio se vincularon con el concepto de "guerras asimétricas", término aún más radicado en el vocabulario castrense. Con ello se hacía referencia a todos aquellos conflictos violentos en los

---

[40] H. A. S. C. (2000): Counter-insurgency an irregular warfare: issues and lessons learned, Hearing Held May 7, 2009, Committee on Armed Services, House of Representatives No. 111-55, US Government Printing Office, Washington. pág. 10

[41] Liang, Qiado and Xiangsui, Wang (1999): University Warfare, Beijing, PLA Literature and Arts Publishing House.

que coexistían simultáneamente elementos "no convencionales" con aquellos típicamente militares o convencionales[42].

Con el transcurso de los años, el fenómeno se amplió con el uso del término "conflictos híbridos", que luego derivó en el más usado y popular "amenazas híbridas". Como veremos en las próximas páginas, la flexibilidad del concepto responde no tanto a una dificultad en la identificación del objeto del estudio en sí, sino más bien a una mejor capacidad de aproximación científica a un fenómeno complejo. Mientras existen teóricos que aún buscan avanzar en una definición clara y distinta, como exigiría la máxima de cientificidad cartesiana, una gran parte de la doctrina prefiere adoptar una visión omnicomprensiva de todo el contexto social en el que surgen las amenazas, conflictos y guerras híbridas. Es más, coherentes con esta lógica, el foco debería estar centrado no tanto en tipologías de conflictos sino en la naturaleza, características y efectos típicos de las dinámicas sociales de hibridez.

En este punto comenzaremos por analizar los estudios específicos que han consolidado la doctrina y cimentado el debate internacional sobre el complejo fenómeno de las amenazas híbridas. En base a los estudios llevados a cabo podremos luego elaborar una explicación razonada sobre la dinámica global de un mundo híbrido que, incluyendo estos trabajos, nos mostrará con más claridad cómo las amenazas híbridas no deberían seguir siendo consideradas como una rara avis, sino, por el contrario, ellas se configuran como los fenómenos típicos y cada vez más recurrentes de un innovador contexto global que ya está aquí.

Surge claramente aquí la necesidad de realizar aquí la primera distinción conceptual. Las guerras o conflictos híbridos se distinguen de las "amenazas híbridas" pues mientras los primeros conllevan implícitamente un elemento de violencia física, o factor cinético, las amenazas no necesariamente implican el uso de la fuerza o violencia, sino que pueden relacionarse con la utilización de

[42] Treverton, G.; Thvedt, A.; Chen, A.; Lee, K. y McCue, M. (2018) pag 74. Addressing Hybrid Threats. Centro de Excelencia sobre Amenazas Híbridas y Swedish Defense University.

múltiples elementos de poder, de sumisión e influencia, todos ellos relacionados con sectores no militares de la sociedad: áreas como la información, la política, la economía, las finanzas, los movimientos sociales, las infraestructuras críticas, las redes sociales, la cultura, el prestigio, la paz social.

Todos ellos constituyen nuevos campos de acción, donde las potencias del futuro buscarán desplegar sus estrategias y tácticas con el fin de ganar las diarias batallas que les permitan imponer su voluntad, mejorar su posición geopolítica y cumplir con su visión estratégica.

En este nuevo mundo híbrido, más que buscar una definición precisa a estos nuevos fenómenos, nuestro primordial esfuerzo deberá estar focalizado en brindar un panorama general sobre las complejas interconexiones y efectos de estas amenazas. No obstante, ello, iniciaremos con un orden cronológico evolutivo de los conceptos, para que el lector logre ir adquiriendo y reflexionando sobre todas las aristas que configuran tal innovador fenómeno. Es por ello por lo que partiremos analizando los aportes doctrinarios más importantes en ámbito militar, para luego ampliarnos a otros aportes que nos permitirán obtener, al final de este capítulo, un cuadro teórico general que avance luego hacia una visión integral sobre cómo las dinámicas híbridas afectan a la sociedad global actual.

3.3. La Doctrina China De La "Guerra Sin Restricciones" Y De Las "Tres Guerras".

Concebido en 1996 y publicado en 1999 por una editorial relacionada con las fuerzas armadas chinas, el libro traducido como "Guerra Sin Restricciones" [43], si bien su traducción literal significa "guerra más allá de los límites", se convirtió rápidamente en un clásico imprescindible a la hora de analizar no sólo las amenazas híbridas sino también, y en modo más general, la visión china actual sobre el desarrollo de los conflictos geopolíticos que se desarrollarán en un futuro cada vez más tecnológico y multipolar.

[43] Liang, Q. y Xiangsui, W. (1999). Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House.

Sus autores, Qiao Liang y Wang Xiangsui, son coroneles superiores con cuatro estrellas de la Aeronáutica Militar china, con experiencia de trabajo como Comisarios políticos y de comando superior y propaganda en el Departamento Político del aeronáutico y el Distrito Militar Aeronáutico de Guangzhou (Cantón), en el sur de China. Considerados como intelectuales del arte de la guerra, comienzan el prólogo de su libro subrayando cómo la guerra, en su concepto tradicional, ha sufrido un cambio radical a partir de la última década del siglo pasado. Más específicamente a partir de la Guerra del Golfo, que se presenta como la última guerra que ha de verdad ganado la que por entonces se estrenaba como la única superpotencia mundial, los Estados Unidos.

A partir de entonces, y en particular modo con la introducción de la tecnología, con la sumisión a la lógica del mercado y con las nuevas modalidades de combate, se modificó también el rol fundamental y preponderante que la guerra tenía a la hora de determinar quién detentaba el poder e imponía el orden en el escenario geopolítico mundial. La supremacía histórica, que hasta ese momento estaba determinada por la capacidad militar y, en consecuencia, por la imposición del principio por el cual "la fuerza tiene siempre razón", se ha quebrado en modo imprevisto.

En un nuevo mundo de incertezas, las guerras sufren una metamorfosis compleja, dando lugar a "semiguerras" o "casi guerras" y evidenciando que, allí donde la violencia militar se ha reducido, ella fue suplantada por violencias de tipo político, económico o tecnológico. Cambia así también el objetivo último de todo conflicto armado, el cual pasa de ser "el uso de la fuerza para obligar a un enemigo a que someta a la propia voluntad" a un nuevo paradigma: "usar todos los medios, incluida la fuerza de las armas y los sistemas ofensivos militares y no militares, letales y no letales, para obligar al enemigo a aceptar nuestros propios intereses".

Esta reflexión sobre el cambio en la naturaleza de la guerra iba de la mano con la mutación que venía sufriendo tal concepto desde la perspectiva ideológica de la China comunista. Si, desde los tiempos de Mao, se cultivó una visión global de guerras de clases entre pueblos oprimidos contra el imperialismo capitalista, a partir de la década de los 80, con el liderazgo de Deng Xiaoping y de Jiang Zeming, se fomentó una estrategia político-militar constituida prioritariamente

por ofensivas tácticas dentro de un cuadro general de defensa estratégica, cuyo último bastión de protección nacional estaba constituido por la disuasión de su arsenal nuclear.

A partir de los 90, China entiende que la tecnología, la profesionalización militar y una planificación operativa omnicomprensiva son esenciales para afrontar con éxito los cruciales objetivos geoestratégicos futuros, sobre todo la reunificación con Taiwán, el liderazgo en Asia y el constante crecimiento económico. Y es para afrontar tales desafíos que los autores han desarrollado la lógica ínsita a este trabajo. Sólo a través de una guerra no convencional en todos los ámbitos sociales, las potencias militares y tecnológicamente menos preparadas podían tener una posibilidad de vencer frente a las superpotencias globales.

Dejando de lado la lógica de las guerras convencionales de destrucción estructural, los autores buscan cómo modificar el equilibrio entre fuerza superior y fuerza inferior. Y, dado que la innovación y los métodos de ataque se desarrollan y perfeccionan más rápidamente que los métodos de defensa, se hace necesario dejar de lado cualquier lógica de guerra de resistencia que diese la iniciativa siempre a la parte con superioridad. Es entonces que se impone una lógica basada en la proactividad y no en la reactividad; en el ataque del enemigo y no en la defensa propia; en la innovación focalizada en identificar y atacar las vulnerabilidades del enemigo, con el objetivo de debilitar eficazmente sus capacidades operativas basadas en una superioridad tecnológica y de equipamiento.

Sin embargo, al ver con cierto escepticismo la posibilidad de alcanzar tecnológicamente a los Estados Unidos, los autores sugieren la búsqueda de una vía alternativa, como natural aplicación del principio filosófico chino Wù Jí Bì Fǎn. [44]Es por ello que no se debe imaginar el futuro de las guerras como guerras de información o ataques de precisión por ayuda de drones y comandos digitales. Toda esta tecnología está ya en su pico máximo de generación, y, por ende, hay que buscar métodos alternativos.

---

[44] Este principio filosófico sostiene que "cuando las cosas llegan a un extremo, tenderán sólo a moverse en la dirección contraria".

Y es aquí donde surge la idea clave del libro. La estrategia de la guerra sin límites requiere, por ende, de una combinación estratégica de terrorismo, manipulación de los medios de comunicación, ataques a sitios web, manipulación de las bolsas bursátiles para causar crisis financieras, difusión de virus informáticos y otras armas no convencionales. Con una claridad pocas veces vista, sobre todo en la literatura china, los autores presienten en que "una hermosa mañana la gente se despertará y descubrirá con sorpresa que algunas cosas gentiles y buenas han comenzado a adquirir características ofensivas y letales."

Es clave destacar aquí tres ideas que luego nos serán de utilidad para explicar el nuevo contexto social de hibridez. Por un lado, los autores enfatizan que la guerra tradicional muta de ser una lógica de "aniquilamiento" o de "sumisión" a ser, en un orden de gradualidad, o bien una guerra de "destrucción estructural," o de imposición del propio interés o de simple aceptación por parte del adversario de su imposibilidad para imponerse por sobre nuestra voluntad.

En segundo término, Liang y Xiangsui subrayan también la importancia de ir más allá de las reglas. En esta nueva "guerra sin límites", vencen los Maquiavelos o los Han Feizis modernos, que logran superar los confines, las restricciones y hasta los tabúes que separan lo militar de lo no militar, combinando varios métodos y utilizando todos los recursos a disposición del modo más eficaz para combatir batallas también fuera del campo de batalla. En vez de quedarnos en una actitud previsible, convencional y estrictamente militar, el libro propone que busquemos vencer en forma rápida y eficaz a través del uso de objetivos asimétricos (negar, destruir, desorganizar, desunir, denigrar y someter) de la estructura organizativa y moral del adversario.

Estas acciones se deben llevar a cabo en modo dinámico, proactivo y pensando fuera de los esquemas establecidos, siempre con una mentalidad avasalladora y triunfal. Todo sirve para lograr estos objetivos: denunciar corrupción gubernamental en el poder del enemigo, reavivar viejas enemistades entre alianzas enemigas, poniendo a la población en contra de su gobierno o de otras poblaciones aliadas, burlándose de sus líderes o evidenciando la ineficiencia de sus instituciones, etc. Lo importante siempre es atacar, a todos, de todas las formas, en todo campo. "Es una cuestión de entender que siempre estamos decidiendo si ser o el cazador o la presa."

Debemos recordar que, ya desde los tiempos inmemoriales de Sun Tzu, se conocían y estudiaban métodos que podríamos denominar "híbridos". En efecto, su "enfoque de los cuatro métodos" explicaba cómo el Imperio Chino ha sabido lidiar con sus enemigos adaptando su respuesta a las características propias de cada adversario, tratando "bárbaramente a los bárbaros", utilizando mercenarios y armando alianzas estratégicas para dividir a sus contrincantes vecinos[45].

La tercera idea que surge implícita del libro, sobre todo a partir de los ejemplos que allí se citan, es la mutación entre medios y fines, entre medios entre sí y entre fines entre sí. Así, por citar un ejemplo, los autores critican la política estadounidense de "cero muertos" pues, desde su perspectiva, esta política no está basada prioritariamente en el valor de la vida humana de sus soldados, sino en un entramado complejo de otros intereses, que van desde la aplicación de métodos de ataque automatizados y a distancia hasta la crítica de los medios masivos de comunicación.

Esta política se impone cada vez más para hacer una demostración pública de su riqueza y de la potencia de sus fuerzas armadas, de su tecnología, del uso de armas costosas y altamente tecnológicas para jactarse de lograr reducir al mínimo las pérdidas humanas. "Sólo una nación rica podría hacerlo," sostienen Liang y Xiangsui. "Cada uno de sus bombarderos es como una montaña de oro volante que vale mucho más que sus objetivos." Es por ello que los enemigos de Estados Unidos han entendido que, "si no puedes abatir sus aparatos militares, mata a sus soldados. Los Estados Unidos quieren la victoria, pero no las pérdidas que ello acarrea".

Este cambio en los medios y los fines será objeto de análisis más adelante, por considerarlo como una de las características esenciales de la hibridez.

Es de destacar que, en 2003, China comenzó a poner en acto su estrategia general de guerra de la información, denominada "Tres Guerras" pues se llevaba a cabo, en manera conjunta y sinérgica, a través de tres líneas de acción: las

[45] Treverton, G.; Thvedt, A.; Chen, A.; Lee, K. y McCue, M. (2018) pág. 74. Addressing Hybrid Threats. Centro de Excelencia sobre Amenazas Híbridas y Swedish Defense University.

operaciones psicológicas estratégicas; las operaciones de manipulación a través de medios masivos de comunicación; y la guerra convencional dentro del marco del Derecho Internacional Público para manipular estrategias, políticas defensivas y la percepción de la opinión pública internacional [46].

3.4 LA VISIÓN RUSA SOBRE LOS CONFLICTOS HÍBRIDOS.

Rusia ha sido desde siempre otro actor fundamental a la hora de desarrollar los conceptos relacionados a la hibridez en campo militar. Y sobre todo en ponerlos en práctica. El Kremlin se ha demostrado el más proactivo e innovador actor internacional en la aplicación de métodos de guerra híbrida. Desde el 2004, se estima que ha atacado de este modo al menos a 27 países de Europa y de Norteamérica [47].

Entre los expertos de Moscú se prefiere utilizar el término "guerra no linear," "guerra de nueva generación" o "guerra especial", para referirse a operaciones como las llevadas a cabo en Crimea, Ucrania, y que luego conformaron una verdadera política de Estado oficial en cuanto a sus relaciones exteriores. Mientras Obama, durante la crisis en Crimea, acusaba al Kremlin de haber vuelto a los "viejos modos" propios de la Guerra Fría, los intelectuales rusos estaban ya explicando cómo la crisis en Ucrania significó el primer ejemplo de una nueva modalidad no linear de entender los conflictos, donde no existen dos bandos contrapuestos, sino que confluyen cuatro coaliciones y se enfrentan todos contra todos [48].

En 2013, el Jefe de Estado Mayor del ejército ruso, Gen. Valery Gerasimov, retomando las teorías de Liang e Xiangsui, hizo públicas las ideas que venía aplicando para entender la "guerra sin límites" como "guerra no linear", con una aplicación especial a las necesidades, potencialidades y visión del contexto geopolítico de la Federación Rusa. Nace así la "doctrina Gerasimov", si bien todos

---

[46] Raska, M. (2015). Hybrid Warfare with Chinese characteristics. Singapur: Nayang Technological University.

[47] Chehadé (2015), Fadi Chehadé at the Senate Commerce Committee, pag. 38

[48] Pomerantsev, P. (2014). How Putin is Reinventing Warfare. Foreign Policy.

reconocen que ella se basa en los trabajos ya iniciados del Gen. Makarov, antecesor de Gerasimov al frente de la Jefatura de Estado Mayor.

Poniendo como ejemplo el caso de las revoluciones de la "Primavera Árabe" y la "Revolución Naranja" en Ucrania, Gerasimov sostiene que dichos eventos, que muchos consideraron espontáneas manifestaciones sociales locales, en realidad constituyen un nuevo modo típico de hacer la guerra en el siglo XXI.

Gerasimov establece que las reglas de la guerra han cambiado en modo sustancial, que las guerras ya no se declaran ni se ganan o pierden, sino que, en este estado de guerra constante, es necesario utilizar medios no militares para alcanzar objetivos políticos y estratégicos en modo más eficaz que con el tradicional uso de la fuerza armada. Desde esta lógica, los Estados deben encontrar y explotar en todo momento las vulnerabilidades de los adversarios en todos los ámbitos sociales.

Desde la perspectiva rusa, mientras los Estados Unidos y Europa aún piensan en términos de alianzas estratégicas como la Unión Europea y la OTAN, en el mundo actual la globalización ha permitido a Rusia forjar alianzas comerciales con las principales corporaciones multinacionales y mantener además una amplia influencia en Estados periféricos cuyos gobiernos están necesitados de financiación o de apoyo internacional.

De este modo, el Kremlin se refuerza por lo bajo, implementando modalidades políticas no cinéticas, manipulando medios, comprando voluntades, fomentando subversiones, haciendo bullying regional, desinformando, atacando cibernéticamente sitios oficiales e infraestructuras críticas. Y todo ello sumado al recurso a la fuerza militar en las situaciones puntuales que así lo requieran, con habilidad quirúrgica y, si es posible, en modo poco convencional e irregular.

Según Gerasimov[49] , las características de esta "nueva generación de guerra" son las siguientes:

1) No es necesaria una declaración de guerra para iniciar acciones militares, las cuales coexisten y se desarrollan en épocas consideradas de paz.

[49] Banasik, M. (2015). How to Understand the Hybrid War. Sicuritologia, pp. 2829

2) Contactos en altas esferas, no hay contacto con los grupos armados específicos.

3) La neutralización de las capacidades militares y económicas se realiza a través de ataques quirúrgicos, ya sea con medios militares como sabotaje o ciberataques, contra la infraestructura crítica que lo sustenta.

4) Uso masivo de armas de precisión, de operaciones especiales, con uso de robótica y nuevas tecnologías aplicadas a las armas.

5) Aprovechar a civiles armados para realizar operaciones encubiertas o sin posibilidad de atribución de responsabilidad.

6) Ataques simultáneos a subunidades y medios militares en todo el territorio del adversario.

7) Ataques simultáneos en todos los dominios: aire, tierra, mar, espacio, ciberespacio y ámbito de la información.

8) Uso de métodos de influencia indirectos y asimétricos.

9) Gestión de medios para influir en la dimensión informacional del enemigo, financiándolos y manejándolos desde afuera.

Se trata de una verdadera estrategia global de conflictividad híbrida o, como sostiene el prof. Mark Galeotti (2017), de una "guerrilla geopolítica". Los intereses del Kremlin en Europa son políticos, buscando distraer, manipular, dividir y desmoralizar a la sociedad, para que los europeos prefieran no meterse con Rusia y hasta darle la razón en ciertos asuntos internacionales, dejándole libertad de acción al menos en su esfera de influencia. Dado que Rusia conoce bien del poderío de la OTAN y de la facilidad con que un conflicto frontal pudiera escalar a una hecatombe termonuclear, la alternativa es mantenerse siempre en un constante estado de "paz caliente" y focalizarse en las vulnerabilidades de Occidente. Y la principal debilidad de las democracias occidentales, desde la visión de Moscú, es su falta de disciplina, rudeza, determinación y unidad.

Es por ello que se busca generar la desestabilización en los sistemas democráticos, promoviendo crisis de legitimidad, maximizando la publicidad sobre la corrupción política interna, promoviendo el disenso generalizado y

apoyando el ascenso de movimientos populistas y nacionalistas. Asimismo, Galeotti (2014) destaca cómo Rusia lleva adelante esta política con todos los medios sociales a disposición y sin una estructura centralizada, permitiendo así que cualquier sector, grupo o agencia tome la iniciativa allí donde vea una ventaja propia o una debilidad ajena.

3.5 La teorización de la conflictividad híbrida desde la perspectiva militar estadounidense.

Varios han sido los intentos de conceptualización sobre las amenazas y conflictos híbridos en el ámbito militar estadounidense. El Tte. Cnel. Hoffman, un investigador del Instituto Potomac de Estudios Políticos del Centro sobre Amenazas Emergentes y Oportunidades del Comando de Desarrollo de Combate del Cuerpo de Marines de los Estados Unidos, es reconocido por sus trabajos sobre el tema[50] . Su trabajo parte de la constatación geopolítica de que los atentados terroristas del 11 de septiembre de 2001 en Estados Unidos significaron el fin del "momento unipolar" y del triunfalismo unilateral que se había generado en el gigante americano desde el fin de la Guerra Fría. Como corolario de este fin de la idea de Fin de la Historia de Fukuyama (1992), los conflictos estatales del siglo XX, según Hoffman, serán reemplazados por guerras híbridas y luchas asimétricas donde no habrá una distinción clara ni entre civiles y militares ni entre violencia organizada, terror, crimen y guerra.

Hoffman parte de un concepto que lo acomuna con las visiones chinas y rusas al respecto: lo importante de toda dinámica híbrida es su preocupación por entender al adversario, y así, descubriendo sus vulnerabilidades, enfocarse en ellas para obtener una ventaja. Para Hoffman, los conflictos híbridos son todos aquellos donde se mezclan y se hacen poco claras las distinciones entre guerra y paz, entre combatientes y no combatientes, entre tácticas tradicionales e irregulares, actos terroristas y desorden criminal.

---

[50] Hoffman, F. (2007). Conflict in the 21st Century: The Rise of Hybrid War. Arlington: Potomac Institute for Policy Studies.

Las amenazas híbridas, en este contexto, buscan específicamente golpear las vulnerabilidades de los Estados Unidos y pueden ser conducidos tanto por Estados como por un variado abanico de actores no estatales. Si bien los actos que configuran a los conflictos híbridos pueden realizarse en modo aislado y descentralizado, Hoffman subraya cómo existe una coordinación y dirección operacional y táctica para maximizar los efectos de tales ataques tanto a nivel material como psicológico del enemigo atacado.

Las guerras híbridas no sólo se presentan como un desafío al modo de pensar en ámbito militar, sino que también son muy efectivas a la hora de identificar y golpear las vulnerabilidades culturales estratégicas del modo de hacer la guerra del ejército estadounidense. Hoffman, citando a Bentz (2009), subraya cómo una de las vulnerabilidades más importantes del sector militar estadounidense es la tendencia a creer que todos los problemas pueden ser resueltos gracias a soluciones tecnológicas. Este error se ha demostrado no sólo costoso en términos económicos, sino también extremadamente nocivo en términos psicológicos para todas las fuerzas occidentales [51].

Si bien Hoffman enfatiza que esta nueva modalidad de guerra no implica el fin de las guerras convencionales, sino que agregan ulteriores complejidades y ponen en jaque los planteamientos científicos tradicionales, tanto en su cognición como en su aplicabilidad práctica.

Hoffman realiza un estudio histórico en búsqueda de casos de guerras híbridas, identificando conflictos antiguos caracterizados por la asimetría de las partes, como en las guerras del Peloponeso entre Atenas y Esparta, pasando por la inmiscusión de Wellington en la preparación de la guerrilla nacional y su coordinación con las fuerzas aliadas contra Francia durante la guerra de Independencia española.

Un caso de manual de lo que implica una guerra híbrida es, a juicio de Hoffman, el conflicto entre árabes e israelíes en el sur del Líbano en 2006. El criterio que determina esta clasificación radica en el uso simultáneo, por parte de Hezbollah, de métodos de guerra tradicional y modalidades de lucha irregulares.

[51] Hoffman, F. (2009). Further Thoughts on Hybrid Threats. Small Wars Journal.

En sintonía con Hoffman encontramos la opinión de David Kilcullen, uno de los expertos en contrainsurgencia más reconocidos en los Estados Unidos. Para él, las "amenazas híbridas" representan un fenómeno donde se mezclan binomios que antes resultaban distinguibles y separados y que ya no lo son en forma nítida, como lo civil con lo militar, lo gubernamental con lo privado, las cuestiones domésticas con las internacionales, los medios violentos con aquellos que prescinden de la violencia, pero logran los mismos efectos.

No obstante, el trabajo de Hoffman fuese extensamente conocido y valorado, el concepto de conflictos híbridos no logró arraigarse inmediatamente en la cultura militar estadounidense. Autores como Simpson, McCuen y Huber no lograron identificar características diferenciadoras significativas que confirmen la existencia de la tipología especial de "guerras híbridas" distintas de otras guerras convencionales[52].

Asimismo, el término brilló por su ausencia, hasta hace relativamente poco, tanto en la "Estrategia de Defensa Nacional" de 2008, como en la "Estrategia de Seguridad Nacional" de 2010, y en la "Estrategia Militar Nacional" de 2011. Sin embargo, en la actual "Estrategia de Defensa Nacional" de 2018 (U.S. Department of Defense, 2018) se recepta, sin nombrarlo explícitamente, varios conceptos similares a los conflictos híbridos, sobre todo cuando se realizan consideraciones sobre cómo los Estados Unidos se deben preparar para los desafíos del futuro.

Por un lado, al hablar del contexto global, se enfatiza cómo nos encontramos en un período de atrofia estratégica, en la que se está erosionando la ventaja competitiva militar, mientras que se observa un incremento en la situación de desorden global y normativo, de volatilidad y de cambio tecnológico nunca vistos.

En este contexto, el terrorismo ha dejado de ser la amenaza número uno para la seguridad nacional, siendo reemplazada por la competición estratégica de otros países, en especial China y Rusia (U.S. Department of Defense, 2018), a quienes acusa de querer consistentemente modelar al mundo según sus modelos

[52] CESEDEN. (2012). El Enfoque Multidisciplinar en los Conflictos Híbridos. Documentos de Seguridad y Defensa, 51. Ministerio de Defensa de España.

autoritarios a través del ejercicio de coacción sobre las decisiones económicas, diplomáticas y de seguridad de otras naciones.

Esta apreciación implica el reconocimiento y la preocupación que para las autoridades estadounidenses representan los presupuestos geopolíticos que sirven para el desarrollo eficaz de amenazas, conflictos y guerras híbridas.

Junto a la acción de estas grandes potencias, el documento acusa a "Estados Delincuentes" (Rogue States), como Corea del Norte e Irán, de desestabilizar varias regiones del mundo a través del apoyo al terrorismo y del desarrollo de armas nucleares, biológicas, químicas, convencionales y no convencionales (U.S. Department of Defense, 2018).

Asimismo, se enfatiza la necesidad de atender los "desafíos por parte de adversarios en cada área operativa", con clara referencia a la multidimensionalidad que caracteriza a los conflictos híbridos (U.S. Department of Defense, 2018).

A diferencia de la Estrategia Nacional de Defensa 2018, la más reciente Estrategia Militar Nacional (U.S. Chief of Staff, 2015), vigente desde 2015, menciona explícitamente a los conflictos híbridos. Ya desde su prólogo se advierte que el actual ámbito global de seguridad es el más imprevisible de los últimos 40 años, con un exponencial aumento del desorden global, de desafíos tanto por parte de Estados como de redes transregionales de grupos subestatales, todos apostando a un rápido desarrollo tecnológico.

Los conflictos híbridos son definidos como casos en los que existe una superposición de la violencia estatal con la no estatal, que se presenta como un continuum de conflictividad donde los actores mezclan técnicas, capacidades y recursos para alcanzar sus objetivos. Asimismo, este documento resalta otras tipologías de conflictos híbridos: aquellos casos en los que fuerzas militares esconden su pertenencia asumiendo identidades no estatales, o cuando los grupos terroristas desarrollar capacidades militares típicamente militares.

Un punto por destacar es la enunciación de tres de las características esenciales de los conflictos híbridos: el incremento de la ambigüedad, la decisión de tomar la iniciativa para paralizar al adversario, quien sufre debido a la complejidad a la hora de tomar decisiones sobre cómo contrarrestar estas

amenazas y por la lentitud en la coordinación de respuestas eficaces. Todos estos factores refuerzan la previsión de que estos conflictos persistirán en el futuro (U.S. Chief of Staff, 2015) (ver figura 1).

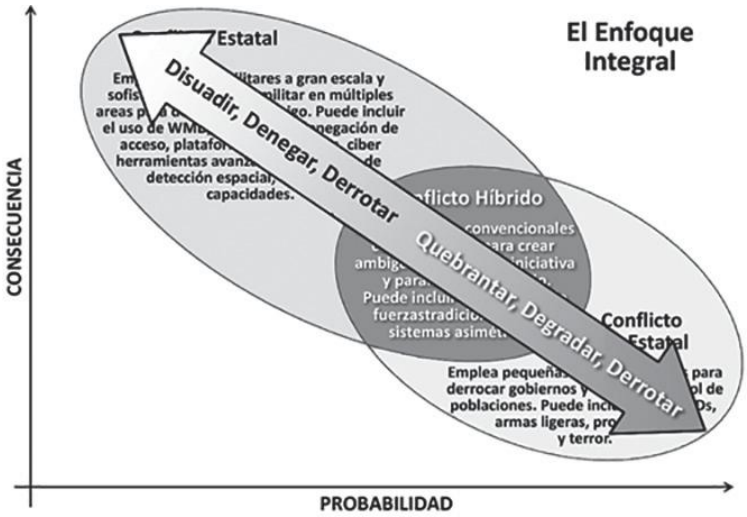
Para lograr sus objetivos, la Estrategia Militar Nacional 2015 promueve un enfoque integral, compuesto por tres objetivos: la disuasión, la denegación y la derrota de los Estados adversarios; el quebrantamiento, la degradación y la derrota de las organizaciones extremistas violentas (VEO, violent extremist organizations);[53] y el refuerzo de nuestra red global de aliados y colaboradores (ver figura 2).

Figura 1. El Continuum de Conflictividad en la Estrategia Militar Nacional USA 2015

Fuente: U.S. Chief of Staff (2015)

Figura 2. El Enfoque Integral en la Estrategia Militar Nacional USA 2015

[53] En inglés es conocido por el doble juego de las tres "D": Deter, Deny, Defeat, por un lado, y Disrupt, Degrade, Defeat por el otro.



Fuente: U.S. Chief of Staff (2015)

3.6. LA NOCIÓN DE GUERRAS Y AMENAZAS HÍBRIDAS DE LA OTAN.

En los últimos años, en el seno de la Organización del Tratado del Atlántico Norte (OTAN) se ha dado un gran impulso al debate académico y al diseño e implementación de innovadoras perspectivas en lo referente a los conflictos híbridos y demás desafíos en la defensa y seguridad local y regional del futuro. Es con la OTAN que los estudios empiezan a orientarse más allá de las guerras híbridas para ir hacia las amenazas, pero siempre desde una perspectiva eminentemente militar.

En el seno de esta gigantesca organización militar se mantiene aún la tensión entre quienes, por un lado, no reconocen una cualidad ontológica específica a las "guerras híbridas", subrayando cómo hablar de híbridos resulta una moda que se extendió demasiado "hasta el punto en que actualmente

dificulta en vez de ayudar a las operaciones conjuntas"[54]; y, por otro lado, quienes, si bien aceptando la dificultad para encontrar una definición precisa, terminan siempre por señalar que "tales fenómenos, sin embargo, son reales"[55].

La OTAN propone una definición de amenazas híbridas vinculada directamente con su propia experiencia de actuación en situaciones de crisis. En particular, su "Enfoque Integral" (Comprehensive Approach) surgió de la constatación, por parte de las fuerzas armadas de la coalición occidental, de que, pese a contar con supremacía militar a nivel global, no contaban con la experiencia y capacidad necesarias para llevar a cabo misiones de baja intensidad donde se priorice la necesidad de estabilización postconflicto, de reconstrucción nacional y de gestión integral de crisis[56].

Ello resultó evidente en regiones como los Balcanes, África Subsahariana, Irak y Afganistán, donde a la inexperiencia militar para gestionar complejas situaciones sociales, se le agregó la inviabilidad económica y la falta de tacto político para promover una reconstrucción institucional local que pudiera hacerse cargo en modo más eficaz de muchas de las problemáticas que los militares no lograban resolver. Para colmar este vacío tanto operativo como estratégico, la OTAN, ayudada por una constelación de organizaciones del sector civil, comenzó a elaborar nuevos protocolos de colaboración cívico militar para dar una respuesta integral, homogénea, interdisciplinaria y multinivel a cada situación de crisis.

Es a partir de esta experiencia propia que la OTAN conceptualiza a dichas amenazas como el "lado oscuro" de su propia actuación, como una acción reflejo llevada a cabo por sus adversarios para contrarrestar el desarrollo de su política de "Enfoque Integral". Así concebidas, las "amenazas híbridas" se configurarían

---

[54] Mattis, J. (2008). USJFCOM Commander's Guidance for Effectsbased Operations. Parameters, pp. 18-25

[55] Giles, K. (2015). "Conclusion: Is Hybrid Warfare Really New?" En Lasconjarias, G. y Larsen, J. (eds.) (2015). Nato's Response to Hybrid Threats. NATO Defense College Forum Paper, 24, p. 337.

[56] CESEDEN (2012), op. cit., pp. 26 y ss

como el uso de medios de cualquier tipo con el objetivo de desestabilizar a las sociedades y las instituciones de los países aliados, especialmente utilizando medios de propaganda, movimientos populares, grupos subversivos y terroristas, recursos digitales y ciberataques [57].

Desde esta perspectiva, las amenazas híbridas serían concebidas no tanto como una innovación disruptiva en clave de ataque sino como una reacción adaptativa en clave de defensa, enfatizando la necesidad de estructurar tanto a nivel teórico como práctico una visión interdisciplinaria, abierta e innovadora para prever y gestionar en manera coherente y eficaz todos los medios a disposición.

A. Jacobs y G. Lasconjarias (2015), dos asesores del Colegio de Defensa de la OTAN en Roma subrayan que la idea de guerra híbrida, si bien presenta algunas deficiencias desde el punto de vista conceptual, resulta útil a la hora de idear nuevas perspectivas innovadoras para afrontar los desafíos en términos de seguridad de la OTAN, permitiendo asimismo aplicar y estudiar perspectivas estratégicas diversas y compararlas. Estos autores definen a la "guerra híbrida" como una forma de conflicto violento que implica simultáneamente actores estatales y no estatales, con el uso de medios para la guerra convencionales y no convencionales y que no se limita a un campo de batalla ni a ningún espacio territorial específico [58]. Como se ve, se pueden distinguir tres dimensiones en esta definición.

El primer elemento es la poco clara distinción entre lo militar y lo civil, lo que abre la puerta a una amplia gama de instrumentos no militares: tecnología, criminalidad, terrorismo, presión económica, medios humanitarios y religiosos, inteligencia, sabotaje y desinformación. Se enfatiza aquí cómo, al mezclarse todos ellos y aplicarse con una estrategia flexible, pero a todo campo, se genera una especie de "invasión invisible".

---

[57] Cusumano, E. y Corbe, M. (eds.) (2018). A Civil-Military Response to Hybrid Threats. Palgrave Macmillan

[58] Jacobs A., Lasconjarias G. (2015). NATO's Hybrid Flanks: Handling Unconventional Warfare in the South and East. NDC Rome Research Paper, 112.

El segundo elemento se relaciona con la experiencia de que generalmente en los conflictos híbridos participan actores no estatales, como pueden ser milicias armadas, grupos de crimen organizado y transnacional, redes terroristas, como así también fuerzas regulares de un país que se hacen pasar por combatientes sin identificación ni bandera.

El tercer factor clave de la definición que dan Jacobs y Lasconjarias (2015) tiene que ver con el espacio, ya que las guerras híbridas no están limitadas a un territorio físico determinado. El campo de batalla se vuelve múltiple y ambiguo, por causa de la tecnología y de las tácticas y técnicas asimétricas.

Gracias a la colaboración constante entre OTAN, las administraciones de sus países miembros y la Unión Europea, el desarrollo conceptual sobre las conflictos y amenazas híbridas fue mutando desde una explicación meramente castrense hacia una más flexible e integral constelación de conceptos sociales interrelacionados sobre el fenómeno, lo que nos servirá luego de plataforma conceptual para el desarrollo de nuestra teoría sobre el mundo híbrido.

Uno de los ejemplos más importantes de avance en materia conceptual lo han producido dos especialistas militares noruegos, P. Cullen y E. Reichborn-Kjennerud (2016), que han trabajado en el marco del Proyecto "Enfrentando las Guerras Híbridas"[59] (Countering Hybrid Warfare) de la Campaña Multinacional de Desarrollo de Capacidades, un esfuerzo de fuerzas militares occidentales por mejorar las capacidades de respuesta y gestión de fenómenos innovadores en ámbito militar. Según estos autores, la novedad de la guerra híbrida radica en la capacidad de los actores, que pueden ser estatales o no, de "sincronizar múltiples elementos de poder en modo simultáneo y, en forma intencional, aprovechar de elementos de guerra que conllevan creatividad, ambigüedad, no linealidad y cognitividad" [60].

[59] Reichborn-Kjennerud, E. y Cullen, P. (2016). What is Hybrid Warfare? Norwegian Institute of International Affairs Policy Brief.

[60] Cullen, P. y Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. Pág. 3

Las guerras híbridas se adaptan de modo tal que resultan difíciles de ser detectadas y desmanteladas, más aún por el uso de la velocidad, la masificación y la ubicuidad que les otorgan las continuas innovaciones de la tecnología digital. Esta definición cita todos los elementos ya referidos anteriormente, con un agregado interesante. Se hace referencia a "elementos de poder" y no de "armas" ni de "medios militares" o "actos violentos". De este modo, se expande el concepto, pudiendo abarcar hipótesis tan amplias como la diplomacia, la propaganda, o cualquier otro medio no necesariamente militar ni violento.

3.7 La labor de la Unión Europea en definir las amenazas híbridas.

En 2015, el servicio interno de investigación del Parlamento Europeo publicó un documento explicativo donde subraya que el concepto de "amenaza híbrida" no es otra cosa que una metáfora que nos ayuda a comprender las complejidades, dilemas e interrelaciones que presenta el actual ecosistema global. No obstante, esta ambigüedad conceptual, estos investigadores han buscado explicar las diferencias entre "amenazas", "conflictos" y "guerras" híbridas.

En base a este documento, las amenazas híbridas serían todos aquellos fenómenos que surgen de la convergencia e interconexión de diferentes elementos, los cuales forman, en modo conjunto, una amenaza aún más compleja y multidimensional. Los conflictos híbridos y la guerra híbrida son dos categorías específicas dentro de las cuales las tácticas híbridas son utilizadas por un estado para alcanzar sus objetivos estratégicos.

Por conflicto híbrido se entiende a una situación en la que las partes se abstienen de utilizar el uso de fuerzas armadas entre ellas, prefiriendo en cambio una combinación de intimidación militar, explotación de vulnerabilidades económicas y políticas, medios diplomáticos y tecnológicos, para alcanzar sus objetivos.

La guerra híbrida se produce cuando un país emplea el uso de la fuerza armada contra otro país o contra un actor no estatal, conjuntamente con una combinación de otros medios (económicos, políticos y diplomáticos).

Esta distinción entre las tres tipologías de híbridos, si bien plausible de ser utilizada, presenta algunos errores, sobre todo pues concibe a la guerra híbrida sólo en base a dos elementos: la combinación de medios y la posibilidad de que intervenga un actor no estatal. Si nos atenemos estrictamente a dicha definición, cualquier guerra en la que se hayan llevado a cabo negociados diplomáticos en modo simultáneo, podría ser considerada "híbrida", algo que no cuadra ni con el concepto de guerra ni con la idea de hibridez. Asimismo, cuando se refiere al conflicto híbrido, parece surgir de la definición un tácito acuerdo entre las partes por evitar el uso de la fuerza. No se hace alusión, al momento de la distinción de que entre las tres figuras podría establecerse una conexión temporal. Es decir, que una simple amenaza pudiera mutar luego en un conflicto y de allí a una guerra.

Es importante destacar cómo también se inició aquí a hacer referencia a que el factor condicionante que fomenta el uso de métodos híbridos de ataque es la intención de escapar a las limitaciones en cuanto a la legitimación, atribución y proporcionalidad que prescriben las normas internacionales.

A partir de la mitad del 2016, la Unión Europea ha estrechado sus lazos de colaboración con la OTAN en el tema de las amenazas híbridas, a través A través de una Declaración Conjunta sobre un paquete de medidas para implementar y con ello se llevó a cabo la implementación de procedimientos operativos en áreas de ciberseguridad y defensa común.

En abril de 2016, la Comisión Europea, junto al Parlamento y al Consejo de Europeo, ha publicado un documento llamado "Comunicación conjunta sobre la lucha contra las amenazas híbridas". Allí se subraya cómo el concepto de "amenazas híbridas" debe mantenerse lo suficientemente flexible como para responder adecuadamente a los cambios del contexto social. Sin embargo, se aclara que existe la necesidad de desarrollar defensas contra las ambigüedades que obstaculizan los procesos decisorios a nivel local, nacional y comunitario, así como la implementación de medidas contra la explotación, por parte de los enemigos de la Unión, de las vulnerabilidades existentes en las instituciones y en la sociedad de la Unión.

En dicho documento se especifica un concepto de "amenazas híbridas" como:

> *La mezcla de actividades coercitivas y subversivas, de métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos y tecnológicos), que pueden ser utilizados de forma coordinada por agentes estatales o no estatales para lograr objetivos específicos, manteniéndose por debajo del umbral de una guerra declarada oficialmente. Suelen aprovecharse las vulnerabilidades del objetivo y generar ambigüedad para obstaculizar los procesos decisorios. Las campañas de desinformación masiva, que recurren a los medios sociales para controlar el discurso político o para radicalizar, contratar y manipular a individuos que actúan por delegación, pueden constituir vectores de estas amenazas híbridas.*

Como se puede observar, residen en esta definición todos los elementos esenciales anteriormente debatidos, distinguiendo las amenazas híbridas de la guerra híbrida en base a tres puntos:

1) El carácter del actor, que puede ser declaradamente estatal o no estatal;

2) Por los medios empleados, que deben ser convencionales y no convencionales; aquí el uso de "y" es clave para sobreentender que se requiere simultaneidad en el uso de ambos medios, marcando así distancia de cualquier otro conflicto irregular.

3) La voluntad, expresa o tácita, del actor de no desencadenar un ulterior conflicto bélico tradicional.

En el Comunicado, las altas autoridades comunitarias resaltan la importancia de aunar esfuerzos para identificar, controlar y erradicar las campañas de desinformación masivas, que generalmente impactan directamente sobre la población europea, hecho clave que generó preocupación entre todos los gobiernos en la última década, sobre todo por el accionar intimidatorio, disruptivo y ofensivo de Rusia y que motivó el accionar firme de la Unión.

El rol más importante de la Unión en este contexto está en colaborar con los Estados en concienciar no sólo sobre esta problemática y sobre cuáles son las vulnerabilidades de cada país tiene y que pueden ser atacadas, sino también

sobre cómo reforzar la resiliencia sistémica y los valores democráticos y las libertades fundamentales que acomunan a toda la Unión. En el próximo capítulo serán analizadas las medidas específicas que la UE ha implementado.

Como producto de la colaboración entre la Unión Europea y la OTAN, en 2017 se creó el Centro Europeo de Excelencia para combatir las Amenazas Híbridas, con sede en Helsinki, Finlandia. En su breve pero prolífica historia, esta institución ha contribuido a echar luz sobre este fenómeno. Desde la perspectiva de este Centro, las amenazas híbridas son:

> *Métodos y actividades que se orientan a atacar vulnerabilidades del oponente. Las vulnerabilidades pueden ser creadas de muchos modos, incluyendo la memoria histórica, la legislación, las viejas prácticas, factores geoestratégicos, gran polarización social, desventajas tecnológicas y diferencias ideológicas. Si los intereses y objetivos de un usuario de estos métodos híbridos no son alcanzados, la situación puede escalar hacia una guerra híbrida donde el rol militar y de la violencia se puede incrementar significativamente. (Centro Europeo de Excelencia para combatir las Amenazas Híbridas, s.f.).*

Las características principales que presentan las amenazas híbridas son tres:

1) la coordinación y las acciones sincronizadas, que apuntan intencionalmente contra Estados democráticos y vulnerabilidades sistémicas institucionales, a través de una amplia cantidad de medidas (políticas, económicas, militares, civiles y de información).

2) las actividades que se aprovechan de métodos que impiden la detección y atribución de responsabilidad y que se encuentran en una zona gris entre la guerra y la paz.

3) el objetivo de influir de distintos modos sobre las decisiones que se toman a nivel local, estatal o institucional a favor y/o en contra de los objetivos estratégicos del atacante mientras afecta o daña al atacado.

De esta definición se pueden destacar varios puntos interesantes. Por un lado, el fuerte rasgo dinámico y proactivo de los perpetradores de las amenazas, quienes están incansablemente monitoreando la situación en búsqueda de

nuevas vulnerabilidades y contextos beneficiosos. Este dinamismo también se evidencia en el proceso que permite distinguir, pero además hacer coincidir las amenazas con la guerra híbrida, la que sería, parafraseando a Von Clausewitz, la continuación de las amenazas híbridas por otros medios.

Por otro lado, de esta caracterización de las amenazas híbridas se evidencia la preocupación del Centro por proteger los valores de las democracias occidentales que constituyen el principal foco de ataque a nivel geopolítico global, hecho que determina la misión final de dicha institución.

3.8. LA TEORIZACIÓN MULTIDISCIPLINARIA SOBRE AMENAZAS HÍBRIDAS.

Con visión preclara sobre la importancia y necesidad de teorización que las amenazas híbridas requerían, ya en 2012, el Centro Superior de Estudios de la Defensa Nacional de España (CESEDEN, 2012) publicó un exhaustivo documento sobre los conflictos híbridos, subrayando la importancia de ofrecer un enfoque integral y multidisciplinario sobre el tema. Así, no sólo se procede a estudiar el fenómeno desde el punto de vista militar y de cooperación cívicomilitar, sino que se ilustran diversas perspectivas desde las áreas de inteligencia, política, asistencia humanitaria, cultura y gobernanza del sector de la seguridad.

Desde el punto de vista de cooperación militar, se evidencia cómo las Fuerzas Armadas de Occidente, si bien cuentan con una gran supremacía militar, presentan debilidades tanto en la conducción de operaciones de baja y media intensidad como en las tareas de estabilización y reconstrucción en escenarios de conflicto. Para mejorar ello se necesita una gran colaboración, coordinación y cohesión entre elementos civiles y militares, públicos y privados, nacionales y multinacionales al momento de encarar procesos de análisis, planeamiento y ejecución de misiones de gestión de crisis. Desde la perspectiva del Enfoque Integral, estos procesos deben ser abiertos, inclusivos, transparentes, flexibles, proactivos, ágiles. Se deberá promover una mayor cultura interna sobre las raíces del conflicto, aumentando el diálogo y creando los espacios necesarios para el liderazgo civil. Sólo de este modo se podrá tener una visión global del problema, manteniendo un compromiso a largo plazo sobre la base de una variada gama de instrumentos multidisciplinarios.

Desde el punto de vista politológico, se destaca una tendencia global a la disminución de los conflictos bélicos tradicionales. Sin embargo, se registran muchos conflictos de baja o media intensidad que son, en su mayoría, conflictos internos, sobre todo en regímenes autocráticos[61]. Todo ello configura un contexto de evolución de los conflictos armados que potencia su carácter híbrido, entendido como multidimensionales y complejos, y donde se hace difícil su adecuada prevención, gestión y solución por parte de los poderes políticos . Para lograr estos objetivos se deben redoblar los esfuerzos en ámbitos específicos de diplomacia preventiva, del cuidado y desarrollo de la sociedad civil durante las tareas de mantenimiento y refuerzo de la paz, y de las medidas de estabilización.

A nivel mundial, existe un sistema de seguridad colectiva a través de la Carta de las Naciones Unidas, que refuerza el principio de intervencionismo hegemónico de las grandes potencias a través del Consejo de Seguridad, con el objetivo final de erradicar progresivamente la conflictividad entre los países. Sin embargo, este intervencionismo hegemónico, al estar estructurado a través de los Estados, acarrea problemas a la hora de lidiar con actores no estatales, como muchas veces ocurre en los conflictos híbridos.

Por ello también es necesario replantearse el rol de los Estados, su relación con los "Estados fallidos" (failed States)[62] y con los "Estados canallas" (rogue States) [63], su responsabilidad y compromiso, su cooperación y apoyo a formas

---

[61] CESEDEN, (2012) De 365 conflictos en el 2009, sólo 31 fueron guerras, mientras que los demás fueron solo crisis, como ataques terroristas, revueltas populares, golpes de Estado, etc.

[62] CESEDEN,(2012). Los Estados fallidos son aquellos donde "no existen instituciones estatales capaces de desempeñar las funciones básicas propias de cualquier Estado, como el control de fronteras, mantenimiento del orden público, protección de los derechos humanos esenciales, etc." Estos Estados "son una de las principales causas de los conflictos híbridos intraestatales".

[63] Los Estados canallas "no sólo cuestionan o atacan abiertamente el orden internacional, sino que lo hacen apoyando y patrocinando a grupos armados irregulares (guerrillas, grupos terroristas, organizaciones criminales internacionales, etc.).

refuerzan las organizaciones institucionales intergubernamentales, supranacionales y no gubernamentales.

En el caso del rol de los medios de comunicación, se distinguen los medios propios de los beligerantes, los cuales van a tener un natural rol de parte, informando y haciendo propaganda para reforzar su propia posición, mientras los medios independientes deberían aportar información objetiva y sin manipular, algo que difícilmente ocurre. En los conflictos híbridos los medios de comunicación masiva tienen un rol relevante por el impacto comunicativo y la gran interconectividad e interdependencia de los actores involucrados.

En todo conflicto híbrido, se busca de alteración del orden de convivencia colectiva imperante, objetivo político que hace difícil una resolución negociada. Los conflictos híbridos hacen también necesaria una adecuada formación en Inteligencia, con específicas evaluaciones socioculturales y red de contactos locales, sobre todo cuando el adversario asimétrico se mimetiza con la población y se aprovecha de complejos escenarios urbanos y diferencias culturales.

En la lucha contra fuerzas insurgentes típicas de los conflictos híbridos, se necesita una especial formación, con adiestramiento y estrategias diferentes a otras formas de conflicto convencionales. En este nuevo contexto, la importancia de la ocupación del terreno es irrelevante y, por el contrario, cobra especial relevancia la necesidad de evitar bajas y daños materiales en la población civil, cuya aceptación o, al menos, no hostilidad será vital para el éxito de la misión. Asimismo, los enfrentamientos directos se vuelven escasos y aumentan los peligros por artefactos explosivos improvisados, distribuidos estratégicamente en el terreno.

Sin embargo, al carecer de una doctrina aceptada sobre la aplicación del Enfoque Integral, resulta siempre difícil determinar cuándo y cómo pasar del uso de medios pacíficos de resolución de conflictos al uso de la fuerza militar. Lo importante es tener siempre una buena estrategia de salida, sabiendo cómo grupos terroristas, organizaciones criminales internacionales, etc.) que desencadenan o refuerzan los conflictos híbridos.".

Combinar todos los recursos a disposición, que generalmente son escasos y tienen mandatos limitados o diversos por parte de sus respectivas autoridades nacionale. "El enfoque debe ser tan civil como sea posible y tan militar como sea necesario."[64]

Este conflicto entre lo militar y lo civil tiene un fuerte impacto en las implicaciones ético-jurídicas de la guerra irregular, donde los no combatientes generalmente no respetan las reglas de la guerra convencional, de los principios de proporcionalidad y discriminación entre civiles y militares, y de la moral en general. Esto puede conllevar frustración y sentimiento de indefensión en las tropas regulares y sobrecarga de responsabilidad en los mandos inferiores al momento de decidir cómo intervenir en situaciones específicas donde el enemigo quiebra todas las reglas. Todos estos factores requieren una profunda reflexión sobre los diferentes tipos de misión y qué capacidades emplear en cada contexto.

Este documento, pionero sobre la temática no sólo a nivel nacional sino también regional, pone el foco de atención en cómo la novedosa iniciativa del Enfoque Integral sirve para coordinar recursos y lograr la unidad de acción bajo mando civil frente a un contexto complejo de conflictividad híbrida. Un correcto análisis, planteamiento, conducción y evaluación de la operación, teniendo en cuenta la riqueza y necesidad de un enfoque multidisciplinario, son claves para afrontar los conflctos cada vez menos convencionales que el futuro depara[65].

[64] Jakobsen, (2012).

[65] CESEDEN, (2012) De 365 conflictos en el 2009, sólo 31 fueron guerras, mientras que los demás fueron solo crisis, como ataques terroristas, revueltas populares, golpes de Estado, etc.

-EL TERRORIMO COMO AMENAZA HIBIRIDA-

IV EL TERRORISMO COMO AMENAZA HIBRIDA

4.1 ATENTADOS YIHADISTA COMO AMENAZAS HÍBRIDAS.

En la actualidad existen muchas organizaciones terroristas que, al amparo de una interpretación errónea del islam, ejecutan secuestros, violaciones o atentados terroristas, tanto en países occidentales como en países musulmanes, sobre todo en Oriente Medio, utilizando técnicas tanto regulares como irregulares, y según el tipo de Atentado que se lleve a cabo podemos encontrar un escenario híbrido del ataque.

No a todos los grupos terroristas les mueven los mismos fines y objetivos, pero si les une un ideario común. Dentro de ese ideario común que propugnan las organizaciones terroristas de corte yihadista, hay que destacar el reclutamiento, a través de la radicalización y el adoctrinamiento del máximo número de adeptos para la causa en beneficio de los intereses de la organización.

Si bien son innumerables las organizaciones terroristas de corte yihadista que constituyen una amenaza híbrida mundial, durante los últimos años se ha destacado el desarrollo de dos modelos divergentes de militancia islamista, el de Al Qaeda y el de Daesh, organizaciones que han venido compitiendo por la primacía en el mundo del islam radical. Ambas organizaciones son muy diferentes en cuanto a las estrategias planteadas, pero ha quedado patenten que persiguen los mismos objetivos, demostrando que una manera efectiva que han sabido explotar las debilidades estructurales existentes en las sociedades musulmanas, aprovechando los vacíos de poder resultantes de la inestabilidad producida por las primaveras árabes.[66]

[66] http://www.ieee.es/Galerias/fichero/docs_analisis/2018/DIEEEA21-2018_Al_Qaeda-Daesh_IFC.pdf [consultado 5 Julio de 2018]

4.1.1 Al Qaeda.

Al Qaeda, literalmente la base, es una organización terrorista compleja y flexible con alcance trasnacional y composición multiétnica que conjuga nuevas tecnologías con fundamentalismo religioso de contenidos neosalafistas.[67]

Fue creada en 1988 por un acaudalado empresario de origen saudí llamado Osama Bin Laden, considerado como el líder indiscutible de la organización hasta Mayo de 2011, cuando fue abatido por soldados estadunidenses en la ciudad paquistaní de Abbottabad .Hasta ese momento, si bien Osama Bin Laden era considerado el líder mediático de la organización ,en la sombra se encontraba Ayman AL Zawahiri, un cirujano de origen egipcio, considerado el líder estratégico de la misma pero carente del carisma de Osama Bin Laden.

En 1998 este tipo de proclamas eran grabadas en video y audio y se distribuían entre los adeptos de la organización, entre los que se encontraban los reclutadores, que las utilizaban para llevar a cabo sus fines a la hora de llevar a cabo la radicalización a través del adoctrinamiento, hecho que hoy en día a cambiado radicalmente debido a la irrupción de las nuevas tecnologías, como veremos en el siguiente punto.

Con la muerte de Osama Bin Laden, Ayman Al Zawahiri asumió el liderazgo de la organización, conservándolo hasta el momento, aunque el gobierno de Estados Unidos posiciona como posible futuro líder del grupo terrorista a uno de los hijos de Osama, Hamza Bin Laden, casado con la hija del jefe de la célula que llevo a cabo los atentados del 11S, Mohamed ATTA.

Las amenazas vertidas por Hamza en Julio de 2016, haciendo un llamamiento a vengar la muerte de su padre en un discurso de más de 20 minutos, así como otros mensajes de audio y video en internet en los que llama a sus seguidores a lanzar atentados contra Estados Unidos y sus aliados occidentales, le han valido para engrosar la lista de los terroristas más buscados del planeta.

---

[67] Reinares, F Y Elorza, A. (2004): El nuevo terrorismo islamista del 11S al 11M. Temas de Hoy. Madrid.

La estrategia de la organización ha cambiado significativamente desde los ataques del 11S. En un principio la organización operaba desde Afganistán bajo la protección de los talibanes, pero la invasión del país por parte de Estados Unidos propició que el liderazgo central de la organización se fuera descentralizando a favor de las franquicias como Al Qaeda en el Magreb Islámico (AQMI), Al Qaeda en la Península Arábiga (AQAP), o de los grupos terrorista que le han mostrado lealtad.

El objetivo estratégico último de Al Qaeda sigue siendo, a largo plazo, establecer un califato global compuesto por muchos emiratos islámicos locales, que actúan en forma de franquicias, a través de una acción continua de propaganda complementada con atentados terroristas.

A lo largo de su historia Al Qaeda, ha reivindicado innumerables atentados cometidos en diversas partes del mundo, en ocasiones planeados directamente por el grupo terrorista y ejecutados por células estructuradas y en otras llevados a cabo por actores solitarios, reclutados y radicalizados por la organización o autorradicalizados a través de las redes sociales y que posteriormente le han mostrado lealtad.

Atentados relevantes cometidos por la organización:

- 7 de agosto de 1998 ataques a la Embajadas de EEUU de Kenia y Tanzania.
- 11 de septiembre de 2001, Atentados en New York y el Pentágono y otro avión que cayó en Pensilvania.
- 11 de marzo de 2004, atentados en trenes de cercanías en Madrid.
- 7 de Julio de 2005, atentados en metro y autobús en Londres.

Con estos atentados Al Qaeda se consolidó como la amenaza internacional más peligrosa del momento, hasta la aparición del denominado Estado Islámico.

El atentado de Charlie Hebdo el 7 de enero de 2015 llegó en un momento en el que la organización llevaba tiempo sin cometer atentados de envergadura en Europa y su actividad se había visto eclipsada por la irrupción en el plano internacional del Estado Islámico, que si bien en un principio compartían idéales e incluso acciones, dejaron de hacerlo cuando el Estado Islámico se enfrentó al Frente Al Nusra, filiar de Al Qaeda en Siria, haciendo caso omiso a las indicación

de la matriz de Al Qaeda e irrumpiendo como una apisonadora en Siria ganando terreno a base de salvajes atentados y acciones indiscriminadas contra civiles, hecho con el que Al Qaeda no estaba de acuerdo y así lo manifestó anunciando la separación definitiva.

4.1.2. Daesh.

Daesh, Estado Islámico, Estado Islámico de Irak y Siria, ISI, Estado Islámico de Irak y Levante (ISIS) o cualquier forma con la que es conocido o autodenominado este grupo terrorista, que nació en Junio de 2014, cuando Muhammad Al Adnani, mediante un comunicado, proclamaba el Califato y días después Abu Bakr Al-Baghdadi lo hace efectivo en una aparición pública en la desaparecida Mezquita de Mosul y se autoproclama califa Ibrahim, pero ya desde años atrás la organización fue constituyéndose debido a las intenciones de Abu Musab al Zarqawiq, que bajo la militancia de Al Qaeda, ya soñaba con dirigir un califato en base a un reconstruido ejército de combatientes islamistas en Irak.

La salida de Irak de la coalición internacional en el año 2011, supuso para la hoy, organización terrorista Daesh, una oportunidad de expansión rápida, que le llevaría en poco tiempo a construir un ejército con convictos y excombatientes que a través de un fanatismo salafista extremista y en base a una actuación concentrada en el terror, se expandió en poco tiempo por todo Irak, utilizando la estructura de Jabhat Fateh al-Sham y la inestabilidad del país de la vecina Siria, llegando a establecerse por la fuerza en parte de las grandes ciudades de ambos países, estableciendo así los deseos de formar el autoproclamado califato.

El denominado como Estado Islámico, cuyo acrónimo en árabe es Daesh, hoy se contempla como un fenómeno trasnacional, que ha sido capaz de evolucionar de un fenómeno interior comarcal a un fenómeno global con capacidad para influir en las políticas occidentales, llegando en su punto más álgido, a obtener una gran posición en la zona de Oriente Medio.

Este grupo terrorista sin lugar a dudas señala elementos y objetivos desfasados, pero, sin embargo, su estrategia y procesos le han llevado a ser un fenómeno global con influencia socioeconómica mundial. Dentro de esas estrategias, la comunicación es uno de los elementos que hacen que del Estado Islámico un fenómeno moderno, especializado y capaz de autoabastecerse y

autofinanciarse, señalando a la organización terrorista como una organización muy similar a un Estado y que, unido a su asimetría y a su ideología salafista, donde el terror y la violencia imperan como señas de identidad, la convierten en la organización terrorista más peligrosa del momento.

Su red de financiación, su reclutamiento utilizando la comunicación global y la difusión globalizada, son elementos de la organización que la hacen camaleónica y difusa a los elementos de protección, pero a la vez, mutable a las vicisitudes operativas de la guerra sobre el terreno.

Esta organización terrorista busca afincarse en países árabes, en los que el conflicto interno permite introducir sus enormes tentáculos, como ha quedado patente en Siria e Irak y cómo está empezando a ocurrir en Libia o Yemen, intentando así establecer un califato que aspira a ser el elemento común predominante y vertebrador del mundo musulmán, como ente de referencia económica, política y social, ensalzando aquellos sentimientos antioccidentales de aquellos musulmanes radicalizados dentro y fuera de su área geográfica de influencia.

La comunicación es un elemento esencial para el desarrollo y supervivencia de la organización terrorista, que unido a la vinculación histórica del tratamiento informativo del terror y del efecto multiplicador de las acciones teóricas que la comunicación actual efectúa, sitúa la política de comunicación de este grupo terrorista a la cabeza de sus procesos estratégicos presentes y futuros.

Varias son las estrategias que esta organización ha desarrollado desde sus inicios, haciendo llamamientos para que se unan a sus filas el máximo número de personas posible en zona de conflicto y en otras ocasiones haciendo llamamientos para que los individuos que le han mostrado lealtad atenten en cualquier tiempo y lugar aprovechando cualquier circunstancia. Tal es así que Abu Mohammad Al Adnani, portavoz del Estado Islámico, su jefe de operaciones y mano derecha de Abu Bakr Al Baghdadi ha lanzado varias misivas, ofreciendo alternativas a todos aquellos que no han podido llegar a su deseado califato con el fin de atentar en cualquier tiempo y lugar y aprovechando cualquier circunstancia.

El 22 de septiembre de 2014 lanzó el siguiente comunicado:

"Si no eres capaz de encontrar una bala o un dispositivo explosivo improvisado (IED), entonces selecciona al impío americano, francés o cualquiera de sus aliados, golpéale la cabeza con una roca, asesínale con un cuchillo, atropéllale con tu vehículo, tírale desde un lugar elevado, estrangúlale o envenénale"

Pero éste no ha sido el único comunicado que ha lanzado, el 21 de mayo de 2016 mediante un audio publicado en el medio londinense Al Furqam, decía lo siguiente:

"Nos dirigimos especialmente a los soldados del Califato en Europa y en los Estados Unidos"

"El acto más pequeño que haréis en sus tierras será más perjudicial y más deseado que un gran acto cometido con nosotros en Sham (Siria). Si alguno de vosotros está deseando llegar al Estado Islámico, sabed que hay otro que está en el E.I y que desea estar en vuestro lugar para atacar a los cruzados día y noche, asustarles y aterrorizarles hasta sembrar el miedo incluso entre los mismos vecinos. Si no podéis actuar, pues lanzar piedras contra el cruzado en su propia casa. No hay que subestimar ninguna acción, ya que sus consecuencias son grandes para los muyahidines y sus efectos son enormes para los infieles…"

Al igual que Al Qaeda, el Estado Islámico, desde su reciente creación, ha reivindicado innumerables atentados cometidos en diversas partes del mundo, en ocasiones planeados directamente por el grupo terrorista y ejecutados por células estructuradas y en otras llevados a cabo por actores solitarios, reclutados y radicalizados por la organización o autor radicalizados a través de las redes sociales y alentados por misivas como las expuestas en líneas anteriores, mostrando así lealtad a la organización.

El Estado Islámico no solo ha cometido atentados en Europa y Estados Unidos, sino que la mayoría de sus atentados han sido cometidos en Irak y Siria contra la población civil o contra todos aquellos que les han combatido sobre el terreno, atentados crueles y violentos al encontrarse dentro de su ámbito de actuación.

Fuera de sus dominios territoriales han reivindicado los siguientes atentados, hecho que reafirma el calado del mensaje en ciertos actores solitarios, ya que algunos de estos atentados han sido cometidos por personas autorradicalizadas y otros por células perfectamente estructuradas a las órdenes de esta organización terrorista:

- Atentado contra Charlie Hebdo, París, Francia, el 7 de enero de 2015. Método utilizado arma de fuego.
- Atentado en París el 13 de noviembre de 2015.París, Francia. Sala Bataclan. Método utilizado arma de fuego.
- Ataques en el aeropuerto de Bruselas, Bélgica y en el metro de Maalbeek. Método utilizado explosivos.
- Atentado en la discoteca "PULSE" en Orlando, Estados Unidos el 12 de junio de 2016. Método utilizado armas de fuego.
- Atentado en Niza, Francia el 14 de Julio de 2016. Método utilizado atropello masivo con camión.
- Atentado en Kabul, Afganistán, el 23 de Julio de 2016. Método empleado explosivo.
- Atentado de Manchester, Reino Unido, el 22 de mayo de 2017 cuando se celebraba un concierto de música en el "Manchester Arena". Método empleado explosivo.
- Atentado en Barcelona y Cambrills, España el 17 y 18 de agosto de 2017. Método utilizado atropello masivo con furgoneta y acuchillamiento con arma blanca.
- Atentado en New York, Estados Unidos, el 13 de octubre de 2017. Método utilizado atropello masivo con furgoneta.

Como se puede ver en la ilustración queda patente la presencia de ambas

organizaciones terroristas en África y Oriente Medio[68].

Fuente: https://www.bbc.com/mundo/noticias-internacional-48214543.

[68] https://www.bbc.com/mundo/noticias-internacional-48214543. [consultado 15 de junio de 2019]

4.1.3 El yihadismo radical como amenaza a la seguridad Global.

No son pocos los Estados que han incluido en sus Estrategias de Seguridad Nacional el radicalismo violento como una amenaza híbrida seria a su orden democrático y su modo de vida.

Es innegable que el terrorismo de corte yihadista proyecta su ideología radical y actúa a nivel global, incluyendo Europa donde en los últimos años ha golpeado duramente en forma de atentados de toda clase.

El radicalismo violento forma parte de las amenazas que han adquirido mayor relevancia en todo el planeta en los últimos años, no solo por la ideología, sino también por que dicha radicalización es el paso previo a que los individuos radicalizados acaben integrándose en bandas armadas o terroristas y terminen cometiendo atentados en cualquier parte del planeta.

El terrorismo sigue castigando de forma ininterrumpida muchas regiones del mundo y entre ellas se encuentra occidente. En los últimos años las organizaciones terroristas han concentrado sus mortíferos ataques contra una población concreta, occidentales, musulmanes chiíes o cristianos en países árabes. La irrupción de esta amenaza desde la plataforma del radicalismo violento ha conmocionado las conciencias del mundo occidental y a grandes rasgos ha puesto en jaque los modelos de seguridad de dicho Estados.

El terrorismo de corte yihadista en la actualidad se mantiene en cotas mucho más altas que en tiempos anteriores a los ataques en New York del World Trade Center o del Pentágono, ataques que hicieron cambiar el mundo en muchos aspectos, entre los que principalmente se encuentra la seguridad, siendo el terrorismo traducido en radicalización violenta, catalogado por muchos Estados como uno de los principales elementos de desestabilización social.

Aunque se podría decir que el mundo occidental es la zona más segura del planeta, también es cierto que, respecto a otras partes del mundo, en los últimos años el terrorismo ha golpeado a occidente con más frecuencia que en otros lugares. A este respecto el año 2015 fue un año nefasto para la seguridad en Europa y sobre todo para Francia donde se cometieron los terribles ataques contra Charlie Hedbo, ataque contra una Policía Municipal en Montrouge, ataque contra un supermercado de comida Kosher, ataque contra la sala Bataclan cuando se

estaba celebrando un concierto, ataques indiscriminados con armas de fuego en zonas de ocio, explosión en las inmediaciones del Estadio de futbol de Francia, ataques que pusieron en jaque la seguridad de los ciudadanos llevando estos últimos, el 13 de Noviembre, a declarar por parte del presidente de la República, el Estado de Emergencia.

El proceso de radicalización en el ámbito del terrorismo yihadista ha sido tema de estudio de múltiples eruditos en la materia y si bien muchos de ellos coinciden en que un proceso de radicalización puede ser interrumpido o que no todas las personas radicalizadas dan el paso a la violencia, esta circunstancia no contrarresta el hecho de que otras personas se radicalicen, tomen el camino de la violencia y cometan atentados.

Es evidente que la radicalización violenta influye de manera directa en la seguridad global. Como se ha visto a lo largo de estas páginas, la captación y posterior adoctrinamiento en diferentes entornos, en la línea de la ideología extremista neo salafista, tiene unos propósitos concretos, inculcar al radicalizado el odio hacia occidente hacia sus costumbres y hacia todo aquel que consideran un mal musulmán.

El hecho de que el individuo radicalizado acabe cometiendo hechos violentos, en ocasiones depende mucho de las posibilidades que tenga para hacerlo, aunque en los tiempos que corren, como se ha visto, se puede atentar de muchas maneras, no hacen falta armas o explosivos.

Hoy en día, se puede decir que existe una amenaza global, sobre todo en occidente que proviene principalmente de actores radicalizados como:

1. Yihadistas retornados de zonas de conflicto. Denominados “Foreing Fighters”. Estas personas en un principio son consideradas como una amenaza real si bien hay algunos de ellos aparentemente muy decepcionados con la causa por la que han luchado, tras sumergirse en el

seno del Estado Islámico, hay otros que tal vez quieran continuar con la lucha en sus países de origen, hecho que no sería sorprendente.[69]

2. Células locales o actores solitarios radicalizados. Cuando se habla de células locales hay que referirse a aquellas células que se crean en un ambiente local por un grupo de personas que se radicalizan o que uno de ellos valiéndose de su posición radicaliza a otros. El ejemplo perfecto de una célula local es la célula de Ripoll, que acabo cometiendo lo atentados de Barcelona y Cambrills en agosto de 2017. En cuanto a los actores solitarios, esta figura se denomina así por su autorradicalización y autoadoctrinamiento, llegando a la autoconvencimiento para la comisión de atentados. Esta figura es muy difícil de detectar porque su naturaleza aislada, dificulta que las Fuerzas y Cuerpos de Seguridad puedan recopilar información sobre ellos y sus intenciones. Un ejemplo de actor solitario que comete un atentado de gran envergadura es el de Mohamed Lahouaiej Bouhlel, residente en Francia y de origen tunecino, que la noche del 14 de julio de 2016 a bordo de un camión de gran tonelaje, arrolló a una multitud de gente en el paseo de Niza (Francia), causando la muerte a 86 personas e hiriendo a 434.

3. Células pertenecientes a Daesh, a Al Qaeda en el Magreb Islámico o en la Península Arábiga. Si hablamos de estas células en un entorno occidental, hay que referirse a aquellas células durmientes pertenecientes principalmente a estas organizaciones terroristas y que se encuentran ocultas a la espera de instrucciones. Aunque no es descartable, es difícil que estas células se mantengan con una estructura férrea en disposición de atentar a día de hoy, motivado por el gran control que se lleva por parte de las Fuerzas y Cuerpos de Seguridad y los Servicios de Inteligencia de determinados individuos ya fichados. Esto no quiere decir que no las haya, lo que quiere decir es que el efecto terrorista muta en función de los golpes que se les asesta, por lo que mantener una organización estructurada y con una logística adecuada, por ejemplo, en Europa, es

[69] https://www.politicaexterior.com/articulos/afkar-ideas/foreign-fighters-europeos realidades-y-retos/ [consultado 16 junio de 2018]

complicado sin ser detectados por las Fuerzas de Seguridad de los Estados. Un ejemplo de estas células fue sin duda los ataques de París del 13 de noviembre en la sala Bataclan, el estadio de futbol de Francia y contra zonas de ocio. Varios de sus autores habían viajado en el año 2013 a Siria y de vuelta había logrado burlar todos los controles de seguridad e instalarse en Francia, alguno de ellos en el barrio parisino de Saint-Denis.

4. Yihadistas liberados de prisión. Se trata de individuos que han salido de prisión tras cumplir condena por encontrarse relacionados con actividades terroristas de corte yihadista, ya sea por pertenencia a banda armada, por colaboración con esta o por llevar a cabo labores de enaltecimiento del terrorismo, captación, reclutamiento y adoctrinamiento. Si bien la principal función de los centros penitenciarios es la reinserción, las estadísticas demuestran y como ya se ha expuesto en el punto 2.1.3 del presente trabajo, que la cárcel lejos de ser un lugar donde reinsertarse es un lugar en el que no solo se reinsertan, sino que se reafirman en sus ideas e intentan radicalizar a otros internos. De ahí que no se considere únicamente una amenaza a aquellos yihadistas que salen de prisión por condenas relacionadas con actividades terroristas, sino que también se consideran una amenaza a aquellos presos que entraron en prisión por la comisión de delitos comunes y que durante su estancia en prisión se han radicalizado. Son muchos ejemplos los que se pueden poner al respecto. En cuanto a yihadistas que salen de prisión y que lejos de reinsertarse en la sociedad, demuestran ser una amenaza para la misma sumándose o liderando otras células yihadistas se podría hablar de Lahcen Ikassrien, preso en la cárcel de Guantánamo, extraditado a España para ser juzgado por la Audiencia Nacional y una vez en libertad aprovecha para liderar una célula yihadista que había mandado combatientes a Irak y Siria, hechos por los que volvió a ser detenido. En cuanto a la segunda figura, individuo radicalizado en prisión que una vez que sale comete un atentado, es significativo el caso de Benjamin Herman, un joven belga, delincuente común que entra varias veces en prisión, lugar donde se radicaliza. En su última salida de prisión días después comete un atentado en Lieja (Bélgica), donde espera a la salida de una cafetería dos agentes de policía, tras atacarles por la espalda con un cuchillo las quita el arma y las

remata en el suelo con sus propias armas, posteriormente abate a tiros a un joven que se encuentra en el interior de un vehículo, hecho que intenta repetir hasta que es abatido por la policía.

Todas y cada una de las circunstancias descritas son elementos que ponen en jaque la seguridad global. Como se ha visto en alguno de los ejemplos descritos, la radicalización violenta y todo su proceso puede ser considerada como una amenaza factible y real a la seguridad global a corto, medio y largo plazo. El individuo que ha sufrido un proceso de radicalización puede o no puede pasar a la acción, pero esa circunstancia no deja de estar latente en su interior y cualquier frustración, sentimiento o animación por parte de otros agentes puede hacer saltar la chispa que le haga pasar línea.

4.2 ESTRATEGAS DE CAPTACIÓN Y COMUNICACIÓN DESTINADOS A ADOCTRINAMIENTO Y CAPTACIÓN.

4.2.1. Uso de las nuevas técnicas de comunicación TIC´s

Las organizaciones terroristas tienen la necesidad de trasmitir su mensaje, el cual de una manera general y sencilla tiene dos objetivos. El primero difundir el miedo y el pánico hacia todas las personas que no piensan como ellos, y el segundo el de captar adeptos para mantener la lucha viva en todas sus vertientes.

A principios de este siglo las organizaciones terroristas como Al Qaeda procuraban asegurarse que los atentados terroristas quedasen grabados para luego poder difundirlos por los medios de comunicación a parte de utilizarlos para la propagan que se encargaban de difundir entre aquellos adeptos a los que pretendían que se alistasen en sus filas. Indudablemente con el paso del tiempo todo evoluciona y aunque el mensaje es el mismo, a manera de difundirlo ha mejorado de una manera alarmante. Anteriormente la propaganda yihadista se distribuía de manera clandestina por los reclutadores siendo el modus operandi en la distribución de la misma el contacto personal entre reclutadores e individuos a los que se pretendía captar. La aportación de los medios de comunicación a este respecto era prácticamente nula y éstos solo daban voz a las

organizaciones terroristas cuando se cometían atentados con graves consecuencias y durante los días siguientes, posteriormente los mismos caían en el olvido.

Con este sistema, el mensaje que distribuían las organizaciones terroristas a través de sus estructuras de captación y propaganda calaban en determinadas personas muy concretas ya que el elemento fundamental de este sistema era el contacto de persona a persona.

Con las llegadas de las nuevas tecnologías todo ha cambiado, hoy en día se puede consumir propaganda yihadista, videos de atentados, ejecuciones y cualquier misiva promovida contra lo que ellos denominan infieles o impíos, desde el sillón de casa con un ordenador desde cualquier lugar del mundo con un teléfono móvil. Este hecho hace que cambien totalmente las reglas del juego, ya que antes distribuir la propaganda, videos, etc, tenía que ser prácticamente de persona a persona y la misma llegaba a un grupo muy reducido de individuos. De esta manera con un "click", el mensaje puede llegar millones de personas en cuestión de segundos en cualquier punto del planeta.

Por ser las dos organizaciones que ofrecen una mayor amenaza a la seguridad global vamos a analizar las estrategias de comunicación de Al Qaeda y más en profundidad la de reciente Daesh, que ha sido un revolución sin precedentes en el denominado ciberterrorismo Ya en el año 2005 Ayman Al Zawahiri, actual líder de Al Qaeda, tenía claro que una parte de la batalla que pretendía librar, la tenía que ganar con la ayuda de los medios de comunicación, que eran quien les daban voz a sus acciones. En sus declaraciones argumentaba que la batalla en los medios de comunicación se libraba para ganar mentes y los corazones de los miembros de la UMMA.

Desde comienzos del siglo XXI, Al Qaeda puso en marcha una campaña de comunicación digital destinada a la elaboración de productos de comunicación con cierta calidad audiovisual y personalizada para distintas audiencias distribuidos en gran medida a través de internet.

Entre su estrategia de comunicación se encuentra la publicación de una revista, llamada "Inspire", cuyo primer número salió en junio de 2010 con el claro fin de socializar su mensaje entre los más jóvenes. Esta revista permitía trasmitir directamente el mensaje a sus receptores sin intermediarios. Evidentemente con la

impresión de la revista, la organización controlaba el enfoque que utilizan para impactar a la audiencia.

Sin embargo, la estrategia comunicativa de Al Qaeda planteaba dos importantes limitaciones, que se detallan a continuación:

1. La comunicación solo se ejerce de manera unidireccional. Se publicaba el material y tenían que ser los usuarios los que accedan a su contenido que se encuentra publicado en páginas web propias.

2. El mensaje se encuentra condicionado por la escasa variedad de temas en sus narrativas, que giraban en torno a dos vertientes, a la justificación de la violencia en base a la interpretación errónea del Corán y al victimismo frente a occidente en su lectura sobre la opresión que sufren los musulmanes frente a éstos.[70]

En cuanto a Daesh, es importante remarcar que esta organización terrorista cuenta con una estructura de comunicación muy poderosa convertida en poco tiempo como uno de sus puntos estratégicos, diseñada para alcanzar a toda una potencial población tanto en el territorio que domina físicamente como en cualquier otra parte del mundo. La estructura de la organización alcanza diferentes medios y vías de difusión que van desde las octavillas y publicaciones impresas locales, a potentes herramientas relacionadas con la difusión a través de las redes sociales e Internet, que hoy en día, se ha convertido en el principal vector de radicalización y elemento de conversión y adoctrinamiento de la organización terrorista.

Conforme a los propios datos ofrecidos por el propio Estado Islámico, en el año 2017 se han lanzado más de 41200 mensajes con diferente contenido multimedia y escrito, sirviéndose para ello de 46 agencias de información y productoras, así como más de 1000 puntos de acceso a la información.[71]

---

[70] http://theconversation.com/terroristas-en-la-red-el-modelo-de-comunicacion-digital-que-hace-temblar-las-democracias-116443. [consultado 15 de mayo de 2019]

[71] Martín, M. Á. B. (2017). La estrategia del DAESH a través de su revista Dabiq. bie3: Boletín IEEE, (7), 338-353.

Desde la aparición del Estado Islámico, diferentes han sido sus grandes elementos de confección de su política de comunicación, la fundación Al Furqan en 2007 como proceso inicial de comunicación convencional, el media center denominado AL Hayat31, año 2013, supuso una evolución en la política exterior de comunicación del Estado Islámico y que entre otras líneas editoriales es responsable de la revista Dabiq[72] y Rumiyah[73] (Primera publicación en septiembre de 2016), pero además es propietaria de diferentes medios de comunicación editados desde el ámbito de influencia del Estado Islámico y que tienen como objetivos fundamentales el reclutamiento y propaganda, principalmente en zonas territoriales alejadas del control del ésta organización terrorista.

Este aparato difusión que se controla directamente desde la jerarquía superior del Califato, está ganando la guerra mediática a todo el mundo y posibilita, a través de toda una red de elementos tecnológicos, la trasmisión y difusión de las ideas de la organización terrorista, utilizando las redes informales o programas no convencionales vinculados a redes sociales secundarias, a las cuales tienen acceso los sujetos más vulnerables de la sociedad y principales objetivo del Estado Islámico,[74] sin olvidar el efecto multiplicador y eco que sus acciones de terror tienen por medio de las redes sociales convencionales y medios de comunicación de todo el mundo.

En cuanto a las formas de propagación del terror y del odio por parte del EI, hay que destacar la proliferación del uso de internet, además de suponer una revolución mundial en su aparición, es un elemento de comunicación global que permite la interconexión instantánea, fácil y a bajo coste de diferentes puntos simultáneamente, lo que hace que sea el canal preferido por las organizaciones terroristas para la propagación de su mensaje.

---

[72] Liang, C. S. (2015). Cyber Jihad: understanding and countering Islamic State propaganda. GSCP Policy Paper, (2), 4.by TAPSTRI Media.

[73] Wignell, P., Tan, S., O'Halloran, K. L., & Lange, R. (2017). A mixed methods empirical examination of changes in emphasis and style in the extremist magazines Dabiq and Rumiyah. Perspectives on Terrorism, 11(2), 2-20.

[74] Droogan, J., & Peattie, S. (2017). Mapping the thematic landscape of Dabiq magazine. Australian Journal of International Affairs, 71(6), 591-620.

Dentro de esta actividad global de comunicación a través de internet, hay que destacar dos elementos esenciales que fomentan su utilización por parte de las organizaciones terroristas. La primera de ellas es el anonimato de la Web, bien a través de la conocida Darkweb o bien utilizando sistemas de evasión de identificación, falsos servidores fantasmas o simplemente utilizando espacios territoriales e Estados fallidos como soportes de la propagación del terror, lo que dificulta sobremanera la identificación de los autores y la lucha en general contra el fenómeno por el anonimato y asimetría de las acciones.

Esta proliferación de capacidad de difusión del Estado Islámico en internet ha sido señala por los servicios de inteligencia de medio mundo como uno de los principales riesgos de la organización terrorista y uno de los elementos que le otorga proyección internacional, ya que obtiene captación internacional de militantes, publicidad global en el mensaje del terror.

En este contexto hay que indicar la intensa proliferación de los espacios webs dedicados a la propaganda del Estado Islámico, así como la numerosa actividad en redes sociales de simpatizantes y personas afines, observando diversas manifestaciones que en la actualidad, así se han monitorizado más de 2000 elementos extremistas en más de 52 plataformas, 46 cuentas Twiter relacionadas con el terrorismo yihadista de Daesh o numerosas publicaciones, llegando el Estado Islámico a captar a 35000 potenciales terroristas a través de ellas 35, lo que lleva a pensar, por sus adeptos y por los propios servicios de seguridad, de la existencia de un supuesto cibercalifato que trabaja para crear nuevas redes sociales paralelas ocultas para los servicios de inteligencia y la policía.36

La evolución de Daesh con respecto a Al Qaeda es específica y significativa, pasando de elementos de comunicación tradicionales a sistemas novedosos y tecnológicamente avanzados, pasando de videos en medios de comunicación y comunicados tradicionales en medios escritos, a toda una acción coordinada y estratégica de comunicación que utiliza las redes sociales y elementos ocultos, pasando e medios convencionales como la televisión o la radio y prensa a canalizar todos sus esfuerzos a través de internet, pasando de escenografías clásicas terroristas a elementos que conjugan terror y composiciones multimedia de vanguardia y del anonimato a la creación de héroes, así la

propaganda del Estado Islámico, como su marca, multiplica sus efectos de captación y atrae a simpatizantes de todos los países del mundo.

Se puede decir que Daesh utiliza todas las formas y plataformas de comunicación social existentes, Twiter, You Tube, Instagram, Telegram, Flickr o Facebook, pero además cuenta con revistas tradicionales, productoras, agencias de publicidad, radios y televisiones afines, además de las aplicaciones y foros de comunicación, así como formas tradicionales de comunicación como carteles u octavillas, modulando su mensaje en cada uno de ellos y cuidando esa comunicación para que la misma, cale en el interior del público al que va dirigido, o lo que es lo mismo, el Estado Islámico dentro de su política y forma de comunicación, utiliza en cada momento el medio y el mensaje apropiado y adecuado para el objetivo o público y propósito con el que se dirige.

En este sentido Daesh utiliza diferentes métodos de comunicación en función si el mensaje va dirigido fuera del territorio que domina o dentro del mismo. En muchas ocasiones el mensaje venera y ensalza la nueva forma de vivir islámica que defiende el ideario tradicional y a sus dirigentes, para ello, además de medios de comunicación locales, utilizan cartelería y octavillas que reparten en los puntos sociales de la ciudad como mercados o mezquitas. Por el contrario, fuera de su territorio, es internet el principal medio de propaganda, captación y exaltación del Califato, utilizando, ya no el lenguaje local sino el inglés, francés o incluso castellano conjugando un mensaje simple con grandes alardes multimedia como vías de difusión de las grandezas de su forma de vivir y de su guerra santa.

La estrategia de comunicación de esta organización terrorista está orientada al más vulnerable y débil, con el objetivo de engrandecer su odio a occidente y de radicalizarlo, además de dar publicidad a su causa, pero, sobre todo, justificarla y legitimarla. Toda estrategia de comunicación tiene como objetivo a los más jóvenes, a los cuales, se les presenta la yihad y su forma de vida como atractiva y plena dentro de su interpretación religiosa, pero a la vez le hacen crecer en su extremismo interno con un planificado y cuidado discurso de odio.

Daesh, además de utilizar la comunicación como un elemento de captación y propaganda, pretende crear un clima de miedo y desconfianza a lo desconocido en occidente, hacer que los ciudadanos tengan terror y no confíen en sus instituciones como elementos de seguridad. Para ello este grupo terrorista

utiliza la nueva era digital y la sociedad global de la información, alimentando su discurso y mensajes a través de todas las vías a su alcance. En este contexto de expansión, que muchos han denominado "cibercalifato", los servicios de seguridad e inteligencia de los diferentes Estados, tienen que observar con cuidado y preocupación el fenómeno, bloqueando el avance del mensaje de odio y radicalismo violento y actuando de manera coordinada, incluyendo la colaboración de diferentes operadoras de servicio, como vía de éxito en la lucha contra esa cuidada estrategia de comunicación y propaganda.

4.2.2. Lugares de captación y adoctrinamiento.

Sin ser un hecho concluyente, se puede decir que existen principalmente dos vías para afrontar los procesos de radicalización, en primer lugar se podría hablar de una radicalización estructurada, en la que cada individuo dentro del grupo tiene su rol y cuentan con la figura carismática de un líder que puede ser o no el reclutador y otra en la que el individuo, de una manera individual, busca aquellos mecanismo que activen su inquietudes respecto a una ideología neosalafista, llegando así, al amparo de su propia justificación a autorradicalizarse.

Si buscamos el significado de la palabra reclutar o adoctrinar, encontraremos que la primera significa "reunir gente para un propósito determinado" y la segunda "inculcar a alguien determinadas ideas o creencias a otras personas". En el contexto yihadista la finalidad del reclutamiento y el adoctrinamiento es sin duda, la de reunir personas con el propósito de inculcarles la ideología radical y en algunos casos instruirlos en una radicalización con finalidades u objetivos violentos como pueden ser la comisión de atentados.

La inestabilidad en los territorios de Siria e Irak y la creación del organización terrorista, autodenominada Estado Islámico, grupo terrorista cuyo objetivo inicial es el de conformar un Estado bajo el cual deben vivir todos los musulmanes, y la proclamación de un califato, que les permita a sus miembros emprender una yihad ofensiva contra todas las naciones que se opongan de alguna manera a su proyecto mundial, para que en el planeta solo exista religión que ellos consideran verdadera, el Islam. Esta circunstancia ha elevado exponencialmente el número de captación y reclutamiento de personas por parte de este grupo terrorista atraídos por su ideal, aunque si bien es cierto que la

captación sobre el terreno en muchas de las ciudades que han arrasado se ha realizado bajo la amenaza y la coacción, ejerciendo la violencia brutal y desmedida contra quien no se unía a sus filas.

Como ya se ha dicho a raíz de este conflicto bélico, se ha observado un cambio en los mecanismos de captación de las personas proyectado sobre las campañas de comunicación lanzadas por este grupo terrorista aumentando sobremanera la captación, reclutamiento y posterior adoctrinamiento de muchos jóvenes en todo el planeta, pero principalmente de jóvenes occidentales y concretamente mujeres y hombres del continente europeo.

A este respecto destacar que el Estado islámico ha basado el reclutamiento militar en una intensa campaña de comunicación, que incluye videos escalofriantes que publican en sus páginas acompañados de largas justificaciones religiosas e históricas. Aunque parezca increíble, muchos jóvenes musulmanes, incluidos aquellos que viven y que incluso ya han nacido en occidente, se fascinan con ellos, pues la violencia proyecta poder y unas perspectivas muy diferentes de la desesperanza que los agobia por faltas de oportunidades y empleo. También reciben por las redes sociales un adoctrinamiento personalizado, constante y muy eficaz, que los conduce a radicalizarse rápida e irrevocablemente. Y lo cierto es que en esos documentos y en esos corresponsales muchos jóvenes desencantados con una sociedad que no les ofrece futuro encuentran respuestas sencillas a preguntas complejas. Solo tienen que entregarse totalmente a un orden religioso que les garantiza el paraíso.[75]

Si bien es cierto que el reclutamiento y adoctrinamiento se efectuará en un porcentaje muy elevado por terceras personas hacía uno o varios individuos, ya sea en persona o a través de campañas de comunicación divulgadas en las redes sociales, hay que tener en cuenta que existe la figura del autoradicalizado. Este tipo de individuos/as suele llegar al autoadoctrinamiento y autoconvencimiento a través de las redes sociales y de la propaganda yihadista que se esgrime de manera imparable a través de las nuevas tecnologías, hecho que será tratado en otro punto.

---

[75] https://www.semana.com/mundo/articulo/estado-islamico-como-llego-ser-tan grande/450566-3. [consultado 16 de mayo de 2019]

Este tipo de personas, una vez radicalizadas, es habitual que ejerza su actividad de apología del terrorismo, captación y adoctrinamiento a otras personas por el mismo medio en el que se radicalizó, mediante las redes sociales o las aplicaciones de telefonía móvil como whatsapp o telegram.

En cuanto a los entornos donde se suele producir la captación, reclutamiento y adoctrinamiento de las personas, si bien éstos son muy diversos, los mismos se producen dentro de las circunstancias ya enumeradas en este punto, por individuos, o grupos de individuos con la figura de un líder carismático, o través de las redes sociales no descartando la ya mencionada figura del autorradicalizado. Respecto a donde se llevan a cabo, es evidente que el captador o reclutador busca entornos que conoce y en los que se desenvuelve con soltura asegurándose un acceso directo o indirecto a través de terceras personas a la persona a la que pretende captar.

4.3 ENCLAVES YIHADISTAS

Si analizamos en contienen europeo observamos que debemos hacer frente a numerosos desafíos que amenazan la estabilidad de los países y que se convierten en factores potenciadores de amenazas híbridas como por ejemplo el terrorismo yihadista.

Si bien es cierto que, desde la eclosión y expansión de la tercera ola de la yihad, caracterizada principalmente por la falta de jerarquía y la movilización yihadista que he ha producido nivel individual, en cierta medida los países de Occidente han conseguido mitigar la amenaza terrorista a través de una serie de esfuerzos conjuntos y han elaborado varias estrategias en materia de terrorismo. A pesar de ello, factores como las crisis humanitarias, el auge de los nacionalismos y el creciente rechazo a la religión islámica gravemente perjudicada a consecuencia de los últimos atentados llevados a cabo por los conocidos “lobos solitarios”; han propiciado la emergencia de los denominados enclaves yihadistas o como algunos autores denominan «no-go zones». -estos enclaves se llevan a cabo principalmente barrios fuera del control policial donde residen mayoritariamente musulmanes y que aplicando de forma ilícita sus propias leyes se convierten en terreno abonado para la radicalización, un foco donde aparecen muchos lobos solitarios.

Mustafa Setmarian, en su obra «Llamada a la Resistencia Islámica Global», definió los enclaves yihadistas como la «aglomeración de la población musulmana en determinados barrios, convertidos en guetos fortaleza, bajo el dominio del islam». Según el ideólogo yihadista, la emergencia y consolidación de estos enclaves marcaría el precedente para la «guerra total» contra Occidente.

Este tipo de enclaves no es algo novedoso si analizamos la historia y el surgimiento de guetos y barrios marginales, ya que su aparición se ha debido a los diferentes factores sociales, económicos y culturales vinculados con la delincuencia, la pobreza y la delincuencia organizada. No obstante, en los últimos años, en la zona europea se está presenciando la proliferación de estos tipos de barrios marginales principalmente bajo la influencia de agentes y estructuras islamistas radicales que han conseguido imponer un orden social y religioso fundamentalista, evadiendo la ley nacional y el control de las autoridades.

Luis De la Corte Ibáñez, experto en terrorismo internacional, en uno de sus libros, titulado « ¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla», hace referencia a una serie de factores que han podido potenciar la penetración del terrorismo en localidades o «micro-entornos» europeos, caracterizados por la concentración de individuos vinculados al yihadismo o de condiciones propicias a la radicalización y emergencia de redes yihadistas[76]». El estudio revela diferentes variables existentes en determinadas localizaciones que podrían convertirse en factores de riesgo.

Estos factores de riesgo los define como «atributos, circunstancias o sucesos cuya presencia o desarrollo incrementen la probabilidad de emergencia o progresión de amenazas extremistas[77]».

---

[76] De la Corte, Luis (2015) «¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla», *Revista de Estudios en Seguridad Internacional,* Vol. 1, No. 2, pp. 1-34.

[77] Idem.

Cuando un micro-entorno cumple con diversos criterios que lo convierten en un territorio vulnerable a la influencia de un extremismo violento y, además, incorpora determinados factores de riesgo, se transforma en un «escenario de riesgo[78]».

El estudio sobre la presencia y el riesgo extremistas clasifica los factores de riesgo de afección extremista asociados a un territorio en ocho categorías: geográficas, demográficas, políticas e institucionales, económicas, socioculturales, urbanística y asistenciales, criminológicas y relacionadas con la amenaza extremista[79] .

A su vez, los factores de riesgo asociados a un territorio vulnerable a la influencia extremista pueden ser de dos tipos: factores permanentes o coyunturales. Los factores permanentes hacen referencia a la permanencia de manera estable en estas zonas. Los factores coyunturales son factores temporales que aparecen y desaparecen según las circunstancias que se produzcan en estos enclaves, influyendo de forma interna o desde fuera del territorio.

Según de la Corte, destaca como factores coyunturales más significativos del fenómeno terrorista actual que han potenciado la consolidación de territorios extremistas los siguientes: «La permanencia en activo de alguna gran organización que pueda ser reconocida como vanguardia de un movimiento extremista y la existencia de algún conflicto armado que involucren a organizaciones semejantes o sus seguidores[80]».

Las organizaciones objeto de estudio, reconocidas como vanguardia de un movimiento extremista, son las organizaciones yihadistas, especialmente, el Estado islámico y su expansión por la Europa contemporánea.

---

[78] De la Corte, Luis (2015) «¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla», *Revista de Estudios en Seguridad Internacional,* Vol. 1, No. 2, pp. 1-34.

[79] Idem.

[80] Idem.

Si llevamos a cabo una minuciosa revisión bibliográfica observaremos que no existen un número elevado de estudios que revelen o confirmen la presencia de estos enclaves o barrios extremistas yihadistas en territorio europeo. Como consecuencia de esto no encontramos una definición empírica y reconocida por la comunidad científica de lo que es un «enclave yihadista». Sin embargo, estas zonas tienen en común una serie de características y factores de riesgo que las diferencian de otros barrios y las configuran como barrios influenciados por la ideología extremista islamista:

- Habitantes de mayoría musulmana, perteneciente a la comunidad de referencia del terrorismo yihadista.
- Presencia de comunidades migradas, alcanzando la segunda y tercera generación.
- Influencia de las costumbres y religión islámicas
- Bajo nivel de integración en otros barrios
- Aparente rechazo a los no musulmanes de la zona o tensión con componente religioso
- Mezquitas clandestinas. En algunas zonas, se escucha la llamada a la oración característica de la religión islámica.
- Circulación y difusión de ideología y propaganda radical islamista

Para finalizar con el estudio sobre la presencia y riesgo extremistas, relacionada con la amenaza extremista, contempla cinco factores de riesgo característicos de esto enclaves:

- Antecedentes de atentados u otras acciones violentas ilegales de autoría extremista
- Presencia de agentes y estructuras extremistas o antecedentes relacionados
- Señalamiento agresivo del territorio en la propaganda extremista
- Emplazamientos, localizaciones, edificios o instalaciones de alto valor estratégico o simbólico

- Presencia o tránsito de colectivos o personas señaladas como objetivos preferentes de la violencia extremista[81]

Estas características, bajo el amparo de las leyes europeas, convierten determinadas zonas en áreas clave de radicalización y reclutamiento yihadista, donde se impone la sharía, ley islámica, por encima de las leyes nacionales.

Medios de prensa británicos han hecho referencia a las «no-go zones» y la campaña lanzada por radicales islamistas a través de estas zonas denominadas «Sharia controlled zones»[82] empapelando las calles con carteles que proclaman el dominio de las leyes islámicas y las actividades prohibidas en la zona: el alcohol, las apuestas, la música o conciertos, las drogas y la prostitución o el porno.

Bruno Navarro Rousseau-Dumarcet, militar en excedencia, director de seguridad y analista de seguridad y defensa, vincula la proliferación de estos barrios islamistas al fracaso de la integración y factores socioeconómicos: «el altísimo porcentaje de población musulmana sumado a un elevado índice de paro y pobreza que lo convierten en "un cóctel muy explosivo que demuestra que la integración ha fracasado».

4.4. ENCLAVES YIHADISTAS EN EUROPA

En las últimas décadas ha quedado patente que Europa representa uno de los principales objetivos del terrorismo yihadista con el objetivo de recuperar los territorios pertenecientes al antiguo imperio del islam.

Desde la expansión del terrorismo yihadista a nivel global, Europa ha desarrollado una tendencia ideológica o religiosa y como consecuencia una serie de sentimientos radicales y extremistas entre sus comunidades islámicas, fruto del profundo impacto de la propaganda y la radicalización en los enclaves yihadistas, donde se observa con una mayor fuerza. En la actualidad, el fenómeno del

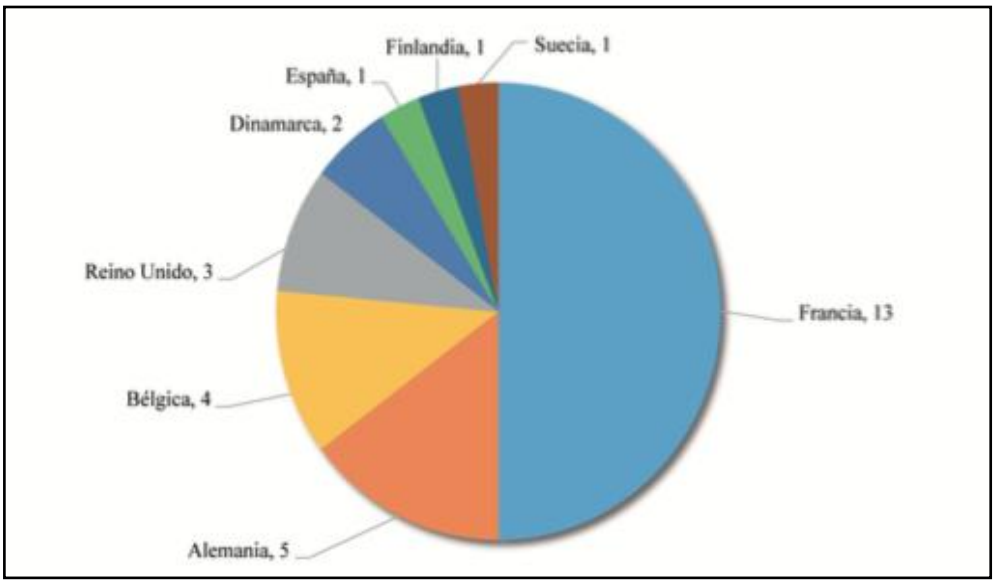
---

[81] De la Corte, Luis (2015) «¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla», *Revista de Estudios en Seguridad Internacional,* Vol. 1, No. 2, pp. 1-34.

82 N.T. «Zonas controladas por la Sharía»

terrorismo está muy presente en nuestra sociedad conquistando barrios y localidades en numerosos Estados europeos.

Los países europeos más afectados por esta expansión yihadista en los últimos años (2014-2017) son los siguientes: Reino Unido, Bélgica, Alemania, Finlandia, Dinamarca, España, y Suecia. A continuación, se muestra un gráfico de la distribución de incidentes terroristas por países[83].



Como podemos observar en el gráfico, aparecen ocho países como los más afectados por el terrorismo en Europa, siendo el más afectado Francia. Algunos de los Estados europeos con mayor presencia de enclaves yihadistas son Francia,

[83] De la Corte, Luis (2018) «La yihad de Europa. Desarrollo e impacto del terrorismo yihadista en los países de la Unión Europea». Informe del Centro Memorial de las Víctimas del Terrorismo. Nº4. Pp. 1-76

Bélgica, Alemania, Reino Unido, España, Dinamarca y Suecia. Los últimos atentados que se han llevado a cabo en Europa han desviado la atención al estudio de determinados barrios y suburbios, los que hemos denominado enclaves. Un importante ejemplo lo tenemos en Francia en el barrio de Saint-Denis, suburbio parisino, se convirtió en escenario de la operación antiterrorista para capturar a Abdelhamid Abaaoud, presunto cerebro de los atentados del Bataclán (París, 13 de noviembre de 2015). Otro ejemplo lo encontramos en Brusela en El barrio de Molenbeek considerado como la cuna de la mayoría de los combatientes belgas que se han unido a las filas de la yihad, también se ha relacionado con diversos atentados en suelo europeo. En reino unido podemos encontrarlos barrios británicos de Birmingham y Luton, donde se han llevado a cabo campañas para imponer la ley islámica por encima de la legislación británica.

En este puno considero muy importante destacar que no solo en cuestión de atentados o víctimas mortales el fenómeno yihadista está cumpliendo lo dispuesto por el ideólogo Setmarian en la «Llamada a la Resistencia Islámica Global», «la aglomeración de la población musulmana en determinados barrios, convertidos en guetos fortaleza, bajo el dominio del islam». Paso previo a la «guerra total» contra Occidente.

El artículo «La Unión Europea y el terrorismo islamista», publicado por Patricia Rodríguez Blanco y Gustavo Díaz Matey, hace referencia a los individuos detenidos por su vinculación con el terrorismo yihadista en Europa: «Son europeos descendientes de inmigrantes musulmanes, estancados en su fase de ascenso social como consecuencia de una vida enmarcada en los suburbios de las ciudades en las que vivían[84]».

Hayder al Khoei, analista del think tank británico Chatham House, asegura que la penetración en Occidente es tal que «Daesh no necesita mandar a yihadistas desde el califato cuando tienen una cantera en ciernes en Europa dispuesta a atentar». Al Khoei señala que el principal objetivo de la tercera ola de

[84] Rodríguez Blanco, Patricia y Díaz Matey, Gustavo (2015). «*La Unión Europea y el terrorismo islamista*». UNISCI, No 39. Pp. 1-14.

la yihad es la guerra entre la Umma y Occidente: «Lo hacen público ellos mismos. No quieren grises, solo blanco y negro, fieles e infieles, que unos odien a los otros y que los musulmanes sientan que no les queda otro camino que su violencia[85]».

Acto seguida llevaremos a cabo un estudio de algunos de los enclaves yihadistas existentes en algunos países europeos, siendo conscientes que este tipo de barrios va en aumento.

4.4.1 Francia

La República Francesa cuenta con una población por encima de los 67 millones de habitantes. El porcentaje de población de confesión musulmana se estima entre el 7-9%. En el año 2017, la cifra de inmigrantes registrada por la Organización de Naciones Unidas era de 7,9 millones. Según algunos estudios, en el año 2030 se prevé que aumente hasta un

Durante el año 2015, la actividad terrorista se centró en Francia. El 7 de enero de dicho año, dos hombres franceses de padres argelinos entraron enmascarados a la oficina del semanario Charlie Hebdo donde se produjo un tiroteo acabando con la vida de 11 personas e hiriendo a otra decena. Ese mismo año, el 13 de noviembre, tres grupos de individuos franceses y belgas llevaron a cabo varios ataques en diferentes zonas de Paris con resultado de 137 personas asesinadas; 89 de ellos fueron retenidos en la sala de conciertos Bataclan antes de ser asesinadas. Ambos atentados fueron reivindicados por el Estado Islámico[86].

Francia se ha convertido en uno de los países más vinculados con la presencia del terrorismo yihadista. Ciertos suburbios franceses, habitados en su mayoría por población musulmana, han sido considerados zonas de marginación, violencia y extremismo islámico.

---

[85] Cabanelas, L. y Calero, F. «*Las canteras europeas de la yihad*». *ABC Internacional*, 2017. Consultado en: https://www.abc.es/internacional/abci-canteras-europeas-yihad-201511291847_noticia.html.

[86] De la Corte, Luis. «La yihad de Europa. Desarrollo e impacto del terrorismo yihadista en los países de la Unión Europea». Informe del Centro Memorial de las Víctimas del Terrorismo. Nº4(2018). Pp. 1-76

En Francia existen aproximadamente 760 barrios que se han convertido en espacios donde rigen la normativa islámica, (La sharía es la ley que impera y las leyes nacionales quedan en un segundo plano),siendo barrios fuera del control de las autoridades francesas y donde se aplica una visión fundamentalista del islam. A este tipo de barrios son denominados por el gobierno galo como «Zonas Urbanas Sensibles» (ZUS), la cuales se han convertido en cuna de numerosos yihadistas que han llevado a cabo su guerra santa en Europa.

Saint Denis, Goutte d'Or, la Chapelle al este de París y Roubaix son algunos de estos barrios donde se fomenta y se predica de forma obligatoria la religión musulmana a los residentes en ella. Las mezquitas retrasmiten sus oraciones a través de los altavoces. Con respecto a la amenaza extremista, se han detectado agentes y estructuras vinculados con la ideología salafista. Los atentados perpetrados en la sala Bataclan, en noviembre de 2015, fueron planeados previamente en el barrio parisino de Saint-Denis, considerado uno de los más críticos enclaves yihadistas en Francia.

El ministro Frances de Interior, Gérard Collomb, para 2019 dio a conocer esta nueva estrategia de seguridad, destacando que los agentes dispondrán de nuevas herramientas tecnológicas para dinamizar y mejorar su trabajo. Por ejemplo, antes de 2019 se cuadruplicarán, hasta alcanzar una cantidad de 10.000, se instalarán cámaras en patrullas y se incorporarán a los uniformes para grabar las intervenciones y poder utilizar las imágenes como prueba.

Collomb señaló que entre septiembre y enero de 2019 se desplegarán 600 policías más en 30 "barrios de reconquista republicana" en los que se ha constatado un incremento de la delincuencia y en los que los habitantes tienen miedo, por ejemplo, de salir de casa o de subir a un autobús público[87].

El barrio de Saint Denis, localizado al norte de París, está compuesto por una población de 1,4 millones de habitantes, 600.000 del total son musulmanes. Saint Denis está dividido en 40 distritos administrativos de los cuales 36 ya están considerados por el gobierno francés como ZUS.

[87] Gérard Collomb (2019). Ministro del Interior de Francia.

Saint Denis cumple las características que lo convierten en una «no-go zone». El ambiente está influenciado por las costumbres y leyes islámicas. A pesar de formar parte de un estado europeo, la penetración del islam más radical y la presencia de agentes y estructuras extremistas lo ha convertido en un enclave más importantes y son aprovechado por los grupos yihadistas para llevar a cabo la segunda fase de la estrategia de Setmarian: lo que se conoce como guerra de enclaves. Asimismo, la difusión de la propaganda yihadista ha conseguido captar a numerosos individuos actuando como lobos solitarios, uno de los actores más habituales en las amenazas híbridas.

Si llevamos a cabo una minuciosa búsqueda bibliográfica sobre este tipo de enclaves podemos destacar a Tamara García Yuste hace una reflexión con respecto al entorno de Saint-Denis: «La sensación que se tiene al llegar al suburbio parisino de Saint Denis es que se llega a un país totalmente diferente. Introducción a la ética islámica, Del islam y los musulmanes, Historias de profetas en el santo Corán y Creer en Alá son algunos de los libros que se pueden comprar en las librerías de este barrio[88]».

Un profesor de la Universidad de Saint Denis y analista, especialista en Oriente Medio, Barah Mikail, hace referencia una de las principales problemáticas sociales desencadenantes de la radicalización yihadista: «Este barrio refleja una parte de la realidad francesa, la de suburbios con gente pobre, que se siente excluida de las percepciones republicanas[89]».

4,4.2. Reino Unido

[88] García Yuste, Tamara (2017) *«Si es usted cristiano no ponga los pies en estos cinco barrios europeos controlados por islamistas». Actuall*. : https://www.actuall.com/persecucion/si-es-usted-cristiano-no-ponga-los-pies-en-estos-cinco-barrios-europeos-controlados-por-islamistas/ [consultado 6 noviembre de 2018]

[89] Cabanelas, L. y Calero, F. (2017) *«Las canteras europeas de la yihad». ABC Internacional*.

Otro de los países con enclaves yihadistas y que han sufrido ataque terrorista es el Reino Unido. Reino Unido cuenta con una población por encima de los 65 millones de habitantes. El porcentaje de población de confesión musulmana se estima alrededor del 4,5%. En el año 2017, la cifra de inmigrantes registrada por la Organización de Naciones Unidas era de 8,84 millones.

Londres ha sido denominada en numerosas ocasiones como «Londonistán» por la influencia musulmana en determinados barrios del país considerados miniestados musulmanes. La existencia de enclaves musulmanes, caracterizados por el extremismo y el control islámicos, ha sido confirmada por las propias autoridades nacionales: «Hay zonas musulmanas de Preston donde, si queremos patrullar, tenemos que ponernos en contacto con los líderes de las comunidades musulmanas para que nos den permiso» –declaración de un policía de Lancashire (Inglaterra) al medio de prensa Daily Mail–.

En Gran Bretaña, la ley islámica está amparada por la Ley de Arbitraje de 1996, que permite al Consejo de la Sharia Islámica (Islamic Sharia Council) la resolución de disputas legales. Este Consejo cuenta con tribunales en ciudades con relevante presencia musulmana: Londres, Manchester y Birmingham, entre otras.

En el año 2014, Tom Winsor, Inspector Jefe de la Policía de Inglaterra y Gales (Chief Inspector of Constabulary), admitió en el medio de prensa London Times la existencia de comunidades en Gran Bretaña fuera del control policial, regidas por sus propias leyes: «Algunas partes de Gran Bretaña tienen su propia forma de justicia. Hay comunidades de otras culturas que prefieren tener su propia policía. En zonas como Midlands, los agentes nunca entran no porque se les prohíba el acceso o tengan miedo, sino porque nunca requieren su presencia, resuelven sus problemas con sus propias leyes[90]».

Anjem Choudary, clérigo musulmán británico y creador del movimiento radical «Need4Khilafah» o «Al-Muhajiroun», fue condenado y encarcelado en 2016 por la predicación de un mensaje islamista de odio frente a diferentes lugares de Londres y su vinculación y apología al Estado Islámico. Choudary

[90] Cabanelas, L. y Calero, F. (2017) «*Las canteras europeas de la yihad*». *ABC Internacional*.

declaró que «dentro de muy poco toda Gran Bretaña será musulmana. Vuestra sociedad se despuebla porque sólo deseáis tener un hijo o un perro. Dentro de pocas generaciones seremos mayoría". Considerado uno de los hombres más peligrosos de Reino Unido, fue puesto en libertad el pasado año 2018[91].

Durante el año 2017 sufrió varios atentados llevados a cabo por lobos solitarios. El 22 de marzo, un individuo británico y musulmán conversó atropelló a decenas de personas en el puente de Westminster utilizando como medio para cometer el ataque un vehículo el cual estrello el mismo contra el Parlamento británico. El atentado, cuya autoría fue asumida por el Estado Islámico, provocó la muerte de cinco personas e hirió a otras 50. El 22 de mayo, un terrorista suicida explotó una bomba en un concierto celebrado en la ciudad de Manchester. La explosión dejó 23 víctimas mortales y 100 heridos, la mayoría menores de edad. El 3 de junio, tres individuos atropellaron con un camión a varias personas en el puente de Londres y, seguidamente, acuchillaron a otras en el mercado de Borough. Estos ataques ocasionaron la muerte de 7 personas, entre ellas un español, e hirieron a 48. La autoría de los tres atentados perpetrados en suelo británico fue asumida por el Estado Islámico.

Londres también ha servido de refugio para yihadistas y puente hacia la radicalización y reclutamiento de la sociedad. Se han encontrado evidencias de grupos islamistas radicales que patrullan las calles de las denominadas «Sharia controlled zones» imponiendo un régimen basado en la ley islámica radical. La «Patrulla Musulmana de Londres» opera por la capital británica, actuando en ocasiones de forma intimidatoria, proclamando la prohibición del alcohol, las apuestas, los conciertos, las drogas, la pornografía y la prostitución.

El barrio de Bury Park, en la ciudad de Luton, y Tower Hamlets, en Londres, ha sido señalado por numerosos medios como enclaves yihadistas y lugares de reclutamiento yihadista. El medio The Sunday Telegraph reveló varios

---

[91] Redacción BBC Mundo.(2016) *«Cómo Anjem Choudary se convirtió en uno de los hombres más peligrosos del Reino Unido sin empuñar un arma». BBC Mundo,* 2016. https://www.bbc.com/mundo/noticias-internacional-37108581**.** [consultado 9 de noviembre de2018]

casos en Tower Hamlets de personas amenazadas por musulmanes radicales por un comportamiento considerado «una violación de las normas islámicas fundamentalistas[92]». Estas localidades, con alto porcentaje de población musulmana, han suscitado debate con respecto a la existencia de enclaves yihadistas en Reino Unido.

4.4.3 Bélgica

Bélgica cuenta con una población alrededor 11,5 millones de habitantes. El porcentaje de población de confesión musulmana se estima en un 5%. En el año 2017, la cifra de inmigrantes registrada por la Organización de Naciones Unidas era de 1,2 millones.

Bélgica mantenía su alarma de riesgo de atentando yihdaista desde 24 de mayo del 2014, cuando un francés de origen argelino, Mehdi Nemmouche, irrumpió en el Museo Judío de Bruselas y mató a tiros a cuatro personas. A pesar de ello, una de las cadenas de atentados más graves que sufrió Europa en 2016 se llevó a cabo en la capital de de este país, Bruselas. El 22 marzo del mentado año, en una terminal del aeropuerto de Bruselas y un vagón de la estación de metro de Molenbeek fueron escenario de dos atentados con bombas que acabaron con la vida de 32 personas e hirieron a varios centenares de personas de todas las edades. Este atentado fue vinculado con el Estado Islámico y con la cédula que perpetró los ataques del año 2015 en París.

La cedula terrorista que llevo a cabo los atentados en suelo belga estableció su red yihadista en el barrio bruselense de Molenbeek, considerado como uno de los principales refugios yihadistas en Occidente por el Ministro de Interior belga,

[92] Cabanelas, L. y Calero, F. (2017) *«Las canteras europeas de la yihad». ABC Internacional*. Consultado en: https://www.abc.es/internacional/abci-canteras-europeas-yihad-201511291847_noticia.html.

Jon Jambon y un barrio «que las autoridades no controlan» según señaló es mismo[93].

Para Carlos Fernández, Catedrático de Derecho Internacional Público y Relaciones Internacionales de la Universidad Rey Juan Carlos y miembro del Observatorio Internacional de Estudios sobre el Terrorismo, una de las claves de que el terrorismo haya encontrado su cuna europea en esta ciudad es la "compleja arquitectura político institucional y administrativa de Bruselas y del mismo Estado belga". Bélgica es un Estado con una alta complejidad y muy descentralizado.

Otro conclave terrorista a tener presente es el barrio Grand Place de Bruselas my próximo al barrio de Molenbeek; sin embargo, la distancia es abismal en lo que se refiere a la cultura e ideología que caracteriza a sus habitantes. En dicho barrio residen más de un centenar de personas de mayoría musulmana de segunda y tercera generación. Este barrio es considerado como un miniestado islámico, cuenta con 22 mezquitas de diferente tamaño establecidas alrededor del territorio. Cinco veces al día se escucha la llamada a la oración en sus calles. Uno de los factores a tener en cuenta y característico de este barrio es la tasa de desempleo que tríplica la media registrada a nivel nacional.

Olivier Vanderhaegen, responsable de antiradicalización en el distrito, define la zona como un nido de radicalización yihadista: "El número de jóvenes que se adhieren sin complejos a discursos radicales aumenta[94]". La propaganda radical circula por el barrio captando la atención, especialmente, de los jóvenes.

La conexión entre el barrio y el terrorismo yihadista se remonta a principios de los años noventa con la fundación del Centro Islámico Belga en Molenbeek, una organización fundamentalista islámica que apoyaba la ideología de Al Qaeda y estaba vinculada con el reclutamiento de combatientes para las filas de la yihad. Los atentados del 11 de marzo del año 2004 en Madrid, el atentado contra el

[93] Sánchez, Álvaro (2017). *«Molenbeek, año I: más radicales, más vigilados». El País, Internacional*.https://elpais.com/internacional/2017/03/21/actualidad/1490090298_194177.html. [consultado 9 de noviembre de 2018]

[94] Idem.

Museo Judío de Bruselas o los atentados de la sala Bataclan en París también apuntan directamente a este conclave yihadista.

Kristof Clerix, experto belga en inteligencia y seguridad, detalla la lista de individuos vinculados al terrorismo islamista con origen en este barrio: «85 personas radicalizadas que los servicios secretos belgas habían entregado al Ayuntamiento de Molenbeek. La lista para todo Bélgica suma 800 nombres e incluye a los que están en Siria o Irak (250), los muertos (75) y los que han vuelto (125)[95] ».

Molenbeek reúne las características que lo convierten en una «no-go zone». Las calles están influenciadas por las costumbres y leyes islámicas en detrimento del cumplimiento de las leyes nacionales vigentes. El discurso musulmán radical y la existencia de agentes yihadistas lo han convertido en guarida y cuna de nuevos miembros del movimiento yihadista global.

4.5 PRESENCIA DEL TERRORISMO YIHADISTA EN ESPAÑA

Según la Estrategia de Seguridad Nacional aprobada en 2017: «El terrorismo, fundamentalmente de carácter yihadista, ha asumido dimensiones cada vez mayores. El terrorismo yihadista proyecta su ideología radical y actúa a nivel global, incluyendo el propio territorio europeo, donde ha protagonizado execrables atentados. En el escenario actual, el principal protagonista de esta amenaza es Daesh, que, por su capacidad operativa, medios, proyección mediática y rápida expansión, se ha convertido en el referente del terrorismo yihadista»[96].

Si analizamos las últimas décadas de nuestro país observamos como España ha sido escenario que ha sufrido diversos atentados y se ha configurado como un territorio de caldo de cultivo para la radicalización de varios centenares de

[95] Sánchez, Álvaro (2017) «Molenbeek, año I: más radicales, más vigilados». El País, Internacional,.

[96] Presidencia del Gobierno. Estrategia de Seguridad Nacional. Departamento de Seguridad Nacional, (2017).

hombres y mujeres que acaban uniéndose a las filas de la yihad. Considerada el Al Ándalus como un territorio propio del pensamiento yihadista, España representa un objetivo principal de las ambiciones yihadistas de reconquistar los territorios que, en otra época, estuvieron bajo el dominio del islam y fueron que fueron arrebatados por la fuerza.

Las referencias a Al Ándalus como antiguo territorio del Islam y tierra de sus antepasados, además de la consideración de Ceuta y Melilla son ciudades ocupadas por el colonialismo español; justifican la desproporcionada presencia del territorio español en la propaganda del Estado Islámico y la presencia del terrorismo yihadista en la actualidad.

El punto de inflexión para España tuvo lugar a principios de los años 2000, cuando Al Qaida puso el foco sobre España e intensificó su presencia y actividad. Desde el año 2004 hasta la actualidad, España ha sido víctima de dos atentados terroristas de índole yihadista entre los que encontramos:

El 11 de marzo del año 2004 tuvo lugar en Madrid el peor atentado terrorista que había sufrido España hasta la época. Dicho atentando fue perpetrado por un grupo importante de individuos, en su mayoría de origen magrebí, residentes en España. Para llevar a cabo este ataque activaron una serie de artefactos explosivos que provocaron 10 explosiones en cuatro trenes diferentes de la red de Cercanías de Madrid. El atentado perpetrado por Al Qaida provocó la muerte de 193 personas y alrededor de 1900 resultaron heridas.

Tras una minuciosa investigación se llegó a la conclusión que la autoría del atentado terrorista del 11-M fue obra de células terroristas de tipo yihadista inspiradas en la primera red de Al Qaida en España, creada a finales de los años noventa.

En los años posteriores al atentado del año 2004, la gran labor llevada a cabo por los servicios de inteligencia y las autoridades y fuerzas de seguridad del Estado español ha conseguido frenar las ambiciones terroristas en España traducidas en intentos de atentado. Ha sido muy importante la preparación que nuestro país ya posee como consecuencia de los atentados ya sufridos por ETA durante varias décadas.

Cuatro años después, en 2008, fue desarticulada una célula terrorista establecida en Barcelona que pretendía hacer explotar el metro de la ciudad catalana con el objeto de perpetrar una masacre en suelo español. El 19 de enero 14 personas mayoritariamente de nacionalidad paquistaní fueron detenidas bajo las fundadas sospechas del Centro Nacional de inteligencia.

Desde los atentados del 11-M hasta el año 2017, se han llevado a cabo 236 operaciones de lucha contra el terrorismo en España que han resultado en la detención de 748 individuos vinculados a actividades terroristas.

El segundo y más reciente atentado en territorio español tuvo lugar en agosto del año 2017 en la ciudad española de Barcelona y el municipio de Cambrils. El 17 de agosto una furgoneta circuló aproximadamente 600 metros sin control por la Rambla de Barcelona provocando la muerte de 13 personas y causando más de un centenar de heridos. Posteriormente, el autor del atentado asesina a un joven en la Zona Universitaria y le roba el coche con la intención de huir. El 18 de agosto se desarrolla una operación policial en Cambrils y cuatro terroristas son abatidos; el quinto terrorista que viajaba con ellos apuñala a una mujer de 42 años provocando su muerte, antes de ser abatido. En total, el número de víctimas asciende a 15.

La autoría del atentado fue asumida por el Estado Islámico a través de redes sociales: «Los ejecutores del ataque en Barcelona son soldados del Estado Islámico y han realizado una operación contra un país de la Coalición».

Hasta el año 20118, según datos oficiales del Ministerio de Interior español, el número de operaciones en España relacionadas con el terrorismo yihadista asciende a un total de 251. En cuanto al número de detenidos, la cifra es de 767 personas vinculadas con alguna actividad yihadista.

La siguiente tabla indica, según las cifras del Ministerio de Interior, el número de operaciones y número de detenidos en España relacionados con el terrorismo de carácter islamista. Por otro lado, indica el número de operaciones y detenidos en otros países en los que han participado nuestras Fuerzas y Cuerpos de Seguridad del Estado, desde los atentados del 11 de marzo del año 2004 hasta el pasado mes de mayo del año 2018.

Según diversos estudios, la gran mayoría de los detenidos o fallecidos vinculados con actividades yihadistas en España son hombres, sobre todo de nacionalidad española y marroquí. La ciudad con más presencia yihadista es Barcelona (24,3) seguida de Ceuta (15%), Madrid (13,6%), Melilla (9,3%) y la provincia de Girona (7%)[97].

En cuanto a las modalidades de implicación yihadista, la mayoría de las acciones realizadas hasta 2017 en España se han perpetrado de forma colectiva (87,7%) en comparación con las actuaciones solitarias (12,3%). Los terroristas conocidos como "lobos solitarios", por lo general radicalizados a través de la propaganda, actúan de manera individual sin ningún tipo de vinculación con células o redes terroristas. Suelen perpetrar atentados sin ningún tipo de organización previa utilizando métodos que aparecen en las revistas y medios de comunicación yihadistas.

Las células terroristas presentes en España desarrollan diferentes funciones que componen la estrategia de actuación yihadista. El proceso de radicalización y reclutamiento de nuevos miembros de la yihad, en la mayoría de los casos, es llevado a cabo por integrantes residentes en España que se encargan a través de redes sociales de difundir los aspectos ideológicos y producir el enaltecimiento de organizaciones terroristas.

En el escenario contemporáneo español, el terrorismo islamista radical representa una de las principales amenazas para la seguridad. A pesar de los centenares de detenciones hasta el momento y las operaciones llevadas a cabo contra el terrorismo, su presencia sigue siendo relevante y sus diferentes actividades en el territorio requieren el constante esfuerzo de nuestras fuerzas de seguridad e inteligencia y la concienciación de la población civil.

Debido a su localización geográfica, España puede considerarse como una de las puertas hacia el continente europeo. Por esto, tanto el terrorismo

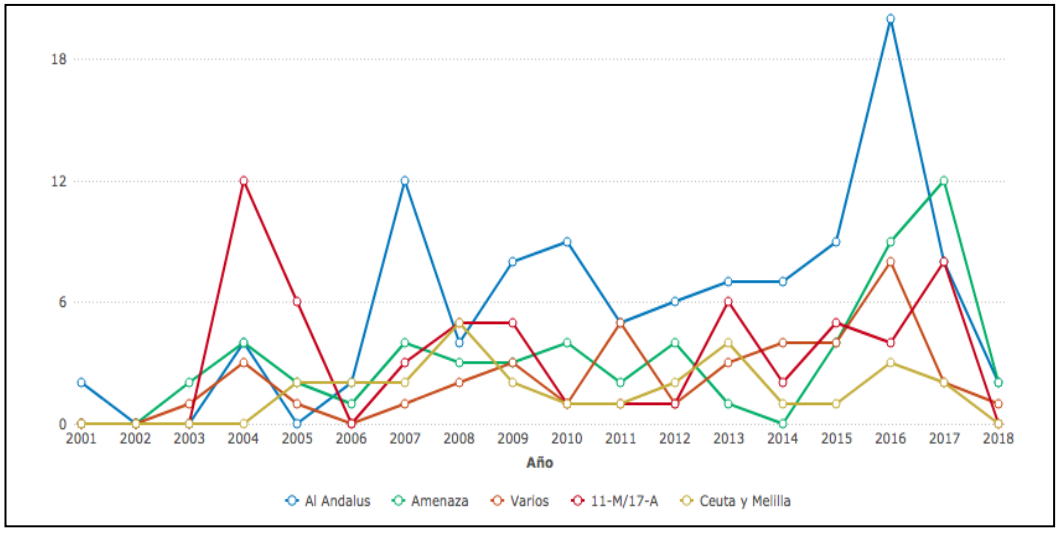
[97] Reinares, Fernando y García-Calvo, Carola (2017). «Actividad yihadista en España, 2013-2017: de la Operación Cesto en Ceuta a los atentados en Barcelona». Real Instituto el Cano, documento de trabajo 13/2017

"doméstico" –dentro de las fronteras nacionales– como el procedente del Norte de África, representan un foco de atención prioritaria.

España, para la ideología yihadista, continúa siendo «Al Ándalus», la tierra bajo el dominio del islam arrebatada por los españoles a la fuerza; su recuperación es un deber incondicional, una obligación personal ineludible para todo musulmán[98].

Al territorio de Al Ándalus, se suman las ciudades de Ceuta y Melilla en las continuas referencias a España por parte de la yihad. Estas dos ciudades españolas están consideradas como «territorios ocupados» por los colonos españoles que es imprescindible recuperar. Al mismo nivel que Palestina, Chechenia y Cachemira.

En la actualidad, España es uno de los países más amenazados por los grupos de ideología yihadista, especialmente el Estado Islámico. La siguiente tabla muestra el número de referencias a España en los medios de comunicación de grupos islamistas:



[98] Pérez Triana, Jesús Manuel (2017). «Al Ándalus en el punto de mira de la yihad: así es la propaganda integrista contra España». Diez Minutos. Págs. 1-6

4.6 PRINCIPALES ENCLAVES YIHADISTA EN ESPAÑA

Como parte de la estrategia para recuperar los territorios arrebatados y llevar a cabo la guerra contra Occidente, la expansión del movimiento yihadista también ha alcanzado localidades españolas convirtiéndolas en «no-go zones». Barcelona, Ceuta, Melilla y Madrid representan los territorios más afectados por la penetración del fenómeno terrorista islámico en la sociedad española.

Las principales «no-go zones» en el Estado Español están localizadas en las siguientes ciudades: Barcelona, el barrio de La Mina; Ceuta, la barriada de El Príncipe Alfonso; Melilla, la Cañada de Hidum, también conocida como «la Cañada de la Muerte», y en Madrid, la Cañada Real Galiana.

4.6.1 Barcelona

El último «Estudio demográfico de la población musulmana» realizado por la Unión de Comunidades Islámicas de España en el año 2018, señala a Barcelona como la provincia española con mayor porcentaje de población musulmana, alcanzando un total de 335.897 personas de confesión islámica[99].

a provincia catalana, caracterizada por la convivencia de numerosas culturas, sufrió, el pasado 17 de agosto del año 2017, un ataque terrorista que provocó la muerte de 15 personas e hirió a otras 131. La autoría del atentado fue asumida por la organización yihadista Estado Islámico. Al día siguiente, Cataluña volvería a ser atacada en Cambrils por la misma red yihadista dejando un muerto y seis heridos.

Los Mossos d'Esquadra han llevado a cabo 17 operativos contra el terrorismo yihadista en Cataluña, resultado de 30 detenciones y más de un centenar de investigados. Según el autor del artículo «La quinta columna actúa en Cataluña», los atentados yihadistas se han visto facilitados por la existencia de una amplia comunidad musulmana que «cuando se concentra en barrios

[99] Unión de Comunidades Islámicas de España (2019). «*Estudio demográfico de la población musulmana*». Observatorio Andalusí.. Págs. 1-18

marginales, constituye caldo de cultivo idóneo para que los terroristas vivan y actúen[100]».

Dicho artículo hace referencia a la Generalitat de Cataluña y la responsabiliza de atraer a un gran porcentaje de población musulmana a la región bajo promesas y, posteriormente, frustrar sus expectativas provocando «el desencanto y la desafección preparando el caldo de cultivo para el surgimiento de grupos terroristas». La consolidación del islamismo radical en diversas zonas de Cataluña ha basado su éxito en la existencia de redes operativas que, según Esteban López, «echan raíces cuando encuentran el adecuado sustrato: comunidades descontentas con afinidad ideológica[101]» y, en este caso, un vínculo religioso muy potente.

El barrio de la Mina, en el municipio barcelonés de Sant Adriá del Besos, ha sido considerado por numerosos expertos como la principal «no-go zone» de la provincia de Barcelona. Gran parte del barrio ha sido ocupado por población musulmana de diferentes generaciones estableciendo, en algunas ocasiones, las costumbres y normas islámicas más radicales.

Barrio de La Mina (Barcelona)

[100] López, Esteban (2017). *«La quinta columna actúa en Cataluña». Defensa.com*. Consultado en: https://www.defensa.com/en-abierto/quinta-columna-actua-cataluna. [consultado 20 de noviembre de 2018]

[101] Idem

En enero del año 2019, tras la desarticulación de una red yihadista en Barcelona como parte de la operación policial «Alexandía», J.M. Zuloaga hacía referencia a la Mina como un «área donde operan militantes yihadistas[102]». La población musulmana de este barrio, considerado una «no-go zone», convive en un clima de precariedad y marginalidad que, combinado con la prevalencia de un sistema de normas propias de vertiente islamista, la convierte en caldo de cultivo para los procesos de radicalización yihadista.

4.6.2 Ceuta

Ceuta es una de las dos ciudades autónomas españolas localizadas al norte del continente africano. En las últimas décadas, la ciudad ha estado vinculada a la amenaza del terrorismo islamista y señalada como una de las principales cunas europeas del terrorismo.

Según el estudio realizado por Luis De la Corte Ibáñez titulado «¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla», el territorio de Ceuta ha estado expuesto al riesgo de afectación yihadista por varios motivos principales: El primero, las características y evolución propia de la amenaza yihadista originando la presencia de potentes redes yihadistas en las regiones próximas del Sahel y el Magreb. El segundo, las características temporales y permanentes del territorio de Ceuta, y su condición de ciudad española.

La Unión de Comunidades Islámicas de España (UCIDE) público en el año 2014 un informe titulado «Estudio demográfico de la población musulmana» situando a Ceuta como la segunda ciudad española, por detrás de Barcelona, con mayor porcentaje de población musulmana, alcanzando la cifra de 37.002

[102] Zuloaga, J.M. (2019) *« Los Mossos desarticulan una célula yihadista en Barcelona con voluntad de atentar». La Razón*. Consultado en: https://www.larazon.es/local/cataluna/operacion-de-los-mossos-contra-el-terrorismo-yihadista-en-barcelona-e-igualada-KF21426936**.**

personas[103]. Los habitantes musulmanes en el territorio representan un 43% de la población de Ceuta.

Una proporción significativa de musulmanes en la ciudad ha desarrollado un sentimiento de discriminación y exclusión por parte de la población de confesión no musulmana. Tales emociones son reforzadas con discursos victimistas promovidos por agentes de radicalización con el objetivo de reclutar nuevos individuos y movilizarlos hacia la violencia terrorista. Estas estructuras se establecen en los barrios más marginales, aprovechando la coyuntura socioeconómica, para incrementar el grado de influencia y afectación.

Barrio El Príncipe Alfonso

[103] Unión de Comunidades Islámicas de España (2019). «*Estudio demográfico de la población musulmana*». Observatorio Andalusí. Págs. 1-18

En el caso de Ceuta, la barriada más señalada por la presencia yihadista es El Príncipe Alfonso, más conocida como El Príncipe.

La precariedad del barrio, la marginalización y el clima de impunidad lo convierten en una zona propicia para el desarrollo de actividades de índole islamista radical características de una «no-go zone». La presencia de inmigrantes musulmanes de segunda y tercera generación, caldo de cultivo para la radicalización, se asemeja a la situación de otros enclaves yihadistas europeos, previamente expuestos.

El Príncipe cumple las condiciones que lo convierten en una de las cuatro principales «no-go zones» españolas. El periodista Luis de Vega escribía un artículo en el año 2015 sacando a relucir la situación de la barriada: «el modelo de Ceuta como crisol de culturas y religiones está cada vez más lejos. Las comunidades mayoritarias, la cristiana y la musulmana, viven cada vez más separadas y no se vislumbra un acercamiento a corto plazo. A los tradicionales problemas sociales y económicos hay que unir el agravamiento de otro, el religioso[104]». La barriada, poblada por un número estimado de 42 mezquitas, se caracteriza por el predominio de la religión islámica.

El escaso control policial favorece la alta tasa de criminalidad organizada y la expansión de una ideología islamista radical. Las detenciones vinculadas con el terrorismo yihadista en Ceuta desde el año1995 al 2015 ascienden a 10, incluyendo la desarticulación de redes terroristas (Véase anexo 3)[105]. La droga es una de las industrias que más dinero maneja y, en ocasiones, la que financia atentados terroristas.

---

[104] De Vega, Luis (2015) «*La convivencia agoniza en el barrio ceutí del Príncipe». ABC España*. Consultado en: https://www.abc.es/espana/20150120/abci-ceuta-principe-convivencia-201501182054.html. [consultado 30 de noviembre de 2018]

[105] Luis De la Corte (2015). "¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla", *Revista de Estudios en Seguridad Internacional,* Vol. 1, No. 2, pp. 1-34.

4.6.3 Melilla

Melilla es la segunda de las ciudades autónomas, junto con Ceuta, que conforman el Estado español; está localizada al norte de África, haciendo frontera con Marruecos.

La Cañada de Hidum (Melilla)

El número de detenciones relacionadas con el terrorismo yihadista, llevadas a cabo entre los años 1995 y 2015, asciende a 10. La presencia de agentes yihadistas en el terreno es una realidad que apunta directamente a una de las zonas más críticas de la ciudad: La Cañada de Hidum, también conocida como La Cañada de la Muerte.

Las principales deficiencias existentes en la Cañada de Hidum, también presentes en la barriada de El Príncipe, son las siguientes:

- Alta tasa de desempleo y desocupación, especialmente en los estratos más jóvenes.
- Infraestructuras urbanísticas precarias y deterioradas.
- Escasez de servicios públicos básicos.
- Rechazo a los cuerpos y fuerzas de seguridad locales.
- Alto porcentaje de población musulmana.
- Influencia de cultura y costumbres musulmanas.
- Falta de presencia policial y clima de impunidad.
- Alta tasa de criminalidad y violencia.
- Casos de radicalización yihadista.
- Detenciones vinculadas al terrorismo yihadista.

El barrio conocido como la Cañada de la Muerte está considerado como la «no-go zone» por excelencia de la ciudad de Melilla. El islam radical ha penetrado en la sociedad imponiendo, en muchos casos, las leyes más fundamentalistas y el rechazo a otras ideologías ajenas a la confesión musulmana.

La marginalidad, la precaria situación y el sentimiento de exclusión han propiciado la expansión de corrientes fundamentalistas de credo islámico entre la población favoreciendo los procesos de radicalización a través de discursos atractivos para los habitantes más vulnerables.

4.6.4 Madrid

La provincia de Madrid, capital de España, representa la cuarta provincia española con más porcentaje de población musulmana, alcanzando un total de 290.991 habitantes que profesan el islam. La capital madrileña se ha convertido en una víctima más de la estrategia de penetración yihadista en la sociedad española y europea.

En noviembre del año 2015, tres marroquíes residentes en Madrid, de entre 26 y 29 años, fueron detenidos como parte de un operativo policial contra el terrorismo yihadista. Uno de los detenidos, vinculado al Estado Islámico, era procedente del barrio madrileño de la Cañada Real Galiana, en la localidad de Rivas-Vaciamadrid.

La Cañada Real Galiana, concretamente el Sector VI, es una zona de Madrid considerada como enclave yihadista por el gran porcentaje de población musulmana regida por leyes islámicas y su conexión con redes terroristas islamistas. A menos de 30 minutos del centro de la ciudad, esta barriada se caracteriza por su condición de precariedad, exclusión y falta de control policial. En esta «no-go zone» madrileña convive una comunidad musulmana que se ha apoderado del territorio en las últimas décadas implantando sus propias leyes.

En el año 2007, el medio de prensa ABC publicó un artículo sobre la creciente preocupación por el germen radical islámico que estaba creciendo en el Sector VI de la Cañada Real Galiana. Asimismo, el artículo hacía referencia a una investigación policial dirigida a un imán de la Mezquita de Valdemingómez por su supuesta vinculación con el extremismo islámico. Según el artículo, el imán

estaba enseñando a jóvenes del barrio a fabricar cócteles molotov. Los vecinos del barrio declararon a favor del líder religioso desmintiendo la información[106].

La falta de urbanización, las tasas de desempleo y desocupación, la falta de control por parte de las autoridades policiales y el clima de hostilidad, son factores potenciadores de un sentimiento de rechazo hacia el orden actual que, combinados con el gran porcentaje de comunidad musulmana, se convierten en oportunidades que organizaciones yihadistas aprovechan para radicalizar a la población. Asimismo, se convierten en áreas prioritarias para establecer sus asentamientos.

[106] Hidalgo, Carlos (2007). «*Los sindicatos policiales exigen que se atajen los brotes radicales en la Cañada Real*». *ABC*. Consultado en: https://www.abc.es/hemeroteca/historico-07-11-2007/abc/Madrid/los-sindicatos-policiales-exigen-que-se-atajen-los-brotes-radicales-en-la-ca%C3%B1ada-real_1641302193786.html.

-CIBERTERRORISMO COMO AMENAZA HÍBRIDA. -

V.CIBERTERRORISMO COMO AMENAZA HÍBRIDA: LA CIBERSEGURIDAD Y EL CIBERESPIONAJE.

En la actualidad es impensable el hecho de creer que nuestra sociedad puede desarrollarse al margen de las nuevas Tecnologías de la Información y la Comunicación (TIC's) o lo que es conocido comúnmente como internet y todas sus diferentes posibilidades y vertientes. A mediados de 2018, el número de usuarios de internet en todo el mundo era del 53% de la población mundial con más de cuatro mil millones de usuarios. Así pues, a efectos prácticos, más de la mitad de los habitantes de nuestro planeta ya son usuarios de internet[107].

Pocos son ya los ámbitos en los que las TIC´s no están presentes. En muchas, estados y organizaciones estas tecnologías ejercen funciones insustituibles y primordiales[108]. Al mismo tiempo, las redes de estas infraestructuras constituyen una de las mayores vulnerabilidades que existen en nuestras sociedades actuales, siendo el ciberespacio uno de los ámbitos de mayor desarrollo actual en materia de la seguridad y la defensa. En la actualidad, el ciberespacio es usado en los conflictos bélicos principalmente porque facilita considerablemente el anonimato del atacante, y a diferencia de otros conflictos, no hay una determinación espacial, siente este aspecto el que la diferencia de las mayorías de las guerras tradicionales donde el límite de actuación del conflicto estaba muy delimitado.

Con la inclusión en todos los ámbitos de nuestra vida de las TIC´s ha dado lugar a lo que se conoce como el nacimiento de la llamada "Sociedad de la Información y del Conocimiento". En la actualidad, entendemos el ciberespacio como el lugar de encuentro para millones de personas en el que todo está interconectado, lo que está provocando que este nuevo mundo de las TICS no pare de aumentar, y como consecuencia, cada vez su repercusión para la sociedad

[107] We Are Social y Hootsuite.

[108] Puime Maroto, J. (2009), "El ciberespionaje y la ciberseguridad", La violencia del siglo XXI. Nuevas dimensiones de la guerra, p. 72.

tenga efectos extraordinarios, manifestándose en muchos ámbitos académicos que llegan a la conclusión que su aparición ha supuesto un antes y un después en la era de la información y la comunicación[109].

Si bien su aparición no es reciente, ya que hace años que empezó a hacerse referencia a la criminalidad y peligro de la informática, este fenómeno de la criminalidad relacionada con el uso de las TIC´s sigue siendo algo nuevo para las instituciones que tienen que enfrentarse a esta constante amenaza[110].

La revolución de las TIC´s, como concepto amplio, abierto y dinámico que recoge todos los elementos y sistemas empleados hoy en día para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, aún no ha finalizado ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio continuará expandiéndose y evolucionando en las décadas venideras.

Estas TIC's, que tanto han facilitado la vida de sus usuarios en todas sus posibles variantes como el comercio, educación, sanidad, defensa, investigación, etc…, va unido intrínsecamente el hecho de la apropiación indebida que pueden hacer otros actores de la información con la intención de lucrarse a raíz de los usuarios de las mismas, al igual que se hacía décadas atrás de forma física, con la salvedad que actualmente el delincuente lo realiza cómodamente a distancia y con un cierto anonimato, consiguiendo con ello que los riesgos sean menores frente a los posibles beneficios que pueden llegar a ser muy sustanciales, es lo que actualmente se conoce como la CIBERDELINCUENCIA.

Los estados no están ajenos a estas amenazas que en los conflictos bélicos anteriores al siglo XXI no se producían por la carencia de este ciberespacio. Cuando el usuario de las TIC's es el propio Estado o una empresa que representa un sector importante para los intereses del mismo en diferentes materias como Defensa, Economía, Alta Tecnología, Industria Química, Energía o Salud, puede aparecer la figura del actor que persigue conseguir el acceso avanzado a estas técnicas de comunicación utilizando una de esas empresas u organismos oficiales

[109] Sánchez Medero, G., (2013) "El ciberespionaje", Nueva Época, p. 115

[110] Miró llinares, F. (2012), "El cibercrimen", Marcial Pons, p. 25

con otros fines distinto a los que persigue el estado y que en muchos casos se encuentra detrás de esos hechos que dan lugar a un Estado hostil, se trataría de CIBERESPIONAJE. En este sentido, el espionaje es un fenómeno que se ha dado desde el principio de los tiempos. Con ello se pretende conocer los planes o actividades de otro estado consiguiendo con ello ventajas importantes a la hora de atacar o incluso para defenderse de las mismas.

A través de las comunicaciones que encontramos en este mundo virtual, se conecta millones de redes, se consigue que las infraestructuras vitales de un país funcionen. Organizaciones como los bancos y las universidades son objeto de ciberataques ya que muchas de ellas son infraestructuras críticas. Por ello, la economía y seguridad nacional vienen condicionadas en buena medida de las tecnologías de la información y de la infraestructura de comunicaciones[111].

Los constantes e imparables avances tecnológicos han delimitado la evolución de los métodos y procedimientos de interceptación y encriptación de la información. Así, por ejemplo, el telégrafo y la radio han sido descubrimientos relevantes en este campo, favoreciendo con ello las técnicas de espionaje. Como ejemplo encontramos la máquina Enigma, utilizada por el ejército alemán durante la Segunda Guerra Mundial.

Anteriormente durante la guerra fría ambos bandos empleaban el espionaje como forma de obtener información, aunque también para desinformar al rival. En la actualidad no solo se usa para obtener información, sino más bien como un arma muy importante en el conflicto bélico.

Sin embargo, el espionaje que se practica hoy en día muy poco tiene que ver con el espionaje de que se utilizaban como técnica de ataque o defensa en aquellos conflictos. Anteriormente, el espionaje consistía en pinchar un teléfono del contrario o en interceptar comunicaciones, siendo el objetivo último obtener información, pero en ningún caso se buscaba manipularla ni destruirla. El ciberespionaje, por el contrario, como veremos en los siguientes apartados, busca

[111] Puime Maroto, J. (2009), "El ciberespionaje y la ciberseguridad", La violencia del siglo XXI. Nuevas dimensiones de la guerra, p. 48.

habitualmente, después de obtener la información, manipularla, borrarla o destruirla[112], consiguiendo con ellos un nuevo tipo de amenaza híbrida.

El principal peligro que existe en la actualidad en el mundo de internet es la falta de consciencia de los propios usuarios al no ser juiciosos con los peligros que existen por el mal uso del mismo, por lo que se tiene la falsa sensación de que se está haciendo uso de las TIC´S con la máxima seguridad y en la más estricta intimidad. El uso del espacio virtual permite un gran abanico de posibilidades y actividades que pueden ser de uso legal p por el contrario ilícito. Es por esta razón, que los términos ciberdelincuencia, ciberterrorismo o ciberespionaje son cada vez más conocidos, como consecuencias de las noticias que cada vez son más globales, al ser mayor el número de actores que han sufrido estas acciones ilícitas.

Ante este aumento imparable de noticias existentes sobre mal uso de las TIC's, los usuarios tienen la sensación de que el uso de la misma se ha convertido en un espacio donde cualquier actividad ilegal puede quedar impune debido a sus dos características específicas y principales. La primera de ellas es la ausencia de fronteras físicas y la segunda la dificultad de encontrar a los responsables y consecuentemente sean castigados, siendo esta impunidad la que conlleva estas nuevas técnicas a los actuales conflictos entre los estados.

La falta de una regulación específica se debe en gran medida a la novedad de todo lo relacionado con las TIC's, su auge imparable y su rápida y constante evolución. Esta falta de regulación dificulta muchos a los estados para poder defenderse de estos ataques de la manera más eficaz posible

Como principal objetivo de todo lo expuesto, está el concebir estos ataques como nuevas amenazas híbridas que se ciernen sobre los estados en los nuevos conflictos bélicos, proporcionándoles los medios y la información útil para evitar en la medida de lo posible que los ataques por parte de actores externos sean ejecutados con éxito.

[112] Sánchez Medero, G., (2013) "El ciberespionaje", Nueva epoca. op. cit., p. 116.

5.1 LA CIBERSEGURIDAD.

La ciberseguridad es un proceso que tiene lugar en un escenario cambiante donde las amenazas existentes podrían tener efectos mucho más complejos y perjudiciales que los propios de las amenazas tradicionales. La globalización ha transformado los pilares del Estados y las bases de nuestra sociedad, hasta el punto de crear una sociedad paralela a la física. Por este motivo, el ciberespacio es un lugar "de encuentro para millones de personas" como consecuencia de la gran cantidad de información que ofrece a los internautas y de su flexibilidad en el uso[113].

MARTÍNEZ ATIENZ define la ciberseguridad como "el compromiso de todos, y, es necesario evolucionar de una cultura reactiva a una prevención y resiliencia. Las principales políticas deben ir dirigidas a fomentar: La resiliencia de nuestro ciberespacio, la colaboración público privada, la educación y concienciación; el I+D+i y la colaboración internacional"[114].

De esta forma, el ciberespacio es un "territorio" que no cuenta con un espacio físico específico (no de tiempo) rompiendo todas las Leyes de la naturaleza conocidas y estudiadas en física teórica (Einstein, Newton) y cuántica (Richard Feynman), ocasionando diversas y complicadas "ecuaciones" a esta otra ciencia y disciplina inexacta como es el Derecho, cuyo modelo se ve amenazado por esta nueva ciberrealidad social.

Al ciberespacio no se le pueden aplicar los criterios tradicionales para clasificarlo dentro de un espacio determinado, y por esta causa no es posible

---

[113] Caballero Velasco, M.Á. (2009), "Ciberdelincuentes: la gran amenaza", Gerencia de Riesgos y Seguros, núm. 122, 2015, p. 66. IV Congreso de CiberSociedade 2009, "Internet: Un espacio para el cibercrimen y el ciberterrorismo"..

[114] Martínez Atienza, G. (2016), "Seguridad y delitos tecnológicos", en Seguridad Pública y Privada, p. 200.

oncretar de igual manera que si se tratase de un territorio físico, qué normas han de aplicarse y cómo se deben administrar[115].

5.2 CIBERCRIMEN Y SUS MODALIDADES

Lo mismo ocurre en el caso de los ciberdelitos: Internet está configurado para que, de forma sencilla y barata, el ciberdelincuente realice sus acciones antisociales anónimamente utilizando un dispositivo (smartphone, ordenador, etc.) de difícil localización territorial en el mundo físico.

En castellano, se emplean los términos de cibercrimen, ciberdelito, cibercriminalidad, ciberdelincuencia, todos ellos, generalmente, bajo un mismo significado. A ello se debe añadir que en España se utilizaban otros conceptos como los de criminalidad informática, delito informático, etc. El origen de estos últimos términos viene de los conceptos ingleses y alemanes como son respectivamente computer crime y Computerkriminalität, para referirse, en muchos casos, al mismo fenómeno al que se hace referencia cuando se habla de la cibercriminalidad o del cibercrimen.

En este sentido, se sustituye el término de delitos informáticos por la de cibercrimen y cibercriminalidad en relación al concepto anglosajón cybercrime[116], procedente de la unión entre el prefijo cyber, derivado del término cyberspace, y el término crimen, como concepto que sirve para englobar la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio[117].

---

[115] E´cija Bernal, Á. (2014), "El Ciberespacio: una herramienta de poder", Editorial Aranzadi, Cizur Menor.

[116] Se atribuye el primer uso de la palabra cybercrimen a John Perry BARLOW (1990) "a not terribly brief history of the electronic frontier foundation" aunque como señala BRENNER ya debía utilizarse fuera del ámbito académico. BRENNER, S. W., "Cybercrime Metrics: old Wine, New Bottles?", en VJOLT, vol. 9, núm. 13, 2004, p. 2

[117] Miró Miralles, F. (2012), "La criminalidad en el ciberespacio: la cibercriminalidad", Marcial Pons, p. 37. Este campo es un ejemplo de la utilización en el ámbito científico de negoologismos derivados de la traducción al castellano de conceptos de otras palabras.

En inglés, parece prevalecer este término frente a otros como computercrime, u otros en los que se utilizan prefijos como virtual, online, high-tech, digital, computer-related, Internet- related, electronic, y e-[118]. En el origen de esta modificación de denominación, está la evolución, desde una perspectiva criminológica, de los comportamientos ilícitos en la Red y la preocupación legal en relación con ellos, concretamente, ser el centro del riesgo la información del sistema informático, a serlo las redes telemáticas a las que los sistemas empezaron a estar conectados y los intereses personales y sociales que se ponen en juego en las mismas. De este modo, en la primera generación de la cibercriminalidad, lo característico era el uso de ordenadores para la comisión de delitos, mientras que, en una segunda etapa, lo primordial es que el delito se comete a través de Internet. Según WALL, existiría una tercera fase en la que los delitos están absolutamente determinados por el uso de Internet y las TIC´s[119].

YAR define el cibercrimen como "aquel delito cuya característica esencial es el rol central que las TIC´s juegan en su comisión"[120]. Aunque en principio, podría parecer que está restringiendo el alcance del concepto, lo que pretende es incluir únicamente aquellas infracciones en las que la utilización de las TIC está relacionada con el aspecto esencial del delito. Por lo tanto, estamos ante un concepto amplio que abarca cualquier comportamiento delictivo puesto en marcha en el ciberespacio, sea el mismo esencialmente nuevo o consista simplemente en la comisión de un injusto tradicional empleando como nuevo medio comisivo el mencionado ciberespacio.

Este concepto debe incluir las infracciones nuevas en su esencia o únicamente en los medios; sean las TIC el objetivo, el medio o el lugar de ejecución; y sean los bienes jurídicos afectados tan diversos como el patrimonio, la seguridad nacional o la indemnidad sexual de los menores. Dicho en otros

---

[118] Smith, R.G., Grabosky, P., y Urbas, G. (2004), "Cyber criminals on trial", Cambridge, Cambridge University Press, p. 5.

[119] Wall, D. (2007), "Cybercrime: the transformation of crime in the information age", Cambridge, Polity Press, pp. 44 y ss

[120] Yar, M. (2006), "Cybercrime and society", Sage, London, p. 9.

términos, si la cibercriminalidad pretende configurarse, en suma, como una categoría criminológica que englobe a todo un conjunto de infracciones con una misma problemática de riesgo y de respuesta penal, bastará con que la conducta, para que sea objeto de esta nueva categoría penal, se realice en ese ámbito virtual con dimensiones espacio temporales diferentes, y caracterizado por la transnacionalidad, la universalización del medio y el estar sujeto a revolución permanente, que es el ciberespacio[121].

Pues bien, una vez considerado el concepto de cibercriminal como preferible hoy en día a la de delincuencia informática, pasamos a sistematizar los numerosos comportamientos ilícitos surgidos en el ciberespacio. Con esta clasificación se busca aportar criterios de diferenciación entre los distintos cibercrímenes con la finalidad de entender mejor la realidad criminológica y las necesidades preventivas de cada tipología de delitos dentro del fenómeno del cibercrimen[122].

Así, la observación de la realidad criminológica nos muestra en un primer momento que el ciberespacio se ha vuelto en algunos casos en un ámbito auténticamente generador de nuevas conductas delictivas cuando las TIC´s son la única forma de realización de la infracción (Hacking; ataque de los insiders, etc); en otros , en cambio, la irrupción del "nuevo espacio" no ha comportado el surgimiento de nuevas formas puras de delincuencia, sino de réplicas de otras ya existentes que cambian sus caracteres básicos al llevarse a cabo en el nuevo ámbito virtual como es el caso del ciberacoso, que posteriormente será estudiado; y, por último, el ciberespacio de sistemas conectados en redes también ha reforzado la importancia de los contenidos al facilitar enormemente su difusión global, lo que ha generado todo un conjunto de conductas en las que la ilicitud no radica más que en la difusión o acceso a determinadas formas de información ilícita o socialmente considerada peligrosa.

---

[121] Miró Miralles, F., "La criminalidad…", op. cit., p. 44

[122] Miró Miralles, F. (2012), "Tipos de cibercrimen y clasificación de los mismos", en El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, pp. 50-51.

Es cierto, en todo caso, que todas las clases de cibercrimen al estar unidas por el ámbito en el que se comete la conducta delictiva tendrán rasgos comunes ya cada categoría, por la forma de incidencia de las TIC,s en la esencia de la conducta criminal, planteará particulares problemas criminológicos y penales.

Con ello, el mayor problema que presenta el supuesto de los "ciberataques puros", entendidos como "puros "por ser únicamente posibles en el ciberespacio, proviene de la total novedad de los comportamientos con la consiguiente falta de estrategias preventivas de carácter criminológico frente a ellas, así como de la inexistencia de preceptos que permitan la incriminación de los mismos.

Por lo tanto, surgen un conjunto de conductas ilícitas en internet consideras totalmente nuevas al caracterizarse por dirigirse contra los nuevos servicios, los nuevos bienes o las terminales que operan en el ciberespacio.

En este tipo de cibercrímenes, las TIC no sólo conforman el medio comisivo de tales ataques, sino que son el único posible, puesto que son medios y objetivos, y no es posible producir la esencia de ilicitud de estas infracciones si no es en el ciberespacio.

Entre estas infracciones podríamos englobar, a título ejemplificativo, el hacking o acceso ilícito a sistemas informáticos, que en otras clasificaciones se suele considerar, además, una tipología determinada de un grupo de ataques más genérico, denominado en terminología de la comunidad informática "data breaches o violación de datos", basado en cualquier forma de destrucción, modificación o acceso a datos de empresas (generalmente se utiliza en este sentido) o de particulares.

El hacking, como técnica mediante la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo, tiene capacidad potencial de ser utilizado con el fin de acceder a cualquier tipo de información que esté en el sistema. El hacking, de forma amplia, es la metodología empleada por los hackers consistente en la superación de cualquier barrera informática, bien sea para el acceso a un sistema, bien para la configuración de una determinada programación funcional, etc. Se trata de una serie de herramientas, que permiten detectar vulnerabilidades en los sistemas de información, y que mal utilizadas pueden producir resultados no deseados.

Dentro de esta categoría de cibercrimen, es muy popular el llamado sabotaje cibernético a través de la infección de virus destructivos que se debe considerar, a su vez, como una tipología del más general comportamiento de distribución de malware o software malicioso destinado a dañar, controlar o modificar un sistema informático. Desde su aparición en los años setenta, los virus se han acabado convirtiendo en un fenómeno casi natural en el ciberespacio[123].

En el caso de la categoría denominada como "ciberataques réplica", entendidos como "réplica" porque el ciberespacio es el nuevo medio desde el que realizar delitos tradicionales, el mayor problema será la potenciación del riesgo para los intereses sociales que se deriva del nuevo medio, vasto e inmenso como es el ciberespacio, en el que se ejecuta la infracción, así como la dudosa capacidad de los tipos penales existentes para dar cabida a conductas similares en lo injusto pero cambiantes en su forma de realización.

Aquí incluiremos el ciberespionaje o snooping (en sentido amplio) y el ciberacoso, fenómenos que serán analizados en profundidad a continuación.

Finalmente, las infracciones llamadas "cibercrímenes de contenido", plantean dificultades propias vinculadas tanto con la dificultad de prevenir la mera difusión de contenidos en el ciberespacio, como con el complejo debate de atribuir responsabilidad a todos los participantes en tal proceso.

Todos esto tipos de ataques que se llevan a cabo en el ciberespacio son utilizados en los nuevos conflictos bélicos, siendo el ciberespacio una de las principales amenazas híbridas.

5.3 EL CIBERESPIONAJE

Tanto los estados como todos los usuarios de internet guardan en mayor o menor proporción una información muy importante, económica y secreta con un contendió de datos en general fundamentales para su seguridad con el fin de garantizar la misma. Sin embargo, dicha seguridad, en los últimos años, se ha visto vulnerada debido lo que se conoce como el CIBERESPIONAJE.

[123] Miró Miralles, F.(2012), "Tipos de cibercrimen…", op. cit., pp. 57 y ss.

Desde un punto de vista científico entendemos el Ciberespionaje como el acto por el cual se obtiene información secreta sin el permiso de aquél quien es dueño de la misma. Dicho acto se realiza a través de métodos exclusivamente cibernéticos que utilizan la red y los ordenadores o terminales con el fin de poner en marcha técnicas de crackeo, hackeo y todo tipo de prácticas encaminadas al robo de información, por medio de distintos programas o códigos maliciosos (malware).

El termino Ciberespionaje está conformado por el elemento prefijal ciber y por el sustantivo espionaje. De acuerdo con el Diccionario de la Lengua Española de la Real Academia ciber proviene del inglés cyber, creado por acortamiento del adjetivo cibernético, relativo a la palabra cibernética. En un sentido amplio, ciber "indica una relación con redes informáticas". Por otra parte, en esta fuente lexicográfica, espionaje se define como "la actividad secreta y fraudulenta encaminada a obtener información sobre un país, especialmente en lo referente a su capacidad ofensiva y defensiva entre otros campos". Es importante aclarar que esta definición hace referencia únicamente a la actividad fraudulenta entre países; sin embargo, en la vida cotidiana aplica también para empresas y particulares.[124]

Los gobiernos han dado prioridad a la creación de sistemas de seguridad potentes para evitar que la información sea visible como una forma de blindarse ante los ataques de ciberespionaje a los que las naciones están constantemente expuestas, Estos nuevos sistemas se conocen como ciberseguridad o ciberdefensa y consisten en todas aquellas acciones de carácter preventivo que tienen por objeto el asegurar el uso de las redes propias y negarlo a terceros.

Si estudiamos este fenómeno observamos que todos los estados del mundo se enfrentan para combatir el ciberespionaje siendo el principal problema determinar la autoría del atacante, dando lugar a una nueva forma de ataque en los conflictos bélicos de este siglo, entendiendo esta amenaza como híbrida. Hasta que no existan políticas claras al respecto, las actividades cibercriminales serán la

[124] https://www.upf.edu/antenas/resultados/ndm/2016.03.neo_esp.html. [consultado 15 enero de 2018].

constante, lo que podría generar sanciones económicas y militares y, por consiguiente, una ciberguerra.

Para España, como para el resto de los países de nuestro entorno, el ciberespionaje sigue constituyendo la mayor amenaza para la seguridad nacional. Durante 2016, los servicios de inteligencia occidentales observaron un importante crecimiento del ciberespionaje económico, especialmente dirigido a las industrias de los sectores de defensa, alta tecnología, industria química, energía y salud, persiguiendo el acceso a desarrollos avanzados teniendo su origen en Estados y empresas. De igual importancia es el ciberespionaje político, con origen en los Servicios de inteligencia que persigue información de naturaleza política, económica o estratégica, así como planes de desarrollo y posiciones nacionales en torno a debates o negociaciones abiertas.

Este tipo de ataques, en cuyo origen hay que colocar a ciertos estados y empresas extranjeras, están provocando alteraciones en el orden económico mundial por lo que tienen de elementos perturbadores de la competencia, sin entrar a considerar ahora otras posibles consecuencias, tales como la utilización de la información indebidamente obtenida para incrementar el arsenal armamentístico de los estados atacantes. De la sofisticación con la que se realizan estos ataques se deriva la dificultad de su detección, que puede demorarse semanas, meses e, incluso, años.[125]

[125]Según un artículo publicado por la revista Volkskrant, (2016), la empresa Rheinmetall, especializada en sistemas para la defensa, había estado siendo víctima de un ataque con posible origen chino desde 2012, habiendo sido descubierto al final de 2015 por la empresa de seguridad Fox-IT.

21 Ciber Elcano (2013) del Real Insituto Elcano y la conferencia "Trojan Horse: The Widespread Use of International Cyber-Espionage as a Weapon RSA Conference 2013" de Mark Russinovich.

5.3.1 La historia del Ciberespionaje

Durante la última década el ciberespionaje ha constituido la mayor de las amenazas del ciberespacio a nivel mundial. Entre las más habituales encontramos aquellas que van dirigida a los sistemas de información de la industria, empresas de Defensa, organizaciones con alto patrimonio en propiedad intelectual e industrial y Administraciones Públicas, aumentado considerablemente estos ataques para debilitar a los estados en materia de seguridad.

La principal dificultad para protegerse de estas amenazas en su complejidad, volumen e impacto que pueden llegar a producir los mismos, habitualmente conducidos a través de APT han sido muy parecidos a lo largo de los últimos años, estas evidencias hacen pensar que estos ataques han sido llevados por Servicios de Inteligencia o Departamentos de Defensa extranjeros, los cuales invierten grandes sumas de capital y numerosos recursos para aumentar sus capacidades de defensa y ataque.

La historia del Ciberespionaje se podía resumir someramente en los ciberataques y su evolución a lo largo del tiempo, si bien es en 2005 cuando podemos definir los mismos desde un punto de vista militar como una amenaza híbrida[126].

Haremos una breve reseña cronológica de varios ataques sufridos en los últimos años.

1982: Sabotaje del gaseoducto de Siberia (Rusia).

1983: Estreno de la película "Juegos de Guerra".

1984: 1er virus de ordenador, pakistaní "Brain".

1986: 1er caso documentado de ciberespionaje en el libro "El huevo del cuco" del autor Clifford Stoll[127]

---

[126] "Stuxnet": 1er ataque cibernético conocido, de EE.UU. a enriquecimiento nuclear iraní.

[127] Stoll (1950) "El huevo del cuco". Físico y astrónomo estadounidense, experto en ordenadores y escritor. participo en la captura del hacker alemán Markus Hess.

1988: Gusano "Morris Worm" creado por Robert Tappan Morris @RTM, con más de 6.000 ordenadores dañados y pérdidas de 98 millones de dólares.

1991: Kevin Poulsen @ Dark Dante es detenido por el FBI por vender secretos militares estadounidenses.

1992: 1er virus polimórfico, "Dark Avenger".

1997: Operación "Elegible Receiver", 1er ejercicio de ciberguerra de EE.UU.: Joint Task Force Computer Defense (Fuerza de Tarea Conjunta de Ciberdefensa).

1998:"Moonlight Maze": Ciberpenetración en el Pentágono, NASA,y Departamento de Energía de EE.UU... Implicación de Rusia.

2003: ANONYMOUS (ver 4.5 AGENTES DE LA CIBERDELINCUENCIA) nace en un foro de un dominio web denominado "4chan".

2003-2005: "Titan rain": Shawn Carpenter descubre violación de datos y extracción de los mismos. El FBI y el ejército de los EE.UU. investigan. Origen en China[128].

2005-2010: "Stuxnet": 1er ataque cibernético conocido, de EE.UU.a enriquecimiento nuclear iraní.

2006: Se lanza WikiLeaks: organización peridística internacional que publica información secreta y confidencial de fuentes anónimas.

2006-2011: "Shaddy Rat": penetraciónde 72 compañías e instituciones gubernamentales.

2007: Estonia: El ataque de denegación de servicios (DDOS) del Nashi al gobierno estonio.

2008: Guerra de Osetia del Sur: Hackeo de Alania TV y denegación de servicios en sitios web de Georgia y Azerbaiyán. Conectados el Departamento Central de Inteligencia (GRU) y el Servicio Federal de Seguridad (FSB) rusos.

---

[128] Titan Rain, (1968) Veterano de la Armada de los EE.UU., rastreó un anillo de ciberespionaje chino.

2008: Atacadas las campañas de Obama y McCain, presuntamente por China.

2000-2009: "GhostNet": penetración de objetivos políticos, económicos y medios tecnológicos en 103 países.

2009-2012: "Flame": software malicioso, complejo y multicomponente dirigido a Irán.

2009-2012: "Gauss": Similar a Stuxnet, enfocado a ciberespionaje.

2009-2010: "Operación Aurora": penetración para modificar el código fuente de Google, Adobe y otros.

2009-2011: "Night Dragon": Extracción de información de compañía energética.

2011: Se funda "LulzSec".

2011-2015: Grupo "Dragonfly", que se cree que es un grupo de patrocinio estatal, apuntan a industrias estratégicas: empresas de suministro energético, principales empresas generadoras de energía, operadoras de oleoductos, proveedores de equipamiento industrial energético, etc.

2012: Penetración en medios que cubren a un líder comunista corrupto: NY Times, Wall Street Journal, Washington Post.

2012: "Shamoon", 1er ciberataque de "borrado masivo", 30.000 ordenadores de Saudí Aramco, se cree que procede de Irán.

2013: "TeamSpy" (operación de ciberespionaje de una década de duración a través de Teamviewer, objetivos de perfil alto en países de Europa oriental y la comunidad de estados independientes (CEI), "MiniDuke" (vulnerabilidades avanzadas en Adobe Reader para recoger inteligencia geopolítica de objetivos de perfil alto, gobiernos e instituciones mundiales), "Red October" (Red de ciberespionaje avanzado con objetivos de agencias diplomáticas y gubernamentales), "NetTraveler" (red internacional principalmente china de ciberespionaje, cuyos objetivos son instituciones gubernamentales, embajadas, centros de investigación científica, complejos militares y empresas petrolíferas), "Icefog" (campaña de ciberespionaje centrada en ataques en la cadena de

suministro para empresas occidentales a través de objetivos en Corea del Sur y Japón), "Kimsuky" (campaña de ciberespionaje con el objetivo de think-tanks surcoreanos).

Junio 2013: Revelaciones de Edward Snowden sobre el programa de vigilancia global llevado a cabo por la NSA que comienzan en el diario británico The Guardian[129].

2014: "CosmicDuke" (dirigido a organizaciones diplomáticas, sector energético, operadoras de telecomunicaciones, contratistas militares e individuos implicados en el tráfico o venta de sustancias ilegales o controladas), "Epic Turla" (operación de ciberespionaje masivo apuntando a instituciones gubernamentales, embajadas, ejército, educación, investigación y compañías farmacéuticas en 45 paises), "The Mask" (atacantes hispanohablantes dirigidos hacia instituciones gubernamentales, empresas de energía, petróleo y gas y otras víctimas de perfil alto con instrumentos complejos), "Crouching Yeti" (campaña continua de espionaje con más de 2.800 objetivos de gran valor en todo el mundo), "Energetic Bear" (infiltrado en los ordenadores y sistemas de más de 1.000 organizaciones del sector global de energía, acceso a datos sensibles y poder de interrupción del abastecimiento energético). 2015: Ataques terroristas al semanal humorístico francés, Charlie Hebdo, los cuales son seguidos por unos 19.000 ciberataques a infraestructuras tecnológicas francesas llevados a cabo por hackers yihadistas o proislámicos. Anonymous lanza una dura campaña contra el EI y sitios web yihadistas. También son objetivas algunas cuentas de redes sociales del Mando Central de los Estados Unidos (US CENTCOM). Intrusión rusa en la Casa Blanca. "APT30", campaña de patrocinio estatal para obtener datos de activos del sudeste asiático (estados, empresas, periodistas, etc.) para China[130].

Entre los ciberespionajes más comunes encontramos el ciberespionaje industrial, el económico y el político.

---

[129] Edward, S (1983) Consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y la NSA

[130] Residencia oficial y principal centro de trabajo del Presidente de los EE.UU

La sociedad de la información, la ausencia de fronteras, la inmaterialidad de la comunicación lleva, en el ámbito de la seguridad mundial, a la falta de relevancia de los límites temporales y espaciales que han constituido, tradicionalmente, su término. La delincuencia informática y los ataques relacionados con ella representan un tipo de criminalidad específica y característica novedosa en los nuevos conflictos. Tal especialidad se asocia con los medios a través de los cuales se conforman estos ataques, como son los medios informáticos y telemáticos.

La mayoría de las sociedades mundiales afrontan una segunda revolución industrial, la "revolución informática", que está sustituyendo el trabajo de la mente humana por máquinas. Los avances tecnológicos en sistemas informáticos, con una capacidad de almacenar y procesar datos prácticamente ilimitados, ha supuesto, también, la introducción de nuevos valores y bienes dignos de ser salvaguardados por el ordenamiento jurídico con una quiebra de los esquemas tradicionales y necesidad de consiguientes modificaciones legales[131].

El espionaje industrial, espionaje económico o espionaje corporativo son formas de espionaje desarrollado con fines comerciales en lugar de fines de seguridad. El espionaje económico es ideado por los gobiernos y es de alcance internacional, mientras que el espionaje industrial o corporativo es normalmente nacional y se da entre las empresas o corporaciones[132]. Por otro lado, la inteligencia competitiva es la actividad de la recolección sistemática, análisis y gestión de la información sobre los competidores industriales.

El espionaje industrial se puede definir como “la actividad de obtener de manera encubierta información, comunicaciones y datos de terceros, de carácter industrial o mercantil y no disponibles para el conocimiento general del

---

[131] Marín Avella, V (2015), “Delitos informáticos”, Colegio Nuestra Señora de la Presentación-Centro, p. 18. Disponible en:
http://es.calameo.com/books/004366584de3db70b6465

[132] Lanz Raggio, M., y López Alfranca, Mª. d. V. (2015), “Ciberespionaje y derecho internacional”, Retos del derecho ante las nuevas amenazas / coord. por María Susana de Tomás Morales, p. 145.

público"[133], empleando técnicas como la penetración o la infiltración en empresas o corporaciones ajenas, el robo de datos, el soborno, o el chantaje.

En internet, ese tipo de ciberespionaje se basa en la misma búsqueda de la obtención de información y datos, pero se sirve de la tecnología disponible a través de red, para acceder a las informaciones y comunicaciones que discurren por Internet o se recopilan en los soportes informáticos o tecnológicos.

Los datos más buscados son los relativos a propiedad intelectual e industrial, patentes, y datos bancarios o económicos de organizaciones o industrias. Se habla de ciberespionaje industrial cuando se persiguen datos de empresas y organizaciones no militares, a diferencia del llamado "acceso a contenidos sin consentimiento" relativo a datos personales[134].

Los soportes en los que se puede practicar esta conducta no se circunscriben únicamente a ordenadores personales. El ciberespionaje se puede dar en tablets, smartphones, dispositivos de almacenamiento, o equipos tecnológicos de otra naturaleza. Todo sistema o soporte con capacidad de entrada y salida de datos, puede llegar a ser espiado, como por ejemplo la información personal de un directivo que trabaja desde su casa o vivienda.

A este respecto, los tipos de ciberespionaje se pueden producir, de acuerdo con los afectados o intervinientes, que son[135]:

1. Individuo-Individuo: Un ciber usuario consigue información y datos personales normalmente de otro empleado de una gran empresa o corporación, a través de su ordenador personal, su smartphone o su Tablet.

---

[133] Écija Bernal, Á. (2017), "Principales conductas antisociales de Internet. Análisis y propuestas de solución (I)", Diario La Ley, núm. 8956.

[134] Idem

[135] Idem

2. Individuo-Organización: Un ciber usuario recopila datos e información sobre una organización, directamente desde sus sistemas informáticos.

3. Organización-Organización: Una entidad logra información y datos de otra, normalmente competencia de la primera, para conseguir una ventaja competitiva.

4. Organización-Estado: Una entidad busca obtener información de las diferentes organizaciones en las que se divide el Estado (Ministerios, Agencias).

5. Estado-Estado: Un Estado recopila información y datos de otro beneficiando a las organizaciones que lo conforman, o con motivo de la Seguridad Nacional.

6. Estado-Individuo: Un Estado consigue información y datos personales de un individuo, de nuevo a través de su ordenador personal, smartphone y tablet, así como de los distintos registros y dispositivos oficiales.

La resolución de esta ciberconducta estaría en la proporcionalidad y en el cumplimiento o compliance de la normativa internacional. Si no se quiere crear alarma social ni vulnerar derechos fundamentales, se debe regular dicha actividad e informar a los ciudadanos.

El fin que se busca es entendible y consiste en defenderse de los ataques del crimen organizado y probablemente los demás Estados salen beneficiados de forma indirecta, aunque estas actividades de tratamiento informático de datos deberían seguir los procedimientos democráticos conocidos, como son el consenso internacional y la aprobación y divulgación de la correspondiente normativa.[136]

[136] Écija Bernal, Á. (2017), "Principales conductas antisociales de Internet. Análisis y propuestas de solución (I)", Diario La Ley, núm. 8956.

En referencia al espionaje económico, este aparece cuando alguien busca adquirir secretos comerciales intencionadamente para beneficio de algún gobierno o agente extranjero. Los competidores extranjeros intentan conseguir todo tipo de información financiera, comercial, científica o de ingeniería.

Un agente extranjero puede ser cualquier oficial, empleado público, apoderado, servidor, delegado o representante de algún gobierno extranjero. Estos agentes tienen como objetivo sustraer, esconder o comercializar algún secreto comercial a través de algún fraude. La forma de conseguirlo es copiar, descargar y distribuir los secretos comerciales sin autorización.

Los competidores extranjeros que buscan inteligencia económica a través de medios criminales generalmente operan de tres formas:

1. Establecen relaciones de negocios inicialmente honestas entre compañías extranjeras e industrias para obtener información económica, sin excluir obviamente los secretos comerciales.

2. Buscan e incorporan de manera agresiva a personas que tienen acceso a la información (normalmente de su misma nacionalidad) y que están trabajando para los Estados Unidos;

3. Realizan espionaje económico a través de acciones como el soborno, intrusión cibernética, robo, rastreo de información desechada (en busca de propiedad intelectual o prototipos) e intervención de líneas telefónicas; o bien,tal y como establece el Informe de Ciberamenazas y Tendencias. Edición 2017 publicado por el CCN-CERT, durante 2016 los servicios de inteligencia occidentales observaron un importante crecimiento del ciberespionaje económico, teniendo su origen en estados y empresas extranjeras, principalmente dirigido a las industrias de los sectores de defensa, alta tecnología, industria química, energía y salud buscando el acceso a desarrollos avanzados[137].

[137] CCN, Centro Criptológico Nacional,(2017) "Ciberamenazas y tendencias", CCN-CERT IA-16/17,, p. 12.

Las motivaciones habituales que persiguen los estados atacantes son las siguientes:

1. Despojar de la propiedad intelectual y la inteligencia sobre las capacidades militares del estado atacado;

2. Negar el uso del estado atacado de sus canales de comunicación en el ciberespacio;

3. Aprovechar las capacidades militares del estado atacado empleando sus recursos militares y de inteligencia, conociendo las vulnerabilidades del estado atacado;

4. Obtener información sobre los planes militares del estado atacado;

5. Realizar actividades insurrectas utilizando sus servicios de inteligencia; y

6. Utilizar proxies o un gran número de elementos externos para cubrir el verdadero origen de sus actividades dentro del ciberespacio.

En los últimos años, el CCN-CERT pronostica un aumento en el ciberespionaje (incluyendo a los dispositivos móviles) en donde se utilizarán exploits de día cero, con vectores de infección desconocidos, diversos canales de exfiltración y técnicas de persistencia avanzadas que emplearán funciones no documentadas.

Como afirman todos los expertos, el espionaje económico se ha multiplicado en los últimos años, fomentado por la crisis económica. El escenario puede ser tanto intranacional como Internacional, como ocurre con frecuencia creciente.

A nivel estatal, se puede considerar que estamos sumidos en una guerra oculta, pero con potencial para provocar daños inmensos, no sólo a empresas sino a todo el tejido económico industrial de un país.

Tanto la amenaza como la necesidad de hacerle frente, están claras; y la recientemente aprobada Estrategia Española de Seguridad así lo refleja, indicando el camino que debe imperiosamente seguirse para garantizar la seguridad de tan importante aspecto nacional.

Pata finalizar en este punto, reseñar que el ciberespionaje político, con origen en los servicios de inteligencia extranjeros, supone una de las principales

amenazas para la seguridad internacional ya que afectan a cuestiones de ámbito nacional o internacional. Europa y España no quedan fuera de esta amenaza: durante 2016 se han revelado multitud de ataques de este tipo que han buscado obtener información de ámbito político, económica o estratégica, así como planes de desarrollo y posiciones nacionales en relación a debates o negociaciones abiertas[138].

5.4 AGENTES DE LA CIBERDELINCUENCIA

Hoy en día, los delincuentes han creado un modelo de operación formalizada y una estructura muy similar a los negocios legales, lo que aumenta el retorno de la inversión (ROI) de la organización criminal durante todo el ciclo de vida del ataque. Los elementos críticos de la "cadena de valor" de los Ciberdelincuentes son:

- Logística, que abarca tanto a las personas como a los sistemas usados para distribuir los bienes adquiridos, ya sean datos de tarjetas de crédito robadas, registros médicos o propiedad intelectual.

- Gestión de recursos humanos, que incluye reclutamiento, investigación de antecedentes y pago al "personal" necesario para cumplir con los requisitos específicos del ataque.

- El desarrollo técnico, que es responsabilidad de los "trabajadores" de primera línea que proporcionan los conocimientos técnicos necesarios para llevar a cabo cualquier ataque, incluyendo investigación, explotación de la vulnerabilidad y automatización.

- El equipo de operaciones, que garantiza el correcto flujo de información y de fondos durante el ciclo de vida del ataque. Este grupo busca activamente reducir costes y maximizar el retorno de la inversión en cada paso que dan.

---

[138] CCN, Centro Criptológico Nacional,(2017) "Ciberamenazas y tendencias", CCN-CERT IA-16/17,, p. 12.

•El equipo de marketing y ventas, que garantiza que la reputación del grupo atacante en el mercado underground es fuerte y cuenta con la confianza del tipo de compradores que demandan estos servicios.

Para poseer una visión global en el que encajar las acciones de los ciberdelincuentes, en la siguiente tabla se muestran las Ciberamenazas[139] más significativas de los últimos años, incluyendo sus agentes y los objetivos perseguidos.

HACKTIVISTAS

El término "Hacktivismo" es un acrónimo del término hacker. El termino activismo hace referencia a la actitud de las personas que participan en movimientos, especialmente de tipo político y social. Según el autor Samuel Alexandra, el Hacktivismo se entiende como "la utilización no violenta de herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos. Estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software" (ALEXANDRA, 2004). A menudo se entiende por la escritura o reescritura de programas informáticos, a efectos de directa o indirectamente promover o privilegiar una ideología política, y por lo general potenciando estrategias o políticas tales como libertad de expresión, derechos humanos, y ética de la información. Los actos de hacktivismo son llevados a cabo bajo la creencia de que las utilizaciones de esas estrategias informáticas tendrán efectos de palanca similares por ejemplo al activismo regular o la desobediencia civil. Se basa en la idea de que poca gente conoce lo suficiente de computación e Internet como para intervenir en pro de un determinado fin, pero esta forma de acción puede afectar a mucha gente.

El término hacktivismo es muy controvertido. Algunos afirman que se acuñó para describir cómo las acciones directas electrónicas podían usarse en favor del cambio social al combinar la programación con el pensamiento crítico.

[139] CCN, Centro Criptológico Nacional,(2017) "Ciberamenazas y tendencias", CCN-CERT IA-16/17,,IA 09/16. Ciberamenazas 2015 y tendencias 2016

Otros utilizan el término como sinónimo de actos maliciosos y destructivos que vulneran la seguridad de Internet como una plataforma tecnológica, económica, y política.

Dentro del Hacktivismo, nos podemos encontrar con los autodenominados ANONYMOUS, que sería un grupo de individuos, más o menos organizados, que desarrollan sus acciones en el ciberespacio movidos generalmente por motivos ideológicos. Su imagen más representativa es la máscara de Guy Fawkes[140], la cual se hizo tan famosa a raíz del argumento de la película V de Vendetta, y que han tomado como ideología propia. En los últimos años sus ciberataques (desconfiguración de páginas web, ataques DDoS o sustracción de datos confidenciales de sus objetivos) pretendieron ser la respuesta a determinadas medidas adoptadas por gobiernos y que consideraban perjudiciales para la libertad de Internet.

CIBERYIHADISMO

A lo largo del año 2015, aparecido en el ciberespacio una nueva amenaza, vinculada estrechamente con los hechos acaecidos hasta la fecha en el conflicto bélico de Siria, y que por su vinculación con el "Internet de las cosas" se denominó, CIBERYIHADISMO.

Este término se vinculó inicialmente con los diferentes grupos de insurgentes que florecieron en el inicio de la guerra civil de Siria, en el año 2011, aunque desaparecidos la mayoría de ellos, únicamente ha prevalecido el mal denominado Estado Islámico[141] (Daesh en su acrónimo en árabe), los cuales usando métodos, procedimientos y herramientas del terrorismo propiamente

[140] Guy Fawkes: (York, 13 de abril de 1570-Londres, 31 de enero de 1606), fue uno de los componentes del grupo de católicos ingleses que intentó asesinar al rey Jacobo I de Inglaterra, en la fallida conspiración de la pólvora en 1605

[141] Grupo terrorista insurgente de naturaleza fundamentalista yihadista wahabita formado por radicales, que en junio de 2014 autoproclamó el califato islámico, pidiendo lealtad a todos los musulmanes del mundo.

dicho, el hacktivismo y la ciberguerra constituye una realidad naciente y supone una de las mayores amenazas con las que se enfrentarán las sociedades occidentales en los próximos años.

Las importantes vías de financiación de estos grupos hacen posible que puedan llegar a adquirir los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los mismos. Hasta el momento, sus ataques se han limitado a la desfiguración de páginas web, ataques DDoS a pequeña escala o, más comúnmente, al uso de Internet y de las redes sociales para la diseminación de propaganda o el reclutamiento y la radicalización, actividades que no exigen grandes conocimientos o infraestructura.

CIBERVANDALISMO

Se denomina cibervándalos a aquellos individuos que, poseyendo significativos conocimientos técnicos, llevan a cabo sus acciones con el único motivo de demostrar públicamente que son capaces de hacerlo. Por su parte, los denominados SCRIPT KIDDIES son aquellos que, con conocimientos limitados y haciendo uso de herramientas construidas por terceros, perpetran sus acciones a modo de desafío, sin ser, en muchas ocasiones, plenamente conscientes de sus consecuencias.

CIBERINVESTIGADORES

Los ciberinvestigadores tratan de buscar las vulnerabilidades que existen en los entornos TIC´s, con el único objetivo de verificar las medidas de protección y seguridad con la que cuentan los sistemas los cuales están investigando. Usualmente, estos ciberinvestigadores realizan sendos informes para empresas, bajo contrato previo, con el fin de informarles de las debilidades de sus herramientas y/o sistemas, pudiendo también realizar un efecto negativo como parte de Sujetos activos de la ciberdelincuencia, y es la publicación en ciertos foros y páginas web de dudosa reputación de estas vulnerabilidades, facilitando la acción de los atacantes, que pueden llegar a beneficiarse de los resultados de las investigaciones. Incluso, se han dado casos de ciberinvestigadores acusados de realizar extorsiones a las entidades investigadas.

-CIBERESPACIO Y TERRORISMO: YIHADISMO 2.0-

VI. CIBERESPACIO Y TERRORISMO: YIHADISMO 2.0

Organizaciones terroristas en el ciberespacio.

El reciente desarrollo y uso de las nuevas tecnologías a través del ciberespacio ha dado lugar a un aumento considerable de la interdependencia y la interconexión a nivel global. Con todo ello podríamos afirmar que la Sociedad Internacional actual no ha obtenido más que beneficios de ello. Tanto la economía como el intercambio de información sensible entre empresas, gobiernos y ciudadanos se ha agilizado de forma muy considerable. No obstante, si efectuamos un profundo análisis de la situación, podremos vislumbrar que el mundo global no ha obtenido únicamente beneficios, sino también nuevos riesgos y amenazas a los que deben hacer frente de la manera más segura posible. En este sentido las medidas implementadas durante los últimos diez años no han sido lo suficientemente eficientes para mejorar la seguridad en la dimensión virtual por parte de los Estados-Nación ni eficaces para garantizar la existencia de un ciberespacio libre de riesgos y amenazas. Una de las consecuencias más visibles de ello es el aumento desmesurado e incontrolado de la propaganda terrorista.

Evolución y cambios producidos en el ciberespacio.

La primera Web apareció durante los años noventa y ha evolucionado considerablemente, habiendo pasado ya por dos configuraciones diferentes. El un primer momento fue la paginaWeb 1.0, donde no existían buscadores, exploradores ni interrelación participativa. En la actualidad estamos situados en el segundo estadio donde la Web en la que operamos, la 2.0, ya ofrece mayores recursos como son la interconexión, la interacción, los foros y las redes sociales.

La Web 1.0 evolucionó a la Web 2.0, un concepto que se acuñó en 2003 y hace referencia al fenómeno social surgido en él, en el cual un sujeto pasivo que recibía la información sin apenas posibilidades pasase a ser interactivo. Con la Web 2.0 el usuario se convirtió en el protagonista de la red, lo que supuso el auge

de blogs, las redes sociales, y otras herramientas de difusión de la información, lo que se conoce como la Web participativa[142]

La web primitiva del siglo XX, conocida como Web 1.0, se caracterizaba principalmente por ser unidireccional, realizándose sobre contenidos estáticos. Las primeras páginas que se subieron a Internet publicaban contenidos de texto que no se podían modificar a menos que no lo hiciese el webmaster, o administrador del sitio web. Tenía una función puramente divulgativa, utilizada principalmente para subir documentos e información cultural, por lo que el webmaster tenía control absoluto sobre lo que se publicar. El advenimiento de la Web 2.0, a mediados de la primera década de este siglo, revolucionó el concepto de red, cambiando las formas de comunicación y adaptándolas a la colaboración y participación entre los usuarios. El objetivo principal de esta nueva web es el intercambio del conocimiento, se trata de una web colaborativa en la que los usuarios pueden generar cualquier tipo de contenido y divulgarlo a través de blogs, foros y, por último, las redes sociales[143].

De estas líneas surge la definición del ciberespacio como un ente en constante trasformación cuyo motor principal es la constante inversión en tecnologías en todos los ámbitos de nuestras vidas, tanto en el ámbito civil como en el militar, con desmesurado y descontrolado aumento de la dependencia para el desarrollo de nuestras vidas de Internet. Cada vez dependemos en mayor medida del uso del ciberespacio ya que cada vez es mayor el número de actores que utilizan la red digital para desarrollar sus tareas.

Esta metamorfosis desproporcionada, incontrolable e impredecible representa la primera brecha en materia de seguridad. Los cambios tan agresivos y constantes que sufre el ciberespacio, principalmente a través de las redes sociales, hacen que los propios encargados de diseñar y proteger las mismas se

---

[142] Calvo, S. (2013) 'De la web 1.0 a internet invisible vulnerabilidades, amenazas y delitos'. en Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. ed. por Ministerio de Defensa. Madrid: Ministerio de Defensa, 491-526

[143] Carlini, A. (2018) 'Las redes sociales como factor de desestabilización'. Instituto Español de Estudios Estratégicos.

encuentren superados con la consecuente incertidumbre que ello proporciona. La Web evoluciona a una velocidad tal que los mecanismos de protección cibernéticos nunca están plenamente actualizados. Esto provoca que, por ejemplo, los cortafuegos digitales o los antivirus siempre se sitúen frente a los ciberataques que puedan diseñar los terroristas, los piratas informáticos o las empresas que se dedican al espionaje industrial en una posición de gran desventaja

The new millennium has had a major impact; the world in which we live is changing. The information society is becoming a global society; the growth of electronic businesses is developing new industrials markets on a global basis. But the information society is built on a very fragile framework the Internet. The Internet is at risk from attacks, historically it was sole hackers, but we are now seeing the development of cyber terrorist organisations[144].

Desde este análisis, podemos afirmar que el ciberespacio se caracteriza desde su nacimiento por una imparable mutabilidad, conllevando consigo el gen de la inseguridad. Es evidente que las amenazas que podemos encontrar en el ciberespacio están más avanzadas que los mecanismos de defensa que disponemos, provocando con ello que los sistemas de alerta temprana no puedan avisar a tiempo de ciertas amenazas y por tanto no cumplen sus funciones. Por lo tanto es fácil prever que este medio seduce a un número elevado de terroristas que consideren más seductor el uso de Internet y se va incrementando exponencialmente.

Torres Soriano, "el uso que de Internet llevan a cabo las redes del terrorismo yihadista se encuentra sometido a una continua y rápida transformación" (2009: 1), que tiene como resultado "un amplio uso de Internet como herramienta de comunicación segura, coordinación operacional, obtención de inteligencia, cibersabotaje, aprendizaje, etc."[145]

---

[144] Warren, M. (2007) 'Terrorism and the internet'. en Cyber Warfare and Cyber Terrorism. ed. Por Janczewski, L. & Colarik, A. Nueva York: IGI Global - Information Science Reference, 42-49

[145] Torres, M. (2009) El eco del terror: ideología y propaganda del terrorismo yihadista. Madrid: Plaza y Valdés.

Dicho esto, y teniendo en mente que la presencia terrorista en el ciberespacio es algo fehaciente y con un crecimiento masivo, surge la reflexión de cómo se ha transformado la red desde el punto de vista de la seguridad.

Internet era en principio todo lo contrario a un lugar de control porque los usuarios no se localizaban geográficamente de forma definida, sus interconexiones eran topológicas y no había un gran ojo robotizado que pudiera controlar todo como en las arquitecturas carcelarias de Jeremy Bentham y su modelo panóptico de vigilancia y control del siglo XVIII.

Pero ante el aumento exponencial de las amenazas y riesgos en la red numerosos Estados están desarrollando políticas que promueven limitar la privacidad y la libertad en la misma y sus ciberterritorios a cambio de una supuesta mayor garantía de seguridad. Con estas iniciativas, en pro de la seguridad, se van reduciendo los márgenes de libertad que es lo que hasta el momento había definido al ciberespacio.

Think about your phone or your tablet. They know for example where you are […] but with your permission, you give us more information about you. You give us information about some friends of you and we can probable use some of that information, again with your permission, to improve the quality of researches. The next thing that we can do is we can take pictures and do the same thing […] All of this is about improving accuracy so one of the things eventually happens is that we do not need you to type it all because we know where you are, with your permission. We know where you've been, with your permission. We can more or less now what you're thinking about[146].

Avanzando con esta postura, buscan intentar un aumento rápido y considerable de la seguridad cibernética a cambio de acotar el anonimato, la intimidad y la libertad la red.

[146] Schmidt, E. (2010) 'From the archives'. Washington Ideas Forum. 1 de octubre de 2010 en el The nAtlantic-Washington Ideas Forum

Que en Estados Unidos se haya denunciado una cantidad masiva de datos recogidos sin permiso previo procedentes de todo tipo de ciudadanos no ha favorecido que las agencias de seguridad americanas hayan mejorado sus mecanismos de defensa frente a las ciberamenazas.

En esta misma línea, en 2015, un analista de gran presitigo de seguridad internacional, Bruce Schneier, llevo a cabo en su sección de la revista el análisis de las declaraciones de un agente de la NSA en referencia al debate sobre la libertad de las personas frente al control en la red, el poder del dato y del metadato y la situación de control en que todos los ciudadanos estamos inmersos:

When you have one person under surveillance, the contents of conversations, text messages, and emails can be more important than the metadata. But when you have an entire population under surveillance, the metadata is far more meaningful, important, and useful. As former NSA General Counsel Stewart Baker said: Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content. In 2014, former NSA and CIA director Michael Hayden remarked: We kill people based on metadata[147].

La conclusión que se extraer de los documentos previamente citados es que el ciberespacio continúa creciendo, su mutabilidad continúa siendo impredecible y las medidas destinadas a incrementar la seguridad en internet no han alcanzado el objetivo de evitar la expansión de las amenazas 2.0.

En los últimos tiempos se han destinado muchos recursos, tanto humanos como económicos, destinado principalmente a llevar a cabo la adopción de una serie de medidas importantes tendentes a combatir todas las actividades terroristas que se llevan a cabo en Internet, tanto en el ámbito nacional como internacional. A pesar de ello, y sin profundizar en la evaluación de la eficacia de estas medidas, debe asumirse que la propia naturaleza de Internet determina que

[147] Schneier, B. (2015) 'NSA doesn´t need to spy on your calls to learn your secrets'. Wired, marzo de 2015.

la lucha contra las actividades terroristas en Internet nunca podrá alcanzar sus objetivos plenamente[148].

6.1 MOTIVOS POR LOS QUE EL TERRORISMO PASA A OPERAR EN EL CIBERESPACIO.

Los conflictos entre seres humanos han ido evolucionando con el paso del tiempo y como consecuencia de ello la comisión de actos delictivos y bélicos ha ido conociendo diferentes escenarios, como la tierra, el mar, el aire y el espacio. Todas estas dimensiones de conflicto pertenecen a un plano material o tangible. Con la entrada del siglo XXI y el desarrollo de Internet, especialmente con las redes de comunicaciones, han hecho posible que surja una nueva dimensión de carácter intangible en la que los actores de la Sociedad Internacional pueden combatir sin la necesidad de enfrentarse cuerpo a cuerpo, de forma anónima y sin una delimitación del terreno de combate; con ello nace ciberespacio. Esta nueva forma de atacar es diferente a la utilizada en los conflictos anteriores, evidentemente por la existencia de este ciberespacio, surgiendo con ello una nueva amenaza en este tipo de conflictos bélicos.

De la misma manera que los conflictos entre Estados-Nación se llevan a cabo en el ciberespacio, comprobando como las organizaciones terroristas como el Daesh también están trasladando sus operaciones a esta nueva dimensión. La expansión del terrorismo a través de la red evidencia la compleja situación en la que nos encontramos, en tanto, los conflictos clásicos se trasladan y metamorfosean en la red. Podemos afirmar el ciberespacio ya se ha constituido a día de hoy como la primera línea de batalla de los principales conflictos contemporáneos.

Con el desarrollo de este nuevo escenario y su expansión a todos los niveles sin límite alguno, llegamos a un punto importante de inflexión sobre el estudio de las Relaciones Internacionales y la Seguridad Internacional. Sus efectos y consecuencias hubieran sido difícilmente imaginables pocos años atrás. Hoy día,

---

[148] Torres, M. (2009) 'Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda'. Real Instituto Elcano. [en línea] (ARI 110) 1-9.

los actores que componen la Sociedad Internacional ya no sólo se enfrentan dentro de la realidad tangible, sino también dentro de una realidad intangible o virtual.

Seguidamente llevaremos a cabo un estudio de las principales razones por las que los conflictos a nivel general y el terrorismo yihadista a nivel particular se trasladan al ciberespacio.

En primero lugar nos encontramos con el anonimato y la impunidad que conlleva. El anonimato que existe en el ciberespacio y la dificultad de configurar procesos de atribución son el principal motivo por el cual los terroristas apuestan en la actualidad por actuar en numerosas ocasiones a través de la red. Se ha observado un aumento diario del número de ciberataques, así como el sustancial aumento, prácticamente diario, del uso de Internet con fines terroristas. Queda evidenciado que se deben principalmente al anonimato con el que se puede operar en la red digital y la ineficacia de los procesos de atribución de responsabilidades tras cometer un ciberataque:

Según un estudio prestigioso, el 95% de los ciberdelitos cometidos quedan impunes. Esto tiene gran importancia nacional e internacional, por el peligro que supone para los ciudadanos, la economía y las infraestructuras críticas[149].

Esta imposibilidad de controlar desde el punto de vista del Derecho Internacional el potencial uso terrorista de Internet ha llevado consigo que la prevención de ciberataques sea un objetivo caracterizado por una gran dificultad ya que "siempre existirá la posibilidad de que cualquiera, desde el salón de su casa, pueda generar y extender un código de catastróficas consecuencias"[150].

Conscientemente podemos llegar a la conclusión que el ciberespacio es un campo sistémico en constante metástasis donde las réplicas entre las IP de los millones de ordenadores que existen en el planeta se producen un espacio de ecos

[149] Duva, J. (2014) 'El 95% de los ciberdelitos cometidos quedan impunes'. El País.

[150] López, J. (2012) 'La evolución del conflicto hacia un nuevo escenario'. en El ciberespacio. Nuevo escenario de confrontación. ed. por Ministerio de Defensa. Madrid: Ministerio de Defensa, 117-166

donde es prácticamente imposible localizar el origen o el autor de un ciberataque terrorista.

El comportamiento terrorista en un ciberentorno ofrece innumerables ventajas operativas para lograr objetivos tantos tácticos como los estratégicos con un elevado anonimato. Ante esta evidencia, las organizaciones terroristas emplean la tecnología informática como una fuerza multiplicadora para facilitar, conformar y diseminar propaganda política y para asegurarse el sigilo y el anonimato tanto las actividades rutinarias como las operaciones tácticas; y para facilitar operaciones que resultan rentables en términos de recursos invertidos[151].

Con la dimensión digital y el anonimato que se produce en ella se plantea un importante problema ya que dificulta, y en ocasiones impide, a las autoridades la identificación de quien o quienes están desarrollando acciones terroristas con "capacidad suficiente para provocar un ciberataque del que derivaran efectos similares a los producidos por el uso de la fuerza armada y actuar así con la debida diligencia"[152].

Internet permite que un terrorista o un simpatizante radical puedan lanzar un ciberataque a cualquier parte de mundo así como publicar contenidos terroristas llegando a millones de individuos sin temor a que le localicen o identifiquen, y consecuentemente, no sufrirá represalia alguna. A este respecto resulta interesante señalar el uso del ciberespacio para difundir propaganda terrorista o generar ingresos para financiar atentados es algo que ya empezó a hacer Al Qaeda bastantes años atrás:

Azzam Publications, based in London and named after Sheikh Abdullah Azzam, a mentor of Osama bin Laden; is a site dedicated to Jihad around the world and linked to Al Qaeda. It is alleged that the Azzam Publications site, which sold Jihad related material from books to videos, was raising funds for the

---

[151] Ranstorp, M. (2004) 'Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información'. Madrid: Editorial Temas de Hoy S.A., 201-221

[152] Torrecuadrada, S. (2013) 'Internet y el uso de la fuerza'. en Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio. ed. por Universidad de Granada. Granada: Universidad de Granada, 91-118

Taliban in Afghanistan and for guerrillas fighting the Russians in Chechyna. After September 11, Azzam Publications came under increased pressure to the point where its products could no longer be purchased through their site.

En definitiva, el ciberespacio, como escenario de confrontación en la actualidad, permite a cualquiera individuo publicar desde cualquier parte del mundo contenidos de todo tipos, mensajes e ideologías radicales, realizar proselitismo o lanzar un ciberataque y, posteriormente, borrar cualquier vestigio o huellas digitales que puedan hacer que las autoridades amenazadas o atacadas puedan detenerlo.

Las investigaciones forenses de la última década, así como los procesos de atribución de responsabilidades son en la mayoría de los supuestos ineficaces cuando su función está destinada de aclarar la autoría de un ataque cibernético y conseguir con ello su impunidad. La posibilidad de emprender de forma anónima acciones destructivas o disruptivas contra la población occidental convierte al ciberespacio en una dimensión muy atractiva para las organizaciones terroristas.

En segundo lugar, el ciberespacio pone a disposición de los grupos terroristas un medio de comunicación prácticamente instantáneo. Al igual que las empresas que operan en bolsa o los ciudadanos que utilizan sus ordenadores para llevar a cabo gestiones bancarias, los terroristas hacen uso de Internet para intercambiar información ya que son conscientes que no existe en la actualidad otro mecanismo de comunicación más rápido y eficaz que los que proporcionan las plataformas digitales para poder operar y conversar de forma segura y en tiempo real. El desarrollo del ciberespacio ha dado a los terroristas nuevos medios a través de los cuales pueden comunicarse sin tener que preocuparse en gran medida por los controles de las autoridades.

La ciberguerra es un proceso con gran auge y sin poder controlarlo, desarrollándose a la velocidad de la luz. Una vez los mensajes y la información atacantes han empezado a correr por los cables de fibra óptica, el tiempo entre el

lanzamiento de un ataque y su efecto apenas puede medirse, lo que supone nuevos riesgos para los encargados de tomar las decisiones durante las crisis[153].

Los microsegundos en los que se tarda en enviar un mail, llevar a cabo una transferencia, publicar un video de una decapitación o lanzar un ciberataque ya no es solo una característica capital que diferencia al ciberespacio de cualquier otra dimensión o campo de actuación, sino también un motivo principal por el que los terroristas cada vez apuestan más por llevar a cabo muchas de sus actuaciones a través de este medio.

En este momento, son las agencias contraterroristas las destinadas para ejercer el control que resulta ser cada vez más férreo debido principalmente a la instantaneidad y eficacia que ofrece el ciberespacio para llevar a cabo cualquier gestión u operación es un factor clave para entender por qué la red digital cada vez despierta un mayor interés en las organizaciones terroristas.

El tercer aspecto a tener en cuenta es la enorme dimensión cibernética, configurándola como un campo de conflicto que promueve la existencia de enfrentamientos asimétricos. En la dimensión virtual de los nuevos conflictos bélicos, a diferencia de lo que ocurría en los conflictos bélicos que se llevaron a cabo a lo largo de nuestra historia, en la mayoría de las ocasiones esta dimensión virtual difiere mucho de la dimensión física o real en la cual dos actores con una potencia de fuego y unos recursos radicalmente desequilibrados pueden enfrentarse de forma directa. En este sentido, sabiendo que el terrorismo se basa en una lógica de enfrentamiento que defiende que no se puede combatir a la potencia enemiga de modo directo sino a través de "métodos no convencionales del empleo de la violencia"[154], el ciberespacio se configura como unos de los medios más que adecuado para llevar a cabo el enfrentamiento asimétrico que los terroristas buscan con el fin de desgastar a la potencia enemiga que los oprime.

---

[153] Clarke, R. & Knake, R. (2011) Guerra en la red. Los nuevos campos de batalla. Madrid: Editorial Ariel.

[154] Münkler, H. (2005) Viejas y nuevas guerras. Asimetría y privatización de la violencia. Madrid.

De estas líneas subyace la idea de que las armas cibernéticas han alterado la forma de comprender las relaciones internacionales y han revolucionado la manera de hacer la guerra. "Un ordenador, un sistema o una red desprotegida es una ciberarma esperando a ser cargada y utilizada, y hasta que aceptemos esta premisa estamos todos bajo riesgo"[155].

El constante desarrollo de las redes sociales ha provocado que los conflictos adquieran un carácter cada vez más asimétrico haciendo posible que la parte supuestamente más débil pueda atacar a un oponente convencionalmente más fuerte a través del uso de herramientas virtuales, con menos recursos pueden llegar a producir un resultado muy dañino, lo que conlleva que aumente el peligro y sea más sencillo atacar. Esta es una de las diferencias con los conflictos bélicos anteriores y una de las características de lo que vengo a definir en mi teses como amenaza híbrida.

Para finalizar este punto, sería muy conveniente destacar que el ciberespacio se entiende como un escenario de conflicto donde los terroristas con menos recursos pueden enfrentarse con sus enemigos de igual a igual. Con el simple acceso a una plataforma digital cualquier terrorista puede atacar a sus enemigos sin correr el riesgo de ser identificado o neutralizado. Todo esto ha conllevado una preocupación a nivel internacional, dando gran prioridad en términos de seguridad a la ciberdefensa y la ciberseguridad.

En cuarto lugar, es imprescindible resaltar que el ciberespacio se caracteriza por ser un campo de información y de acción completamente abierto a cualquier ciudadano y consecuentemente a cualquier terrorista. El desarrollo de las TIC´s y la constante inversión en el perfeccionamiento de la red digital han provocado que el ciberespacio haya sufrido un uso exponencial a lo largo y ancho de todo el mundo. Se podría decir que la extensión tecnológica ha sido tal que prácticamente se ha democratizado globalmente el acceso al ciberespacio.

[155] Caro, M.J. (2010), 'Alcance y ámbito de la seguridad nacional en el ciberespacio'. en La seguridad un concepto amplio y dinámico. V Jornadas de Estudios de Seguridad.

El principal problema se encuentra en que la citada democratización no sólo tiene efectos positivos, sino que también tiene efectos extremadamente dañinos para la seguridad internacional.

Internet es una gran red con un diseño descentralizado. Los diseñadores de Internet no querían que pudieran controlarla los gobiernos, ya fuera de forma individual o colectiva, de modo que diseñaron un sistema que otorga mucha más prioridad a la descentralización que a la seguridad[156].

Cualquier usuario o destinatario de Internet puede sufrir un robo de identidad y ser vigilado, incluso ser captado, por una célula terrorista y pasar a convertirse en un potencial terrorista individual o en una víctima de los mismos.

En esta sentido, académicos de renombre internacional en estudios sobre terrorismo como Magnus Ranstorp y David Rapoport advierten que el acceso prácticamente ilimitado y descontrolado al ciberespacio se convierte en un elemento imprescindible para explicar por qué muchas organizaciones terroristas han apostado tan fuerte por el uso de la red: "El ciberespacio ha permitido al grupo/movimiento terrorista sobrevivir incluso a las presiones de las más severas medidas de seguridad implantadas dentro de los Estados" [157].

Es importante reseñar que "la extensión del terrorismo en el curso de los últimos decenios del siglo XX no obedece en consecuencia a una revolución de los medios de la violencia, sino a una explotación de la revolución mediática"[158].

De este texto podemos extraer la idea basada en afirmar que el desarrollo del ciberespacio y la posibilidad de acceder a él sin ningún filtro que lo impida ha permitido que las operaciones terroristas se hayan propagado de forma dramática a lo largo de todo el mundo.

---

[156] Clarke, R. & Knake, R. (2011) Guerra en la red. Los nuevos campos de batalla. Madrid.

[157] Ranstorp, M. (2004) 'Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información'. en El nuevo terrorismo islamista. Del 11-S al 11-M. ed. por Reinares, F. y Elorza, A. Madrid

[158] Münkler, H. (2005) Viejas y nuevas guerras. Asimetría y privatización de la violencia. Madrid

Para finalizar con este punto de estudio, podemos concluir que la facilidad con la que se puede acceder a las bases de datos disponibles en el ciberespacio actual, como consecuencia del aumento de la redes sociales de comunicación, ya no sólo es una característica que defina el mismo, sino también es una aspecto muy importante y preocupante a tener en cuenta cuando nos preguntamos por qué muchas organizaciones terroristas que identifican el mundo digital como uno de sus principales escenarios de actuación.

En quinto lugar, analizáramos el aspecto económico. El ciberespacio proporciona a aquellos que hace usos de él y que por tanto actúen en mismo una alta rentabilidad económica. Desde el diseño hasta la construcción y el lanzamiento de un ciberataque, requiere una inversión financiera menor si la comparamos con los recursos monetarios que se exigen para realizar un atentado físico convencional y tradicional. El hecho de que Internet sea una plataforma accesible prácticamente desde todos los lugares del planeta y que tanto el hardware como el software tengan cada vez un precio menor, invita a los miembros de los grupos terroristas a trasladar sus contiendas a la dimensión virtual.

Otro aspecto para tener muy en cuenta y muy característico es que el terrorismo se expande rápidamente al ciberespacio debido a la capacidad y flexibilidad operativa que este ofrece. Ya hemos definidos en puntos anteriores las facilidades que proporciona para llevar a cabo esta expansión.

Organizaciones terroristas, como pueden ser el Daesh o Al Qaeda, dirigen sus ataques haciendo uso de este medio principalmente debido a la capacidad destructiva y garantía de alcance que ofrecen los ciberataques. Un ataque de denegación de servicio o una bomba lógica, dentro de la multitud de amenazas cibernéticas que pueden diseñarse, no sólo tienen una gran capacidad de dañar, alterar, robar o borrar la información que se desee, sino que también garantizan el cumplimiento de la misión.

Para concluir con esta descripción tan detallada, una de las principales características del ciberespacio es que se trata de un campo que evoluciona a velocidades impresionantes provocando con ello que los mecanismos de control y de la ciberseguridad siempre vayan a remolque de las amenazas. En muy difícil prevenirse de una amenaza que no ha existido nunca.

Esta ausencia de los sistemas de alerta temprana da lugar a la inexistencia en muchas ocasiones de los mecanismos de prevención de ciberataques y la incapacidad de limpiar las redes sociales de contenidos terroristas principalmente debido a su carga constante desde diferentes puntos del planeta es algo que motiva que los responsables de dicha propaganda apuesten por el ciberespacio como su nuevo campo de trabajo. Un claro ejemplo lo encontramos en Abu Bakr al-Baghdadi con la declaración el califato, la importancia del cibercalifato siempre ha sido mayúscula.

El hecho de que cualquier terminal conectado a la red pueda ser una potencial arma de propaganda, infiltración, destrucción o disrupción aumenta considerablemente las posibilidades de los terroristas de alterar el equilibrio securitario de sus enemigos. El aumento de la interdependencia y la interconexión entre todos los actores de la escena internacional aumenta las probabilidades de que una campaña de amenazas o un simple ciberataque tenga éxito.

En definitiva, tal y como anticipábamos al principio del apartado, el ciberespacio no es únicamente la quinta dimensión donde los seres humanos se enfrentan, sino también la primera línea de batalla donde se libran los principales conflictos actuales, una de la más que evidentes amenazas híbridas.

6.2 HERRAMIENTAS UTILIZADAS PARA AMENAZAR EN ESTE MODELO DE AMENAZA HÍBRIDA.

Los atacantes están haciendo un uso masivo de herramientas desarrolladas para otros fines distintos a los utilizados en los nuevos conflictos bélicos, tales como la monitorización de sistemas o la realización de pruebas de penetración. Algunos ejemplos de ello son los servicios SaaS (Software as a Service o booter services), que permiten a los atacantes perpetrar ataques de Denegación de Servicios Distribuidos (DDoS) a través de un sitio web.

EXPLOITS, EXPLOIT-KITS Y EXPLOIT DRIVE-BY

Del inglés exploit, "explotar" o "aprovechar", es un programa informático malicioso (malware) que intenta utilizar y sacar provecho de un bug o vulnerabilidad en otro programa o sistema. Se suelen corregir con hotfixs o parches.

Los exploits suelen utilizar vulnerabilidades como: desbordamiento de buffer, condición de carrera (race condition), error de formato de cadena (format string bugs), Cross Site Scripting (XSS), Inyección SQL, Inyección de Caracteres (CRLF), denegación del servicio, Inyección múltiple HTML (Multiple HTML Injection), ventanas engañosas (window Spoofing), etc.

Estas herramientas no sólo se utilizan en páginas web dudosas, sino también en aquellas otras absolutamente legítimas y fuera de sospecha. También son muy comunes los ataques por Watering Hole[159] que constituyen un mecanismo habitual para iniciar ataques dirigidos especialmente cuando las páginas web infectadas son de visita frecuente por parte de personas de la organización-víctima. Sin embargo, los exploit- kits más habituales se centran en Adobe Flash.

CÓDIGO DAÑINO / RANSOMWARE / CRYPTOWARE

El código dañino es un software que realiza funciones no deseadas, no solicitadas o perjudiciales en un sistema infectado, mientras que el RANSOMWARE es un código malicioso que cifra la información del ordenador e ingresa en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga.

---

[159] Abrevadero. Estrategia en la que se ataca a un grupo en particular (organización, sector o región) en tres fases: 1. Adivinar/observar los sitios web que el grupo utiliza a menudo. 2. Infectar uno o más de ellos con malware. 3. Infección de alguno de los miembros. Su eficacia se basa en la confianza depositada en las páginas web que se visitan con asiduidad. CCN-STIC 401

El CRYPTOWARE es una variante del ransomware, pero cifrando el contenido del ordenador.

Representan una de las herramientas más utilizadas para realizar las infecciones que preceden a los ataques. El número total de versiones de código dañino para PC se estima actualmente en más de 439 millones siendo Windows el sistema más afectado, al tiempo que el número de malware en plataformas móviles sigue aumentando de manera incesante un 96% de este código dañino afecta al sistema operativo Android. A modo de ejemplo, podemos citar el caso Coinvault, una infección investigada conjuntamente por la Policía Holandesa y Kaspersky Lab, en la que pudo determinarse que, aproximadamente, el 1,5% de las victimas hicieron efectivo el pago del rescate.

Es lógico que aparezcan nuevas variantes, dado que se calcula que un tanto por ciento de las víctimas satisfizo el rescate, lo que estimula a los delincuentes para mejorar continuamente sus herramientas y sus objetivos: grandes empresas, pymes y consumidores finales; nuevos sistemas operativos y nuevos dispositivos incluyendo los dispositivos móviles.

SPAM.

Este término se puede subdividir en dos tipos, el spam tradicional y spam de código dañino. Tras un aumento en 2014, el spam tradicional disminuyó en 2015, aproximadamente el 30% del volumen del año anterior. Sin embargo, el que lleva malware, utilizando direcciones de correo electrónico obtenidas en otros sistemas infectados, aumentó significativamente y constituyó la principal fuente de infecciones.

Se encontraron muchas muestras de código dañino de la familia Geodo[160]. Se ha observado, además, que se distribuyen cada vez más profesionalmente. La utilización de técnicas de engaño y suplantación, el uso de versiones individuales

[160] INST. NAC. DE CIBERSEGURIDAD DE ESPAÑA Malware de tipo troyano que infecta ordenadores con sistema operativo windows. Los ordenadores infectados pasan a ser parte de una botnet, con lo que pueden ser utilizados para cometer actos delictivos.

del código dañino y el control horario de la descarga, son herramientas dirigidas a provocar la infección del sistema del usuario sin que el software antivirus sea capaz de detectarlo.

ATAQUES DDOS

Un ataque de denegación de servicio (DDOS), es un ataque a un sistema de computadoras o red que causa que un servicio recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobre carga de los recursos del sistema atacado.

En 2015, algunos sectores que han denunciado novedosos ataques de este tipo han sido las instituciones educativas o los servicios de transportes públicos. No obstante, los preferidos son la industria del juego (35,3% de los ataques) y la industria del software/tecnología (25,2% de los ataques). También se tiene evidencia de que se están utilizando servicios Booter que permiten perpetrar un ataque sin grandes conocimientos técnicos (DDoS-as-a-Service) y los denominados ataques por reflexión donde se utilizan servidores de acceso público para reforzarlo. Esto hace que los operadores de este tipo de servidores se conviertan en coautores (involuntarios) de las acciones dañinas.

BOTNETS

BOTNET es un Robot Network, lo que se conoce como la red de robot o zombies). Se trata de una red de equipos infectados por un atacante remoto. Los equipos quedan a su merced cuando desee lanzar un ataque masivo, tal como envío de spam o denegación de servicio. Las botnets son utilizadas por los ciberdelincuentes de forma masiva, al objeto de sustraer información, cometer fraude de banca online, atacar a la disponibilidad de los sistemas informáticos o enviar spam. Debido a la profesionalización de los ciberdelitos, operar una botnet es relativamente fácil y poco costoso para los no especialistas. Por ello, el nivel de peligrosidad actual continúa siendo crítico y la tendencia va en aumento.

- En febrero de 2015 se desactivó una botnet especialmente significativa: Ramnit, que había causado aproximadamente 3,2 millones de infecciones en todo el mundo.

•Gracias a su cuota de mercado, los sistemas principalmente comprometidos por botnets son Windows, aunque los atacantes están redoblando sus esfuerzos para dirigirse contra sistemas Mac OS X y Android.

OFUSCACIÓN

Se denomina ofuscación cualquier actividad llevada a cabo por los atacantes para dejar el menor número posible de trazas de sus acciones, con el objeto de dificultar su identificación, la metodología seguida, etc. Un ejemplo de ello es el uso de servicios legítimos para la distribución de código dañino como por ejemplo ejemplos en Dropbox, Pinterest, Reddit, Google Docs. Gmail, etc...

INGENIERÍA SOCIAL

Constituye uno de los vectores de ataque preferidos por los agentes de las amenazas, que engañan a sus víctimas, para que permitan la instalación de programas dañinos, y todo ello al objeto de acceder a la información del sistema atacado.

En este caso, los atacantes tienen la posibilidad de obtener de forma rápida y anónima datos personales de sus víctimas a través de las redes sociales y suele constituir la primera fase de los ataques dirigidos tratando de adivinar la contraseña de la víctima, generando confianza, correos electrónicos personalizados o spearphishing.

El ataque del "falso presidente" ha sido muy lucrativo en el entorno comercial en 2015, Este ataque consiste es hacerse pasar por un directivo de la organización, encargando a un empleado la transferencia urgente destinada a un proyecto secreto).

WATERING HOLE

El ataque se vale de los mismos empleados de la empresa haciéndoles descargar involuntariamente malware a la red de la organización atacada cuando visitan una determinada página web controlada por el delincuente.

El ataque es altamente efectivo ya que con la infección de un solo terminal, se puede lograr que miles de víctimas descarguen la amenaza y, de un solo ataque, controlar la información de toda una entidad víctima. El éxito se

incrementa porque los delincuentes utilizan vulnerabilidades, no conocidas públicamente, que no han sido solucionadas por el fabricante y no son por lo tanto 100% efectivas.

LIBRERÍAS JAVASCRIPT

Web invocan directamente una librería en lugar de copiarla a su propio sitio web. Si un atacante logra manipular una librería está en condiciones de atacar a todos los sitios web que contengan una llamada dinámica a la misma.

ROUTERS INALÁMBRICOS

Los routers de particulares y pymes comprometidos permiten, por ejemplo, ajustar la configuración del DNS (Domain Name System) para redirigir el tráfico a páginas web infectadas, formar parte de una botnet, propagar código dañino y penetrar en la red o manipular el tráfico sin ser detectado.

ROBO DE IDENTIDAD

Habitualmente, el robo de identidad de los usuarios, contraseña u otros datos se lleva a cabo mediante mecanismos de ingeniería social, instalación de código dañino en los sistemas de la víctima o a través de ataques previos a sitios web. Con estos programas los atacantes pueden obtener un beneficio económico directo con la venta de identidades robadas y con un margen muy amplio, por lo que, esta actividad se mantendrá como una amenaza permanente en los próximos años.

BLINDRADARS

BlindRadars o bloquear el tráfico aéreo, se trata de una técnica de interferencia electrónica de los radares de las torres de control y de los sistemas de seguimiento de aeronaves. Mediante esta técnica los centros de control de tráfico aéreo pierden la localización exacta de los aviones, por lo que los controladores aéreos no pueden desarrollar su labor y no pueden guiar a los aeroplanos en su ruta de viaje y en los despegues y aterrizajes, pudiéndose producir choques en el aire o que el avión se estrelle en su maniobra de aproximación a la pista de aterrizaje.

ATAQUE POR ROBO DE INFORMACIÓN: PHISHING

Más del 40% de los programas maliciosos que se envían vía mail tienen como finalidad robar información personal y financiera. Muchos de ellos son dirigidos a empresas. Con el surgimiento del modelo de negocio online, fueron apareciendo nuevos y cada vez más complejos ataques informáticos que buscan obtener información confidencial de los usuarios, dando lugar a una nueva modalidad delictiva, encuadrada dentro del marco de las estafas.

De los principales métodos actuales para obtener información personal de usuarios, el primero de ellos es el Phishing. El phishing es una modalidad de obtención de información llevada a cabo a través de Internet que intenta obtener, de manera completamente involuntaria y fraudulenta, datos personales o sensibles que posibiliten realizar una estafa, utilizando metodologías de Ingeniería Social. El segundo, son los códigos maliciosos como backdoor, keylogger o los troyanos bancarios (bankers).

En cuanto al phishing y spearphishing, correo dirigido de alguien conocido, son las herramientas más utilizadas para iniciar ataques personalizados y también los más temidos a la hora de sufrir un ciberespionaje.

6.3 CIBERTERRORISMO O TERRORISMO EN LA RED.

Cuando se hace referencia al termino ciberespacio surge la necesidad de llevar a cabo una profunda reflexión basándose en los conceptos de terrorismo en red y ciberterrorismo. Dependiendo del experto que lo haya estudiado encontramos una u otra interpretación, dato que nos indica que la distinción entre ambos conceptos no está nada clara. Si atendemos a Maura Conway, experta en terrorismo virtual y profesora de la Dublin City University, no es lo mismo hablar de terrorismo en la red que de ciberterrorismo:

My preference is to distinguish between cyberterrorism and terrorist use of the Net. This is the distinction FBI Director Robert Mueller seemed implicitly to be drawing in a March 2010 speech in which he stated that “the Internet is not only used to plan and execute attacks; it is a target in and of itself…We in the FBI,

with our partners in the intelligence community, believe the cyber terrorism threat is real, and it is rapidly expanding[161].

Ahora bien, si atendemos al experto en cibercrimen Fernando Miró Llinares comprobamos que él no considera que exista una distinción tan clara entre ambos conceptos. Desde su perspectiva el fenómeno del ciberterrorismo debe entender desde un prisma más abierto.

Si bien el término ciberterrorismo se utilizó en un primer momento para referirse a los ataques a sistemas informáticos, hoy en día el mismo lo utiliza, en sentido amplio, como forma de referirse a los efectos del riesgo social que conlleva la unión entre terrorismo global y nuevas tecnologías de la información[162].

Desde otro punto de vista, La doctora Sagrario Morán Blanco se adhiere a la postura de Miró y apunta que a nivel internacional "no hay un concepto de ciberarma definida jurídicamente, aceptado institucionalmente o compartido doctrinalmente" por lo que "una acción cibernética puede ser calificada como cibercriminalidad, ciberespionaje o ciberterrorismo".

De todo lo estudiado hasta el momento llegamos a la conclusión que en absoluto es fácil tipificar, precisar e identificar las múltiples y variadas amenazas que existen en la actualidad en la red. Por lo tanto, y a pesar de la dificultada de dar una definición de estos conceptos, en mi estudio vamos a intentar conseguir una postura que admite ambas posiciones, pero que se decanta por entender que no existe una diferencia entre los conceptos de terrorismo en la red o ciberterrorismo. Esta Tesis defiende que no existe tal dicotomía ya que cualquier organización terrorista utiliza la dimensión digital no como un fin en sí mismo, sino como un medio a través del cual intenta alcanzar en mayor medida sus objetivos.

---

[161] Conway, M. (2011) 'Privacy and Security against cyberterrorism. Why cyber-based terrorist attacks are unlikely to occur'. Communications of the ACM [en línea] 54 (2) 26-28.
[162] Miró, F. (2012) El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid

Most of the terrorists have not mastered the technology necessary for launching large scale attacks. However, some websites offer technologies for hire on the internet and provide information to reach bot-nets to execute `Distributed Denial of Service Attacks´. Since the cyber terrorism is the convergence of terrorism and cyberspace, not only the devastating terrorist cyber attacks but also terrorist actions such as propaganda and recruiting carried out on the Internet should be considered as `cyber terrorism´. Terrorist organization websites agitate public opinion, educate and motivate the members, command and control the organization, make propaganda to the target population and provide information to carry out cyber attack. Therefore, both the terrorist cyber attacks and the use of internet websites by the terrorists should be treated together and evaluated under the definition of the cyberterrorismo[163].

Con ello debemos destacar que los terroristas identifican y hace uso la red como un instrumento que cataliza perfectamente un diseño destinado para incrementar el éxito del resultado de sus misiones. Por tanto, la web es utilizado como medio por parte de los terroristas para expandir sus amenazas y su influencia por todo el planeta. De este modo se llevan a cabo operaciones ciberterroristas que no implican que la Web sea en sí misma un fin, sino que es utilizada como un medio a través del cual se ejercer una presión aun mayor sobre todos sus enemigos. Un claro ejemplo de este modo de proceder lo encontramos en el terrorismo yihadista anticipado por Murat Dogrul, Adil Aslan y Eyyup Celik en 2011[164] y verificado por Sagrario Morán Blanco en 2017.[165]

---

[163] Dogrul, M., Aslan, A. & Celik, E. (2011) 'Developing an International Cooperation on Cyber Defense and Deterrance against Cyber Terrorism'. International Conference on Cyber Conflict. Tallinn, Estonia 2011 [en línea] 2 de julio

[164] Dogrul, M., Aslan, A. & Celik, E. (2011) 'Developing an International Cooperation on Cyber Defense and Deterrance against Cyber Terrorism'. International Conference on Cyber Conflict. Tallinn, Estonia 2011, 2 de julio

[165] Morán, S. (2017) 'La ciberseguridad y el uso de las tecnologías de la información y la comunicación (tic) por el terrorismo'. Revista Española de Derecho Internacional, 195-222.

There are many reasons that why cyberspace is an attractive choice for the terrorist purposes. Cyber attacks offer the capabilities for terrorist activities with wider-reaching impacts. Using cyber attacks, terrorists can inflict much wider damage to a country than they could by resorting to physical violence. With traditional terrorist activities, such as bombings, the impacts are isolated within specific physical locations and communities. Large part of the population acts only as observers and they are not directly affected by terrorist acts. The media and public attention is more likely to focus on the destruction of property and/or loss of life than whatever `cause´ the activity was intended to promote. The ability of cyber terrorism activities to effect wider part of the population may give the groups involved greater leverage in terms of achieving their political and social objectives. [166]

El principal objetivo del terrorismo, que no es otro que aterrorizar a la población a través de sus atentados, es más `sencillo´ que nunca gracias al efecto multiplicador del miedo que los atentados tienen gracias al uso de las TIC´s. Recordemos el sentimiento de terror que generó la visualización, a través de las redes sociales, del degollamiento del periodista norteamericano, James Foley, en agosto de 2014, por un terrorista del Estado Islámico de Iraq y el Levante.

6.3.1 La web como un instrumento necesario para el Ciberterrorismo.

El ciberespacio como una estructura rizomatica, entendida esta como la utilización de unos principios de conexión y heterogeneidad, destacan la existencia de un tipo de relación arbitraria entre estratos donde todos los puntos están entrelazados e interconectados, consiguiendo con este que la información fluya de forma segura a los terroristas, permitiendo con ello realizar de forma fácil donaciones anónimas a través de organizaciones sin ánimo de lucro que acabarán financiando los propósitos terroristas y que actuan de forma descentralizada permitiendo con ello tener redes de colaboradores con unos

[166] Dogrul, M., Aslan, A. & Celik, E. (2011) 'Developing an International Cooperation on Cyber Defense and Deterrance against Cyber Terrorism'. International Conference on Cyber Conflict. Tallinn, Estonia 2011 2 de julio

costes económicos muy bajos, que a su vez consiguen reclutar y movilizar a muchos simpatizantes a través de mensajes que se transmiten a gran velocidad en las redes sociales; y, ante todo, le permite acceder a enormes masas de información desde casi cualquier lugar del planeta.

A través de los estudios realizados por Maura Conway, llegan a la conclusión en 2006 de cuáles eran las cinco áreas virtuales donde los terroristas invertían más tiempo:

The Internet is a powerful political instrument, which is increasingly employed by terrorists to forward their goals. The five most prominent contemporary terrorist uses of the Net are information provision, financing, networking, recruitment, and information gathering: […] Information Provision: This refers to efforts by terrorists to engage in publicity, propaganda and, ultimately, psychological warfare. The Internet and the advent of the World Wide Web in particular, have significantly increased the opportunities for terrorists to secure publicity. […] Financing: The immediacy and interactive nature of Internet communication, combined with its highreach properties, opens up a huge potential for increased financial donations as has been demonstrated by a host of non-violent political organizations and civil society actors. […] Networking: This refers to groups' efforts to flatten their organizational structures and act in a more decentralized manner through the use of the Internet, which allows dispersed actors to communicate quickly and coordinate effectively at low cost. […] Recruitment: This refers to groups' efforts to recruit and mobilize sympathizers to more actively support terrorist causes or activities. […] Information Gathering: This refers to the capacity of Internet users to access huge volumes of information, which was previously extremely difficult to retrieve as a result of its being stored in widely differing formats and locations [167].

El estudio de Conway en referencia a los usos de la red por parte de los terroristas sigue siendo completamente válido en la actualidad. Igualmente, otro autor, Marc Sageman, ya avanzo en su momento que el escenario en el que en la

[167] Conway, M. (2006) 'Terrorism and the Internet: New Media-New Threat?' Parliamentary Affair, 59 (2) pag. 283-298

actualidad os encontramos: "I noted the greater role of the Internet in neojihadi communication"[168]

Desde este carácter descentralizado y deslocalizado de la red, y teniendo presente los cinco campos señalados, vamos a centrar el análisis en dos importantes grupos terroriastas como son Al Qaeda y Daesh, organizaciones terroristas que han dado lugar a la denominación yihadismo 2.0.

6.3.2 El uso del ciberespacio por parte de la organización terrorista Daesh.

La mencionada organización y sus adeptos interaccionan con la Sociedad Internacional haciendo uso de la red existente en el espacio mostrando una intolerancia sanguinaria hacia cualquier otro grupo humano que no comparta su visión perturbada y deliberadamente deformada de la Sharia. Los responsables de Daesh utilizan una gran cantidad de revista y videos que ellos mismo llevan a cabo con la finalidad de expandir su mensaje y remarcar que dicha organización terrorista no detendrá la expansión de su califato ni el genocidio que se está cometiendo hasta que no finalice por completo su guerra santa contra los infieles.

La unión del ciberespacio con el hecho terrorista ha llevado a cabo una verdader evolución social y con ello el nacimiento de un nuevo modelo terrorista. Se trata de terroristas yihadistas internautas o "yihadistas de sofá, que cómodamente desde su casa y a través de las fuentes abiertas recopila material para difundir la yihad y expresar sus ideas radicales"[169] . De este hecho subyace la idea de que el entorno de Daesh utiliza de forma intensiva y extensiva Internet.

Todos hemos visto como utilizando nuevas herramientas de comunicación como Twitter y Facebook narran espeluznantes ejecuciones y actos de barbarie cometidos. Las autoridades han cerrado muchas de estas redes sociales sin poder evitar dicha difusión, dando lougar al desarrollo de una plataforma propia muy

---

[168] Sageman, M. (2017) Misunderstanding Terrorism. Philadelphia: University of Pennsylvania Press

[169] Calvo, S. (2013) 'De la web 1.0 a internet invisible vulnerabilidades, amenazas y delitos'. en Ciberseguridad. Retos y amenazas a la seguridad nacional en e

similar a la desarrollada por Mark Zuckerberg: "5elafabook"[170] . En dicha red social, cuyo nombre podría traducirse como "Califatobook" se difundían de forma diaría y natural las grabaciones de las barbaridades a las que sometían a los infieles que tenían secuestrados.

Desde su constitución en 2014 como una especie de pseudocalifato, los atentados perpetrados por Daesh se difunden en el ciberespacio de forma casi inmediata. Por un lado, las revistas online Dabiq y Rumiyah son los altavoces mediáticos del grupo terrorista en la red. Por otro lado, la agencia de comunicación Amaq se dedica principalmente a reivindicar los atentados a través del ciberespacio. De esta forma, el aparato de propaganda terrorista se retroalimenta con el aparato de captación terrorista en el ciberespacio. Dos casos paradigmáticos ocurridos en el ciberespacio en 2015 y en 2017 hacen evidente cómo la evolución de estos dos aparatos en el ciberespacio continua activa:

En 2015 emitieron en código abierto un mensaje donde incitaban a cualquier fiel a asesinar a soldados de Estados Unidos cuyos nombres aparecían en una lista difundida en la propia red: "Un grupo hasta ahora desconocido autodenominado `Organización de Hacking Estado Islámico´ publicó los nombres, fotos y direcciones de unos 100 soldados estadounidenses en línea, amenazándoles y pidiendo que se les ataque" (CNN, 2015). El entonces director del FBI, James Brien Comey, admitía ante los medios la vulnerabilidad de la red:

En 2017, también en código abierto, emitieron un video donde mostraban los planes de recuperar el Al-Ándalus. El video muestra a un joven de origen cordobés, Al Qurtubí, reivindicando en español la necesidad de ejecutar el Yihad para recuperar la tierra del califato, el antiguo Al Ándalus. El video se cuelga en la red el 24 de agosto de 2017 como cibermensaje producido por las agencias de Daesh tras el atentado cometido en las Ramblas de Barcelona el 17 de agosto de 2017. En él incorporan imágenes del citado atentado y destacan el éxito del mismo. El protagonista advierte sobre la propuesta imparable de Daesh en su lucha contra los infieles y hace un llamamiento en la red a continuar la guerra: "El

[170] Iriarte, D. (2015) 'Califatobook`, la red social de los seguidores del Estado Islámico' ABC.

Yihad no tiene fronteras. Haced Yihad donde estéis. Alá estará complacido con vosotros […] Al Ándalus volverá a ser lo que fue, tierra de Califato" En la revista Rumiyah de septiembre de 2017, reinciden en el cibermensaje terrorista.

En ambas acciones, el aparato terrorista de Daesh ha llevado a cabo sus actos terroristas a través de las redes sociales activando un ingente listado de simpatizantes en países occidentales. La comunidad internacional está asistiendo desde 2014 al crecimiento de forma alarmante y preocupante del uso de la red por parte del Daesh para la captación, incitación y puesta en prácticas de actos terroristas.

En este sentido, es realmente preocupante observar que en los últimos meses de 2018 Daesh, a pesar de haber sufrido un recorte significativo de sus territorios en Siria e Irak tras la presión ejercida por la Coalición Internacional, no se ha limitado a mantener activos sus aparatos y sistemas virtuales de captación y propaganda, sino que está incrementando las acciones de intimidación digital sobre el espectro de población a la que desea amedrentar, aterrorizar y eliminar.

6.3.3 Al Qaeda: Nuevas técnicas de ataque, el uso del Ciberespacio.

Como ya se ha mencionado es este capítulo, Al Qaeda fue la primera organización terrorista que incentivó el uso del espacio virtual para la consecución de sus objetivos, obteniendo unos buenos resultados. Tras los ataques contra el World Trade Center y el Pentágono a principio de siglo y las consecuentes operaciones militares llevadas a cabo por Estados Unidos en Oriente Medio, la organización terrorista Al Qaeda sufrió un grave deterioro en sus infraestructuras físicas obligándoles a reinventarse. En un primer momento se llegó a creer que podría ser el fin de la organización, derivó principalmente a una serie de cambios que transformó drásticamente la naturaleza del grupo y con ello sus métodos de actuación. Con ello podemos llegar a la conclusión de que Al Qaeda encontró en el ciberespacio un nuevo campo de operaciones a través del cual redirigir sus intervenciones y poder alcanzar sus objetivos. Este grupo terrorista dirigido y liderado por Osama Bin Laden se reconfiguró como una organización terrorista que mantenía unos ideales medievales y se guiaba por un código religioso completamente tergiversado y descontextualizado históricamente, pero que volvía a resurgir gracias a los avances tecnológicos del siglo XXI, el ciberespacio. Al Qaeda empezó a utilizar Internet para expandir su

propaganda y los discursos de su líder. Con este uso del cibereapcaio consiguieron rápidamente ser escuchados por millones de personas al ser compartidos y reenviados en masa a través de los cibercafés de la época.

De la misma manera que en Londres los responsables de Azzam Publications se dedicaban a vender documentación electrónica para financiar los atentados y extender las redes de captación, en España Al Qaeda también desarrolló un uso intensivo del ciberespacio a través de su Red Ánsar Al Mujahideen (RAAM). Según recoge un Auto de la Audiencia Nacional de 2012 "El grupo autodenominado `Ánsar Al Mujahideen Network´ aparece integrado por un reducido `núcleo duro´ de individuos con una larga trayectoria en plataformas yihadistas en Internet a través de las cuales se incitaba a cometer actos terroristas[171]" En dicha sentencia se define a RAAM como un grupo extremista radical que hace uso del ciberespacio para financiar atentados y expandir su ideología yihadista.

A esta red pertenecía Mudhar Hussein Al Malaki, denominado como el "bibliotecario de Al-Qaeda" (El Mundo, 2014), quien desde 2005 incitaba a cometer atentados y preparaba cursos online para llegar a ser terrorista. Hussein Al Malaki, que fue detenido en 2012 por practicar "la yihad mediante la palabra" (El Mundo, 2014), consiguió a través del uso de las tecnologías convertir el ciberespacio en uno de los medios más fértiles para captar, reclutar y adoctrinar a nuevos combatientes para Al Qaeda.

Con el paso del tiempo la organización terrorista Al-Qaeda ya no es solamente una organización que, mediante el aprovechamiento de las nuevas tecnologías, concretamente de la propaganda a través de Internet desde 2007, sino se ha transformado a sí misma en un movimiento social, que da acceso a su

[171] Audiencia Nacional (2012) Diligencias Previas 26/2011-W. Juzgado Central de Instrucción Nº5, Madrid.

iolencia ideológica, a cualquier persona, en cualquier lugar del mundo, que simplemente disponga de un ordenador y una conexión a Internet.[172]

6.3.4 El uso terrorista de las TIC´s como nuevo medio de amenaza en los conflictos bélicos.

Otro grupo terrorista como el el Daesh ha encontrado en la red un medio perfecto para conseguir sus objetivos expandiendo su propaganda y llevanado a cabo sus tareas de reclutamiento, adoctrinamiento y expansión. A pesar de tantos estudios llevados a cabo en referencia a esta materia, no podemos decir que exista un consenso entre todos los expertos que permita aclarar si el denominado ciberterrorismo es una amenaza realmente tan dañina como algunos describen. Desde punto de vista de Peter Warren Singer[173] y Allan Friedman[174], el mundo se encuentra obsesionado con los efectos que se puede tener un ciberataque terrorista. A su entender, tal visión de la realidad es un error ya que el número de víctimas producidas por el ciberterrorismo a día de hoy continúa siendo cero.

Estos autores siguen la línea de pensamiento consistente en revaluar las amenazas y riesgos que nos rodean con el fin de valorar de una forma objetiva el daño que dichos ataques pueden provocar. Con ello se pretende relacionar las amenazas y riesgos que rodean el amplio ámbito de la seguridad para comprender cuáles son las que verdaderamente causan un mayor número de muertes.

---

[172] Balañá, J. (2011) 'El uso de las nuevas tecnologías por parte de los grupos terroristas islámicos (yihadistas), ed. Por Instituto Universitario General Gutiérrez Mellado de Investigación sobre la Paz, la Seguridad y la Defensa. Madrid: IUGM, 649-676

[173] Warren, M. (2007) 'Terrorism and the internet'. en Cyber Warfare and Cyber Terrorism. ed. Por Janczewski, L. & Colarik, A. Nueva York: IGI Global - Information Science Reference, 42-49

[174] Singer, P. & Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Nueva York: Oxford University Press

Queda demostrado científicamente que el terrorismo es una amenaza real, pero no existencial. Según mi opinión, hay que evitar crear un clima de temor permanente ya que ha quedado demostrado que no sirve como un método efectivo para hacer frente a este tipo de amenazas, aunque en muchas ocasiones son utilizadas para recortar derechos y deberes existentes en las sociedades abiertas y basadas en el imperio de la ley.

Peter Warren Singer y Allan Friedman intentan disminuir el nivel de alerta que existe en la actualidad en referencia a la amenaza del ciberterrorismo:

Let us be clear: the worries over vulnerabilities in critical infrastructure to cyberattacks have real validity. From 2011 to 2013 probes and intrusions into the computer networks of critical infrastructure in United States went up by 1700 percent [...] But just as our fears inspired all sorts of potential new terror attacks scenarios in the immediate aftermath of 9/11, the key is distinguishing between our nightmarish visions of what might happen from the actual uses of the Internet by terrorist groups [...] There are threats out there, but there are no threats that threaten our fundamental way of life.[175]

Singer y Friedman argumentan que gran parte de la comunidad científica ha exagerado las consecuencias que puede tener el ciberterrorismo. Desde su perspectiva no creen en la posibilidad de que un grupo terrorista tenga acceso a los instrumentos necesarios como para llevar a cabo un ataque cibernético a gran escala es algo imposible a día de hoy. Estos expertos norteamericanos llegan a la conclusión de que las consecuencias que producen de algunos de los ciberataques más conocidos de la historia se han sobredimensionado considerablemente. Entre sus como ejemplo resaltan en caso de los ciberataques que Estonia sufrió en 2007 por parte del gobierno ruso. A su entender, el impacto que tuvieron los ciberataques en la vida diaria de la población de Estonia fue considerablemente reducido tanto en su intensidad como en su duración. Consideran que el daño que puede generar a producir en la población de un ciberataque como el que sufrió Estonia en 2007 o el que sufrió Georgia en 2008, no puede compararse con

[175] Singer, P. & Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Nueva York: Oxford University Press.

los efectos más devastadores que se derivan de la explosión de una bomba sucia, un coche bomba o una cadena de atentados, donde hay un mayor daño humano, tanto físico como moral.

A pesar de ello, es muy interesante observar que tras afirmar que tanto los medios de comunicación como los gobiernos y los expertos han exagerado el daño que puede tener una acción ciberterrorista, "the threat of cyber terrorism, in paticular, has been vastly overblow"[176], ambos autores inmediatamente se desdicen siguiendo las advertencias de John Michael McConnell, director de la National Security Agency durante la Administración Clinton y director de Inteligencia Nacional durante el segundo mandato de George W. Bush. McConnell donde se ha advertido en numerosas ocasiones que los terroristas cada vez adquieren un mayor número de medios destinados a circular más libremente y anónimamente él en ciberespacio.

The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking. The problem is not one of resources; even in our current fiscal straits, we can afford to upgrade our defenses. The problem is that we lack a cohesive strategy to meet this challenge.[177]

A consecuencia de estas advertencias, Singer y Friedman moderan su discurso y admiten que el número de grupos terroristas operando en Internet cada vez es mayor, ergo, la probabilidad de alterar nuestro equilibrio securitario a través de medios virtuales aumenta cada vez más.

En lo que sí aciertan por completo los autores del libro "Cybersecutiy and Cyberwar. What everyone needs to know", es al explicar la forma en la que los terroristas usan actualmente Internet. Singer y Friedman apuntan que la mejor forma de comprender por qué los terroristas hacen un uso cada vez mayor del

---

[176] Singer, P. & Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Nueva York: Oxford University Press

[177] McConnell, M. (2010) 'How to win the cyber-war we're losing'. The Washington Post [en línea] 28 de febrero.

ciberespacio en sus operaciones, es preguntarnos a nosotros mismos porqué utilizamos cada vez más Internet en nuestras vidas.

A modo de resumen, debemos resaltar que Internet permite a las múltiples organizaciones terroristas a planear sus operaciones en la oscuridad, al tiempo que pueden comunicarse fácilmente y con la garantía de un anonimato casi indescifrable.

Durante las últimas décadas observamos acontecimientos que pueden demuestran que el ciberterrorismo no es algo del futuro sino una amenaza actual que lleva poniendo en jaque nuestra estabilidad. Partiendo del atentado tan trágico 11 que sucedió en septiembre de 2001, y cinco días después de los ataques a las Torres Gemelas, Estados Unidos empezó a tomar una seria conciencia sobre el papel que estaba jugando el ciberespacio en la extensión del fenómeno terrorista de carácter religioso. La utilización de los servicios de mensajería electrónica rápidos y encriptados, sumada al uso de cibercafés como plataformas de intercambio de información, hizo que el gobierno de Estados Unidos reaccionase de una forma muy drástica, como nunca habíamos visto.

La Administración estadounidense quiere intentar mantener a salvo Internet de los ciberterroristas. El FBI ha lanzado una alerta contra el terrorismo cibernético, y el Senado norteamericano llevo a cabo la aprobación una serie de medidas que ayudan a la policía para pinchar Internet.

Estas medidas encontraron aún más justificación cuando en 2002 Reino Unido fue objeto de "5.589 ataques provenientes de Egipto, Pakistán, Marruecos y Turquía". No obstante, no fue hasta el año 2010 cuando Reino Unido empezó a alertar ya de forma contundente sobre las peligrosas sinergias existentes entre el ciberespacio y el terrorismo. Fue Theresa May quien por fin reconoció que el llamado ciberterrorismo se encuentra ya entre las mayores amenazas a las que se enfrenta Reino Unido.

Dos años después, compartiendo esta misma visión, Estados Unidos a través de Leon E. Panetta, que en ese momento era Secretario de Defensa, alertó sobre las preocupantes brechas de seguridad existentes en el ciberespacio:

Defense Secretary Leon E. Panetta warned Thursday that the United States was facing the possibility of a `cyber-Pearl Harbor´ and was increasingly

vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government […] Defense officials insisted that Mr. Panetta's words were not hyperbole, and that he was responding to a recent wave of cyberattacks on large American financial institutions.[178]

Ya en el año 2014 podemos encontrar muchas evidencias de que el uso del ciberespacio con fines terroristas era un fenómeno desgraciadamente en auge y con rápido desarrollo. A nivel nacional, el que fuera Director del Departamento de Seguridad Nacional entre 2011 y 2018, Alfonso de Senillosa Ramoneda, quien admitió que España estaba siendo utilizada como un instrumento para conseguir herramientas por parte de los terroristas del Estado Islámico mediante Internet. Como consecuencia de este fenómeno, la Guardia Civil empezó a detectar un aumento cada vez mayor del número de perfiles en redes sociales que difundían de manera continuada numeroso contenido apologético de ETA y de otras organizaciones terroristas como Al Qaeda y Grapo.

Un año después, las alarmas en relación con el ciberterrorismo se encendieron una vez más mostrando a la sociedad internacional que las organizaciones terroristas gestionaban un gran número de sus operaciones vía Internet. Los terroristas no sólo utilizaban la red para hacer propaganda de su mensaje o captar nuevos adeptos, sino también para atacar nuestras infraestructuras críticas. En el plano nacional, varios medios de comunicación se hicieron de eco de cómo el Ministerio del Interior había detectado un incremento del uso del ciberespacio con fines terroristas aún mayor que el registrado en el año 2014. "El Ministerio del Interior ha detectado una especial actividad de los grupos yihadistas en las redes sociales e Internet y ha advertido de que el 80 por ciento de los terroristas que son captados para integrar grupos radicales surgen por esa vía" [179]. Asimismo, Fernando J. Sánchez Gómez, director Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) llamó la atención

[178] Brumiller, E. (2011) 'Panetta Warns of Dire Threat of Cyberattack on U.S.' The New York Times

[179] Europa Press, (2015)

sobre los riesgos que conllevaba la presencia cada vez más notoria de terroristas en Internet. "El ciberterrorismo no deja de ser una parte del conjunto de las ciberamenazas. Año tras año vemos como éstas van creciendo exponencialmente, tanto en número como en sofisticación. Hay más ataques, y cada vez son más agresivos"[180].

En el plano internacional, el reconocido experto en materia de seguridad informática Eugene Kaspersky expresó que "desgraciadamente sus predicciones alarmistas sobre ciberseguridad se han hecho realidad y advirtió de que la próxima gran amenaza de Internet es el ciberterrorismo"[181], siendo Daesh uno de los mejores ejemplos. Respecto a esta organización terrorista cabría apuntar que el factor que está permitiendo que su resiliencia sea tan efectiva es, esencial y principalmente, el uso de Internet.

Un caso paradigmático que nos permite continuar nuestro análisis en torno al ciberterrorismo fue el ciberataque yihadista sufrido por el canal internacional francés TV5 Monde el 9 de abril de 2015. La clave de esta ofensiva terrorista radicaba en que no fue necesario llevar a cabo la detonación de una bomba, la voladura de un edificio o la ejecución de una matanza brutal en un lugar público para provocar el caos. Daesh se limitó simplemente a atacar mediante embestidas cibernéticas los servidores y las redes sociales de una de las televisiones francesas con más audiencia para conseguir producir un daño psicológico muy considerable. Francia ha sufrido 19.000 ataques informáticos desde el 10 de enero, al menos una decena de ellos a páginas oficiales del Ministerio de Defensa. Fuentes próximas al vicealmirante Arnaud Coustillière, responsable de la ciberdefensa del Estado Mayor, han confirmado que estas interferencias se incrementaron después de las manifestaciones de repulsa a los atentados yihadistas celebradas en toda Francia.

Ante tales hechos, lo inteligente hubiese sido activar los sistemas de alerta temprana en el ciberespacio. Sin embargo, la reacción gubernamental ante esos

---

[180] Muñoz, P. (2015) 'Los ataques ciberterroristas aumentan y cada vez son más especializados'. ABC [consultado 27 enero 2019]

[181] Quincoces, A. (2015) 'Eugene Kaspersky: La amenaza ciberterrorista, al albur ya sólo de voluntades'.

19.000 ciberataques terroristas de nivel medio bajo fue infravalorar la amenaza y afirmar lo siguiente: "Ha sido una crisis como otras similares en el pasado, y no ha tenido consecuencias importantes en ningún caso" [182]. Y como si dichas palabras no hubieran sido suficientes, el Ministerio de Defensa francés hizo públicas unas declaraciones en las cuales se sacaba a relucir la errónea pero exultante confianza que Francia tenía en sí misma y en sus cuerpos de seguridad físicos y cibernéticos: "No hay una ciberguerra […] Ninguno de esos ataques ha conseguido finalmente su objetivo, gracias a la vigilancia de los equipos del Estado Mayor"[183].

Los hechos demuestran que se optó por quitar peso al problema. Las autoridades francesas consideraban que no era bueno exagerar la amenaza. El fallo se encuentra en que François Hollande jamás pensó que solo dos meses y medio después todos sus ciudadanos iban a ver, gracias a un ciberataque, el logo del Daesh proyectado en una de las televisiones con más cuota de audiencia.

La idea que subyace del caso francés es que el problema no está en que el destino sea caprichoso y se produzca un ciberataque contra un canal de televisión, sino en negar o infravalorar una amenaza que ya tenía en ese momento un peso y unas capacidades más que evidentes. En esta dirección, en España, Dolores Delgado García, actual Ministra de Justicia y entonces fiscal coordinadora contra el terrorismo yihadista en la Audiencia Nacional, expuso de forma muy acertada los problemas que se derivan cuando se infravalora la cuestión del ciberterrorismo o no se ponen trabas al uso del ciberespacio por parte de Daesh u otras organizaciones:

"En muy pocos años en España hemos pasado de las células extremistas que se limitaban a dar apoyo logístico a otros grupos a un terrorismo global y exprés que crea nuevos terroristas en cuestión de meses y que crece exponencialmente con la intención de matar. […] Desde que se inicia la captación hasta que alguien decide incorporarse al Estado Islámico o realizar acciones aquí pasa muy poco tiempo, dos o tres meses. Lo mismo

---

[182] Yárnoz, C. (2015) 'Francia ha sufrido 19.000 ciberataques en cinco días'. El País 15 de enero.

[183] Idem.

sucede en Siria o Iraq, donde reciben un entrenamiento muy rápido. Un proceso donde Internet, las redes sociales y sus recursos mediáticos tienen un papel fundamental. […] Ahora, a través de Internet –que ya es una herramienta terrorista material–, se financian, marcan caminos a zonas de conflicto, consiguen documentación falsa, apoyo logístico y también enseñan a utilizar armas, preparar explosivos o distribuir manuales sobre cómo comportarse cuando son detenidos o instrucciones para lograr eludir las investigaciones policiales"[184].

En 2016, teniendo en cuenta que "the aim of terrorism, after all, is not just physical destruction, and depending on who the attackers and the victims are, the psychological effects of cyber terrorism can be just as powerful as the real thing" las aparatos de comunicación y propaganda de Daesh incrementaron su actividad en internet. Por un lado, aumentaron su el número de perfiles en redes sociales mundialmente conocidas como Twitter, Facebook, Telegram o YouTube y, por otro lado, diversificaron las plataformas y aplicaciones web en las que estaban presenten para garantizar una mayor expansión de contenidos y asegurar que los videos de los atentados siempre estuvieran disponibles en algún repositorio digital.

En 2017, teniendo en mente las advertencias realizadas por Michael L. Gross, Daphna Canetti y Dana R. Vashdi cuando afirmaban que "leveraging its success at conventional terrorism, Islamic State will move seamlessly and effectively to cyber terrorism to produce outsized fear and panic", la responsable del Área de Ciberseguridad del Departamento de

Seguridad Nacional, María del Mar López Gil, afirmó que "el ciberterrorismo es una amenaza para la seguridad nacional […] ya que los terroristas utilizan las redes sociales como herramientas de propaganda y captación" [185].

Estas afirmaciones procedentes del ámbito nacional coincidían con las apreciaciones y publicaciones que Maysaa Zerzri, miembro del Center for Apllied Policy Research (CAP) y analista del Ministerio de Relación Constitucionales,

[184] Martín, E. (2015) 'El Estado Islámico capta terroristas en dos meses'

[185] IT Digital Security, (2017)

Sociedad Civil y Derechos Humanos de Túnez, quien en 2017 también incidía en que las organizaciones yihadistas en general y Daesh en particular estaban haciendo uso de multitud de redes sociales para atraer la atención de potenciales terroristas y posteriormente radicalizarlos:

Today, DAESH and many other organizations are utilizing social media platforms to select individuals for radicalizing or recruitment purposes. Recruiters identify potential targets by monitoring Facebook profiles and conversation threads and assess whether they are genuine sympathizers. They conduct further examination by adding them as friends and only engage in private communication only after they are certain of the individuals' faithfulness[186].

Maysaa Zerzri también llamó la atención sobre el uso de la deep web por parte de los terroristas de Daesh. La existencia de un mercado negro o black market cada vez más extenso y profundo permitía a los yihadistas encontrar documentación para autoradicalizarse, preparar explosivos caseros o alcanzar las capacidades necesarias para diseñar un ciberataque suficientemente efectivo como para provocar un grave daño psicológico en la población. Estos hechos mostraban que los miembros de la organización terrorista liderada por Abu Bakr al-Baghdadi no tenían la necesidad de crear desde cero una ciberarma ya que solo debía de acudir a la deep web para comprar allí todo aquello que necesitaran a un precio y un riesgo muy reducido.

Terrorists are using the Internet for data mining to collect information of particular places and individuals as potential targets for attacks as well as recruitment […] terrorist organizations use the Internet and especially the Dark Net to disseminate training materials to conduct physical attacks, and distribute guidelines and instructions to equip their members and supporters with the necessary skills in order to support their cyber defense and to improve their offensive capabilities[187].

---

[186] Zerzri, M. (2017) 'The Threat of Cyber Terrorism and Recommendations for Countermeasures'. Center for Applied Policy Research

[187] Idem.

Recent events suggest that while cyber jihadists appear to remain of low skill and under- sophisticated, their toolset is expanding. Between December 2016 and January 2017, two distinct pro-ISIS cyber threat groups experimented with distributed denial of service (DDoS) attacks and achieved limited apparent successes. Although the attacks have since ceased, these actors have expressed interest in engaging in similar and potentially more offensive cyber activities in the future[188].

En 2018 el informe "European Unión Terrorism Situation and Trend Report" elaborado por Europol mantiene la necesidad de tener activos los sistemas de alerta temprana en lo que se refiere al uso de la deep web por parte de Daesh "some terrorist groups now turn to online criminal markets, using the crime-as-a-service industry to buy access to the capabilities that they themselves are lacking" (Europol, 2018: 15) y reconoce el peso de la amenaza que representa el ciberterrorismo.

5.4.4.1. Correos electrónico como munición.

Tras lo anteriormente expuesto cabe plantearse qué tipo de escenarios pueden ser potenciales objetivos de la actuación terrorista en términos reales y digitales. Es altamente probable que en ningún potencial escenario una organización terrorista separe su potencial balístico de su potencial cibernético, es decir, lo que puede esperarse en un futuro inmediato tiene que ver con una combinación de ataques físicos con ataques cibernéticos. Al combinar los ataques armados con el lanzamiento de ciberataques, los terroristas podrían debilitar drásticamente el proceso de toma de decisiones de sus enemigos. Esto es lo que sucedió en la confrontación entre Rusia y Georgia donde la combinación de balas y correos electrónicos tuvieron una gran capacidad destructiva:

La combinación de las operaciones armadas con las cibernéticas buscaba causar una pérdida de capacidad operativa y de confianza en las instituciones políticas, militares y

[188] Wolf, K. (2017) 'Cyber Jihadists Dabble in DDoS: Assessing the Threat'

financieras del país y bloquear la capacidad de comunicación entre dichas instituciones, entre el gobierno estonio y sus ciudadanos y entre Georgia y el mundo exterior[189].

Para Magnus Ranstorp "el escenario más probable para el futuro es la utilización de ataques electrónicos para causar pérdidas económicas y amplificar la conmoción social junto a un ataque terrorista convencional". Jessica Stern y J.M. Berger, autores del libro "Isis: The State of Terror", han señalado como en el caso de Daesh "none of this online activity existed in a vacuum, and much of it was strategic" y advierten de lo fácil que sería paralizar el comercio global mediante ataques informáticos: "They have not yet been extremely visible carrying out more sophisticated activities such as high-level cybercrime or more destructive attacks, but I suspect this is just a matter of time" [190].

El hecho de que los ataques ciberterroristas se produzcan en la red y no causen un gran estruendo no significa que no sean sumamente dañinos. Solo es necesario combinar lo físico con lo virtual: "Security researchers have proven it is entirely possible for criminals 1.500 miles away to seize control of your car when you are driving 65 mph down the highway [...] What they do with your hacked vehicle is limited only by their imaginations" [191].

Además, incluso si la tecnología en manos de Al Qaeda o Daesh no fuera suficiente y el ciberataque no alcanzase su objetivo, el simple hecho de intentar ejecutar un ciberatentado contra el aeropuerto JFK de Nueva York o contra los cables submarinos que conectan la fibra óptica entre continentes, permitiría sembrar una inseguridad económica y un miedo psicológico de tal dimensión que su victoria sería inmensa. Recordemos que el objetivo final del terrorismo ya sea a través de instrumentos físicos o virtuales, es implantar el terror en sus enemigos mediante una guerra psicológica, por lo que es indiferente si el apartado ciberterrorista está perfeccionado del todo o no, ya que el pánico que derivaría de un ciberatentado sería algo sin precedentes. El simple estallido del caos ya sería

---

[189] Ganuza, N. (2010) 'La situación de ciberseguridad en el ámbito internacional y en la OTAN'. en Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. ed. por Ministerio de Defensa. Madrid: Ministerio de Defensa, 165-214

[190] Graham, E. (2015) 'Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?

[191] Idem.

en sí mismo una fantástica victoria para los terroristas. Consiguientemente, desarrollar una industria cibernética que les permita llevar a cabo ataques informáticos combinados con ataques físicos no sería "desperdiciar recursos finitos" [192], sino emplearlos de forma mucho más eficaz y efectiva.

Obviamente, sería erróneo interpretar que estas argumentaciones apoyan las líneas de pensamiento que defienden que los terroristas van a focalizar a partir de ahora única y exclusivamente "su energía en materializar ciberataques"[193]. En este sentido, los ciberataques son y serán un instrumento más de las organizaciones terroristas, lo que no quiere decir que se centren de forma exclusiva en el desarrollo de ataques a través de la red. No obstante, este escenario recibe cada vez mayor atención debido a las ventajas operativas y tácticas que ofrece. Por decirlo de otro modo, Internet cada vez es más prioritario tanto para los terroristas como para los que los combaten. Mientras los terroristas están aprendiendo a sacar mayor beneficio de las redes sociales, del comercio electrónico, de los servicios de mensajería instantánea, de las bases de datos, o de la localización vía satélite, los Estados que luchan contra esta amenaza deben de ser conscientes de que el terrorismo tiene una nueva dimensión, la red y es en ella donde también deben combatirlo.

[192] Ranstorp, M. (2004) 'Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información'. en El nuevo terrorismo islamista. Del 11-S al 11-M. ed. por Reinares, F. y Elorza, A. Madrid: Editorial Temas de Hoy S.A., pag. 216-217.

[193] Idem.

-SITUACIÓN ACTUAL DE LAS AMENAZA HÍBRIDAS-

VII. SITUACION ACTUAL DE LAS AMENAZAS HIBRIDAS.

7.1 LAS GUERRAS DE CUARTA GENERACIÓN.

7.1.1 Introducción.

La idea de estas guerras no es nueva. El pensador chino Sun Tzu dijo: "Es difícil participar en guerras contra una fuerza militar más fuerte con la misma simetría. Por lo tanto, deben buscarse diferentes métodos para usarlas con el fin de infligir bajas por la fuerza". Dirigirse a la unidad comunitaria donde se rompe la cohesión social conducirá a la destrucción del poder militar.

El término de Guerra de Cuarta Generación fue utilizado por primera vez en 1989 por un equipo de analistas estadounidenses, (Stergas Lindh) para describir guerras basadas en el principio de descentralización.

La Guerra de la Cuarta Generación (4GW) se denomina Guerra contra las Organizaciones Terroristas, según el concepto estadounidense, en el que ambos bandos de la guerra tienen un ejército regular, en cambio alguno posee células ocultas dispersas por todo el mundo[194].Este tipo de guerra moderna incluía nuevas dimensiones que no existían antes. Una de estas dimensiones y es la guerra de información. Aunque esta guerra ha existido desde tiempos antiguos, ha adquirido nuevas características y principios como, siendo este uno de los métodos de las guerras más importante de la cuarta generación, lo que requiere que todos los países árabes se unan para enfrentar las guerras de la cuarta generación. Estas organizaciones utilizan todo tipo de delitos materiales como el asesinato y el moralismo. La tecnología es fundamental y encontramos informes y grabaciones de video de alta calidad en las operaciones terroristas.

Un comité de expertos militares acordó que las guerras de cuarta generación fueron llevadas a cabo en Estados Unidos, desarrolladas por su

[194] Mahmud, Atia (2017): Las guerras de cuarta generación, Dar El hoda publicación y distribución, Cairo, P. 32.

ejército de los Estados Unidos y conocidas como Guerra Asimétrica, donde el ejército de los Estados Unidos no se enfrentó a ningún país después de los eventos del 11 de septiembre de 2001, en el sentido de organizaciones que luchan en todo el mundo, y ha ocultado células que están activas para atacar los intereses de los países hostiles y las instalaciones económicas así como las líneas de transporte, con el fin de debilitarlos frente a la opinión pública interna con el pretexto de obligarlos a retirarse de interferir en sus áreas de influencia como (Hezbollah- AL QAEDA).

La Guerra de Cuarta generación de la guerra apunta al sistema a través de la creación de sistemas mentales internos en todos los niveles, que toman la forma de la guerra de grupos religiosos de línea dura o la guerra de los grupos económicos y financieros y la guerra de los grupos científicos que comercializan tecnología.

Los ciberataques constituyen uno de los marcos de acción preferidos principalmente por su bajo coste si los comparados con los importantísimos beneficios que pueden obtenerse, los escasos riesgos asumidos y la dificultad de determinar los actores y consecuentemente su inmunidad. Es importante tener en cuenta que este tipo de acciones permite que la infraestructura tecnológica de un tercer país pueda servir de base para la perpetración de un ataque, lo que dificulta aún más su atribución.

Todos los estados occidentales, en mayor o menor medida, son objeto de ciberataques con origen en otros Estados con el fin de obtener información de relevancia económica, geoestratégica o militar. Es significativo el número de países que están desarrollando capacidades para llevar a cabo operaciones de ciberespionaje.

Los países donde se han situado el mayor número de ataques actualmente son Rusia y China. No obstante, existen países emergentes en el desarrollo del ciberespionaje, como son Colombia, Corea del Norte, India, Irán, Marruecos, Pakistán, República Dominicana o Venezuela.

Finalmente, destacar que los Estados en ocasiones realizan los ciberataques contratando servicios de terceros actores o en ocasiones bajo la cobertura de movimientos hacktivistas, claro ejemplo de la existencia de un conflicto bélico híbrido.

Para definir el concepto de "Guerra de cuarta generación "observamos que sus raíces están muy arraigadas en la Guerra Fría entre los Estados Unidos y la Unión Soviética, utilizando métodos modernos de guerra que dependen de guerras secretas a través de individuos y grupos entrenados para causar disturbios en países y llevar a cabo operaciones terroristas.

Estados Unidos apoyó a Al Qaeda contra la Unión Soviética en Afganistán y las fuerzas vietnamitas en la guerra de Vietnam derrotaron a Estados Unidos, el ejército más poderoso del mundo, con pérdidas humanas y materiales. Este es un buen ejemplo de las guerras de la Cuarta Generación. El 11 de septiembre es otro ejemplo de estas guerras, que ilustra la capacidad de una fuerza irregular representada por al-Qaeda para atacar la torre comercial de los EE. UU. E infligir bajas en los Estados Unidos y atacarla en su propio territorio.[195]

Las guerras de cuarta generación son definidas por el escritor académico militar estadounidense (Antonio Etsivaria), Las guerras asimétricas son guerras desiguales que significan guerras basadas en un tipo de insurgencia en la que las fuerzas irregulares usan todos los medios tecnológicos, políticos, económicos y sociales para forzar al enemigo, lo que representa una fuerza sistemática para abandonar sus políticas y objetivos estratégicos.[196]

Bajo este concepto de Guerras de la cuarta generación, las guerras se diferencian principalmente:

- Por el uso de los medios de comunicación de diversas maneras.
- Quinta línea y organizaciones de la sociedad civil del mismo país objetivo.
- Por la existencia de operaciones de inteligencia.
- Por la influencia política de los partidos y organizaciones y todos los medios y métodos posibles mediante el uso de elementos que incluyen una base terrorista no nacional o multinacional dentro del estado por motivos religiosos o étnicos o demandas históricas con fondos indirectos de los

[195] Munaser, Said (2006): Las guerras y su concepto, el Colegio de líderes de Egipto, Cairo, P.121.

[196] Etsivaria, Antonio (2008): Las guerras asimétricas son guerras desiguales, P. 61.

estados enemigos (voluntarios, armas, municiones, equipos, asistencia para la planificación).

•Por el uso de la guerra psicológica a través de medios sofisticados y la manipulación psicológica y el uso de estaciones y canales que falsifican las imágenes y los hechos, debido a la financiación de estaciones y canales que atraen a los medios y la opinión en la comunidad.

•LA existencia de un uso inteligente del factor tiempo y atraer la atención a cuestiones secundarias.

•El uso de todas las presiones (políticas, económicas, sociales, militares), incluida la amenaza de reducir la ayuda, en su caso, las amenazas de uso de la fuerza.

•Haciendo estallar los problemas étnicos y religiosos en el estado mientras las minorías impulsan la rebelión.

•Uso de organizaciones de la sociedad civil, redes sociales, medios específicos y sitios web.

7.1.2 Objetivos y Características de las Guerras de Cuarta Generación.

Estas guerras no tienen como objetivo destruir el establecimiento militar o destruir el poder del estado, sino apuntar a agotar el poder del estado enemigo y erosionar lentamente su voluntad para obligarlo a llevar a cabo lo que quiere la fuerza que usa este tipo de guerra. Con ello buscan el fracaso del estado a través de operaciones lentas llevadas a cabo en países hostiles para que parte del territorio de ese estado no esté bajo su control y, por lo tanto, facilite el control de los grupos terroristas en esta región y lance las operaciones terroristas para atacar a los países hostiles.

Esta guerra política afecta a diferentes aspectos. Por ejemplo, la situación de seguridad en un país tiene un impacto directo en la capacidad del estado para obtener préstamos, lo que le da a este tipo de guerras diferentes formas de influir en la posición del estado.

Las organizaciones que utilizan la Guerra de la Cuarta Generación tienen como objetivo alcanzar el éxito político, no el militar, y enfocarse en cambiar la mentalidad de quienes toman las decisiones, es decir, cambiar las opiniones y políticas de quienes toman las decisiones en la dirección deseada por el adversario mediante la presión psicológica y de los medios.[197]

Los objetivos de la guerra de información en la nueva guerra moderna podemos dividirlos en dos grandes grupos diferenciado, la guerra de información ofensiva y guerra de información defensiva.

El objetivo de la guerra de información ofensiva imponer el control sobre las capacidades que posee la otra parte, el sistema C4ISR, que es (comando - control - comunicaciones - computadoras - inteligencia) a través del cual existe la posibilidad de implementar varios sistemas de control entre los que cabe destacar:

- El sistema dirigido a la obstaculizando los sistemas de información del enemigo.
- La implementación del engaño electrónico contra los sistemas de información mediante la introducción de microbios electrónicos para lograr la inexactitud de la información y el error en los resultados del análisis.

Para conseguir el objetivo que se persigue en la guerra de información defensiva se centra sus esfuerzos en conseguir un seguro electrónico para los medios utilizados en el sistema (C4ISR) sobre nuestras fuerzas y mantener la excelencia y la confidencialidad en el campo de la tecnología y la guerra de información.

Estas guerras se caracterizan por la existencia de grupos e individuos que no están directamente vinculados con el estado y que operan dentro del estado hostil al que se debe atacar. Es difícil detectarlos. Estos grupos e individuos están dispersos por todo el país. Se llevan a cabo en una gran escala y en un área geográfica no definida, a diferencia de las guerras tradicionales donde se conoce el territorio del combate o el teatro de operación.

---

[197] Kamal,Salah (2009): Objetivos de guerra de cuarta generación Dar Algazaer publicación y distribución Algeria, P. 23

Se utilizan medios tecnológicos, intelectuales y económicos, y el lado más débil recurre al uso de medios tecnológicos para resolver la guerra a su favor, en contraste con las guerras convencionales en las que se usan las armas convencionales y de manera directa.

Estas guerras duran largos períodos debido a su dependencia de las tácticas de guerrilla como sucede en el caso de la guerra que se basan en el terror que produce en la sociedad.

Las características de la guerra de información en el teatro de operaciones no están vinculadas a los límites geográficos, en dicho teatro se encuentra la información, pero no está determinado el momento ni el límite territorial donde atacar, con independencia que se encuentren en tiempo de paz o tiempo de guerra y con ello gran dificultad de advertir cuando ocurren para tomar las contramedidas de manera oportuna, las armas utilizadas son de calidad especial, nuevas y poco convencionales. Esta guerra requiere especialistas con alta cualificación científica y tecnológica ante la existencia de un nuevo campo de batalla en el que operan organizaciones ilegales que se preparan para el crimen y actos violentos organizados, se trata de una de las guerras más difíciles en el liderazgo militar, donde están expuestos a una gran cantidad de información y las especulaciones y las perspectivas son ilimitadas, lo que dificulta el desarrollo de planes completos y claros para abordarlos, aumentar la carga de inteligencia y análisis de información y centros de estudio para poner en práctica todas las posibilidades, expectativas y métodos de confrontación, la dificultad de determinar qué se debe proteger y las debilidades en el sistema de información y la dificultad de encontrarlos y, si se descubren, ya ha comenzado.[198]

Los objetivos de la guerra no se limitan a las instalaciones militares o combatientes, sino que incluyen una amplia gama de objetivos de importancia política, económica y social, donde se abordan las debilidades del enemigo.

---

[198] Abdel Hamid, Mohamed (2012): Guerra sin lucha, Dar Anglo publicación y distribución, El Cairo, P.22.

Los ataques asimétricos son más tensos, más creativos y dañinos debido al uso de los medios tecnológicos modernos. El objetivo de estos ataques terroristas es el poder gobernante y la población en conjunto, a diferencia de las guerras tradicionales que son el blanco del ejército y la autoridad gobernante.

La globalización ha desempeñado un papel importante en la influencia de estas guerras, ha ayudado a la creación de grupos terroristas generalizados y su uso de métodos no convencionales para contrarrestar la paz y la seguridad internacionales al proporcionar redes de Internet para facilitar la comunicación[199].

Entre las estrategias utilizadas destacaremos los mecanismo tendentes a obstruir el proceso político de enmiendas constitucionales y nuevas elecciones para el parlamento y el presidente para que este caos dure el mayor tiempo posible pretenden difundir un estado permanente de caos comunitario mediante el agotamiento de la sociedad y el agotamiento del estado en batallas internas sobre temas que pueden ser justos y conseguir con ello una atmósfera de guerra psicológica y mediática que viene del extranjero para promover ideas y creencias que dividen más a la sociedad.[200]

7.1.3 El papel de la guerra de la información en el escenario actual.

Muchos líderes y especialistas creen que la guerra de información es el elemento más influyente en los conflictos de hoy en día. Este tipo de guerra no es sorprendente en la era de la información. El tremendo progreso de la tecnología de la información durante la última mitad del siglo XX ha creado oportunidades sin precedentes para la explotación de la información.

El principal objetivo va dirigido a intentar Lograr el control de la información en el escenario de la guerra, lo que lleva a la confirmación de la derrota del enemigo antes del inicio de la batalla, este objetivo se puede implementar a través de los siguientes:

---

[199] Hesham, Halaby (2017): Estrategia militar de cuarta generación de guerras, Dar Bairut publicación y distribución, Lebanon, P. 43

[200] El centro democracia para estudios estratégicos (2015): Edición Abril

- Acelerar el colapso del enemigo al esparcir las semillas de la duda entre sus líderes, atacando e influenciando en la toma de decisiones y paralizar con ello su capacidad de cambiar de una etapa a otra.

- Cáscara de la capacidad del enemigo en el control, la advertencia y la orientación.

La guerra de información se organiza a través de diferentes puntos de vista sobre la mejor manera de beneficiarse de este modelo de guerra y sus fuentes. Uno de los ejemplos lo encontramos en la tecnología de las aeronaves ha alcanzado la base del poder aéreo, lo que a su vez ha llevado a la creación de fuerzas aéreas y la tecnología de la información también conduce al principio de la guerra de información y, por lo tanto, crea unidades independientes de guerra de información.[201]

7.1.4 Componentes de los procesos de información desde el punto de vista militar.

Cuando incluimos operaciones de información en cualquier operación militar o no militar dirigidsa a controlar el pensamiento del oponente para tomar la decisión e implementarla de una manera que sea útil para nuestra fuerza y con ello evite que el oponente practique tales operaciones contra nuestras fuerzas independientemente que el oponente sea un estado hostil, un estado amistoso o una organización rival. Este conjunto de operaciones persigue objetivos específicos tales como:

1.- Evitar el flujo de información entre los comandantes y sus unidades. Este objetivo se puede lograr mediante uno o más de los siguientes:

- Operaciones aéreas para la destrucción de los centros de mando y control.

- Operaciones especiales para cortar las líneas de comunicación y sabotear las estaciones de retorno.

---

[201] Zineb Hosny, Ezz El Din (2016): El impacto de las guerras de cuarta generación en la seguridad nacional árabe, El Centro Democrático Árabe, P.62 - 63.

- Atasco electrónico en las comunicaciones enemigas.

2.- Distorsionar la información del oponente sobre el campo de batalla. Los medios disponibles para lograr este objetivo son:

- Falsos objetivos en radares enemigos por engaño electrónico.
- La implementación del engaño militar en el teatro de operaciones, como mover algunos elementos de fuerza a áreas alejadas de la dirección real del proceso y la implementación de procedimientos de ocultamiento y camuflaje.
- Desglosar las redes informáticas de la deducción e inyectarlas con información inexacta.

7.2 CREACIÓN DE UN CERT, "COMPUTER EMERGENCY RESPONSE TEAM".

Un CERT consiste en la creación de n Equipo de Respuesta ante Emergencias Informáticas. Las siglas CERT provienen del inglés, "Computer Emergency Response Team" y consiste en la creación de un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de la seguridad global de las redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

También se puede utilizar el término CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas) para referirse al mismo concepto. De hecho, el término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, que está registrado en EE. UU. por CERT Coordination Center (CERT/CC).

7.2.1 Requisitos Básicos para el establecimiento de un CERT.

En cualquiera de los países que estudiaremos en el próximos capítulo el CERT se ha generado en base a los entornos vulnerables propiciados por los

riesgos y amenazas que el entorno cibernético lleva de la mano, una nueva cultura de organización, administración y control, orientada a mejorar las capacidades de sus recursos humanos en materia cibernética y a sus instalaciones para prever algunos eventos, en definitiva, generar una cultura que propicie la ciberseguridad y servirá para dar respuesta además de propiciar el restablecimiento de los sistemas en menor tiempo.

En este contexto las Fuerzas Armadas, deben dedicar sus esfuerzos en dos vertientes principales a partir de las estructuras de respuesta creadas.

1. Que las instalaciones propicien ambientes seguros y mejora en la cultura orientada a la Ciberseguridad.

2. Que puedan desarrollar iniciativas para defender la nación de amenazas externas con la Ciberdefensa orientada a defender y responder oportunamente a las amenazas.

Conforme a las definiciones dadas para el CERT y CSIRT, podemos deducir que estas organizaciones pueden ser creadas en función del ámbito de su competencia, ya que los términos tienden a ser utilizados indistintamente debido a que, en su modo de actuar, realizan actividades que se entrecruzan o se relacionan.

La primera que relacionaremos es el CERT, el cual por definición es un Equipo de reacción rápida ante incidentes informáticos, es una Organización especializada en responder inmediatamente a incidentes relacionados con la seguridad de las redes o los equipos publicando alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.[202]

De acuerdo con lo dispuesto ea la Agencia de la Unión Europea para la seguridad de las redes y la información (ENISA), el CSIRT proviene del inglés Computer Security Incident Response Team, y se asocia al mismo concepto que el

[202] CCN, Centro Criptológico Nacional. (2015). Guia de Seguridad (ccn-stic-401) Glosario y abreviaturas. Madrid: Editor y Centro Criptológico Nacional.

CERT, sin embargo, estos últimos fueron asociados a una estructura capaz de reaccionar ante la ocurrencia de un evento, siendo el CSIRT algo más preciso que implica incluso los servicios de prevención, alertas y avisos para los servicios de prevención de la seguridad pública o privada. Como resultado, el nuevo término CSIRT se estableció al final de los años 90. En la actualidad, ambos términos (CERT y CSIRT) se utilizan de manera sinónima, siendo CSIRT el término más preciso.

Observando ambas definiciones, podemos observar que, aunque ambas surgen del mismo aspecto de seguridad informática, no es menos cierto que el CERT es más asociado a enfrentar una emergencia que ya ha provocado un colapso en algunos de los sistemas y el CSIRT se orienta a las capacidades preventivas en términos de seguridad, alertas e intrusión.

Estos equipos entienden por ciberataque a una Operación llevada a cabo por individuos, instituciones o Estados, ya sea de forma ofensiva o defensiva, con la finalidad de causar daños y destrucción de objetos e infraestructuras. Sin embargo una consideración interesante a este aspecto es determinada por la propia definición en cuanto al fin que persigue, ya que es difícil determinar si estos ciberataques persiguen la muerte de las personas, su alcance o las consecuencias sin son previsibles de antemano, por esto desde el punto de vista del Derecho Internacional de los Conflictos Armados mejor conocido como DICA, es difícil enfocarlo en una de sus categorizaciones, ya que aunque como norma general no genera muerte de las personas, pero si los efectos colaterales causados hacia componentes físicos o lógicos de un sistema informático, como el caso de la transportación.[203]

Entre los requisitos más importantes para tener en cuenta para la creación de CERT, independiente de los dispuesto en el marco legal los recursos necesarios (humanos, tecnológicos, físicos y lógicos), la organización no solo debe surgir de la nada, sino que es parte de un proceso de madurez, que debe dar inicio con una instancia tecnológica, que luego pueda dar sus primeros pasos. En

[203] Antonio Diaz, Fernandez, María, Teresa Cabre, Marcelino Elosa, Josefa Gomez Enterria. (2013). Diccionario LID de Inteligencia y Seguridad. Madrid: LID Editorial Empresarial.

consecuencia se deduce que la oferta de los servicios que mantengan sean proporcionales al medio al que deberá enfrentarse, de ahí que la propia Guía para la Creación del CERT/CSIRT elaborada por el Centro Criptográfico Nacional de España señala algunos aspectos a considerar para cada una de estas instancias.

- EL tiempo de operación, ya que las instancias de este tipo que operen una, dos o tres tandas en función de 8, 16 o 24 horas requerirán entonces personal operativo para cada una de estos. Sin embargo, se destaca que las entidades que prestan estos servicios en horario laborables corren el riesgo de acumular mayor cantidad de demanda de servicios.
- El tamaño a la población o usuarios que se les brindara el servicio, ya que dependiendo de la cantidad de usuarios, estos habrán de demandar determinadas acciones o atenciones de servicio que pueden hacer colapsar la propia estructura, producirse una denegación de servicio o una perdida en la credibilidad en función a la recepción de los operarios o la capacidad de resiliencia.
- El grado de autoridad entre los usuarios y la relación jerárquica, en atención al orden de prioridades para la atención, si se trata de un evento que afecta a toda una institución, departamentos o individuos, pero en el ambiente militar, supone además que aún se tratare de señalamientos individuales, debe considerar el nivel jerárquico de la instancia de mando que requiere la atención.
- La expedición regular de normativas y avisos de seguridad con la autoridad de aplicación inmediata y obligatoria.
- EL estándar de tiempo para la respuesta es requerido para identificar y medir la capacidad del CERT en atender a las demandas por debajo del tiempo requerido, puede ser en 12, 24 o 72 horas, a partir de que sea recibido el requerimiento, lo cual estará asociado a la disponibilidad de receptores automáticos.

En cuanto al proceso de maduración y proyecto de crecimiento, hay que tener en cuenta que la creación de un CERT involucra un proceso en el cual sea considerado maduro, y que propicie la creación de otras instancias similares en

los diferentes cuerpos o servicios dependientes del Ministerio de Defensa, creando una infraestructura que permita interconectar todos los CERT/CSIRT de los distintitos países. El tiempo para considerar para su madurez es de dos años aproximadamente.

Asimismo, en cumplimiento a los términos de la Estrategia de Seguridad Cibernetica de la OEA.[204], se establece que dado el creciente número de incidentes de seguridad y en respaldo a la Estrategia Interamericana Integral de Seguridad Cibernética, el CICTE formulará planes para la creación de una red hemisférica que funcione 24 horas al día, 7 días a la semana, de Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT) con la capacidad y el mandato de divulgar correcta y rápidamente información relacionada con la seguridad cibernética y proporcionar orientación y apoyo técnico en el caso de un incidente cibernético.

Esta estrategia demanda que puntos nacionales CERT/CSIRT mantengan un enlace permanente con los organismos regionales y mundiales, a los fines de anticipar cualquier daño a sus sistemas.

7.2.2. Ventajas que ofrece la creación de un CERT.

Conforme a la CCN-STIC-810, Guía de Creación de un CERT/CSIRT, la creación de este tipo de estructura refleja algunas ventajas que pueden ser resumidas en la mejora de los tiempos de respuesta y la resolución de incidentes mediante: La centralización de las acciones en una única estructura, eficiencia en el uso de recursos, incremento de la coordinación internacional con grupos de contacto similares, adquirir las competencias para detectar, manejar y reponerse en breve tiempo.

Asimismo, mejor la eficiencia de los costos de adquisición de servicios ya que es la única entidad especializada, con las competencias técnicas para decidir en cuanto a la adquisición de bienes y servicios para la seguridad informática.

---

[204] Resolución AG/RES. (2004) estrategia de seguridad cibernética.

Las instituciones estatales al igual que los componentes del Ministerio de Defensa de la República Dominicana han venido realizando una serie de actividades enmarcadas en el proyecto Republica Digital, el cual consiste en proporcionar acceso a los servicios y con calidad a todos los ciudadanos a través de las redes informáticas. Busca garantizar el acceso de los dominicanos a las tecnologías de la información y comunicación, con el objetivo de reducir la brecha digital y brindar mejores servicios a la ciudadanía. Esta iniciativa está fundamentada en cuatro ejes principales y dos transversales.

Estos servicios dispuestos a todos los ciudadanos requieren que a través de uno de sus ejes transversales como la Ciberseguridad, genere la confianza en los medios electrónicos, atendiendo a las capacidades institucionales para proteger y preservar la información. Conforme al mandato de la Estrategia Nacional de Ciberseguridad 2018-2021 se procura crear las condiciones necesarias para garantizar el uso de las nuevas tecnologías, los medios electrónicos, las redes gubernamentales y privadas y preservar la información.

Otra de las ventajas que ofrece la configuración de un CERT es que en además de proporcionar confianza y seguridad en la población este debe estimular a una cultura de ambiente seguro donde no solo se tome en cuenta la participación de las instituciones estatales y de los Cuerpos de Defensa, sino que además propicie la participación publico privada.

7.2.3. La importancia de la Gestión de Riesgo en la creación de un CERT/CSIRT.

Si nos referimos a la Gestión de riesgo, la Estrategia Nacional de Ciberseguridad establece como una de sus prioridades la identificación del método o forma para evaluar el mismo del modo más especial y los más preciso posible dentro de la dificultad que ello supone.

Del análisis de las definiciones anteriores podemos concluir que un activo es cualquier recurso de la institución o la empresa que sea necesario para desempeñar las actividades diarias y cuya no disponibilidad o deterioro supone daño o un costo elevado. Sin embargo, dependiendo de la naturaleza de los servicios prestados y los niveles de exposición, algunos activos quizás no sean tan vulnerables como otros.

En el documento del Instituto Nacional de Ciberseguridad de España, bajo el título: "Gestión de riesgos: Una guía de aproximación para el empresario" (INCIBE, 2019) identifica el nivel de riesgo como la estimación de lo que puede ocurrir con un activo que ha sido afectado por una amenaza.

Para la Gestión del Riesgo se precisa desarrollar dos grandes tareas: El análisis del Riesgo, y el tratamiento de riesgos. El objetivo que se persigue con estas tareas consiste en indagar el nivel de riesgo en base a la ocurrencia en el histórico, hacer una clasificación de las amenazas y establecer la frecuencia en que ocurren además de los posibles impactos en función del daño que puedan provocar.

Si nos referimos al tratamiento del riesgo, éste se asocia a las acciones que la institución pretende abordar y a los fines de reducir el impacto que pueda causar la amenaza. Esto supone una inversión en recursos que en muchos casos debe ponderarse en función del beneficio que puedan aportar.

Para el tratamiento del riesgo, existen varias hay opciones que pueden ser aplicadas ante las que destacemos por su importancia:

1) Eliminación total del riesgo: Esto puede ser alcanzado, cuando se logran eliminar las causales que lo provocan o cuando el activo es fácilmente reemplazable o sustituido por otro que no puede ser afectado de igual forma. (Por lo general puede ser más costosa).

2) Reducirlo o mitigarlo: Cuando a través de algunas medidas se puede lograr que baje el nivel de riesgo a niveles manejables o que no retrasen, interrumpan o detengan las actividades. Puede ser gestionado tomando medidas preventivas que reduzcan el impacto de la amenaza.

3) Transferirlo o compartirlo: Cuando la institución tiene la facilidad de contratar a un tercero para algún servicio o tarea, pasando la responsabilidad o el riesgo a otro.

4) Aceptarlo: Cuando se asume el riesgo en función a márgenes de tolerancia, daños recuperables o cuando la probabilidad de ocurrencia es muy alta, ya que la frecuencia en términos de meses o años para que ocurra, son elevadas.

Sin embargo, cuando se habla de la Gestión de Riesgos en cuanto a la seguridad de los estados, el principal activo es la información, la infraestructura para su manejo y almacenamiento y los equipos para utilizarla. Esto abarca la información física en documentos, así como la que se encuentra en espacios virtuales o en la nube.

En este sentido hay que priorizar la seguridad de la información y debe preservarse su confidencialidad, Integridad y Disponibilidad. La Confidencialidad debe ponderar tres elementos importantes, debe estar disponible o divulgada al personal autorizado, la Integridad en que la misma debe permanecer igual que como la remitió el emisor, y la disponibilidad que debe estar accesible al usuario que la requiera.

7.3 ESTRATEGIAS DE ONU EN CIBERSEGURIDAD.

El panorama de los Servicios de Inteligencia (SI's) en los países desarrollados ha evolucionado mucho desde la aparición de Internet haya en la década de los sesenta. La clásica idea del espía buscando información de interés a pie de calle es cada vez menos frecuente. Hoy en día, gran cantidad de nuestras actividades diarias giran en torno a las TIC's.

Por este motivo, muchos países han invertido grandes recursos en la transformación de su tecnología llegando a tener en la actualidad, una gran capacidad para llevar a cabo operaciones de APT. Debido a esta evolución tecnológica han surgido multitud de grupos APT. Entre ellos encontramos "Equation Group".

"Equiation Group" utiliza una amplia infraestructura de servidores de C&C de más de 300 dominios y más de 100 servidores. Los servidores están alojados en múltiples países, incluyendo los Estados Unidos, Reino Unido, Italia, Alemania, Panamá, Costa Rica, Malasia, Colombia y la República Checa.

Desde 2001, "Equation Group" ha estado muy activo infectando miles de víctimas en más de 30 países, cubriendo los principales sectores de interés estratégico, tecnológico y militar. En agosto de 2016, se dio visibilidad desde una cuenta de Twitter una serie de información donde se vinculaba al grupo

"Equation Group" con la NSA de los Estados Unidos, y que supuestamente, también estuvieron vinculados con los ataques Stuxnet[205], Regin o Fanny.

En cuanto a la incidencia en España, en los años 2014 y 2015 diversos departamentos ministeriales de nuestro país, al igual que ciertas empresas fueron objetos de ciberataques relacionados con el espionaje (ciberespionaje) procedentes de equipos ubicados en Rusia y China.

Como viene siendo habitual, los correos electrónicos maliciosos fueron la herramienta más usada por los sujetos activos. Actualmente, el Spear Phising es la técnica que obtiene los mejores resultados para los atacantes. Los Ministerios de Industria, Interior, Defensa, Asuntos Exteriores y de la Presidencia registraron el mayor número de tentativas de ciberataques, usando en todos los casos los métodos y las herramientas de las Amenazas Persistentes Avanzadas (APT's).

Al igual que años anteriores, en los incidentes críticos registrados se vieron afectados diferentes empresas estratégicas españolas, en las que diferentes atacantes, principalmente con origen en China, cuyo objetivo era el robo de propiedad intelectual e información I+D de estas compañías.

Conforme a las políticas desarrolladas en la Organización de las Naciones Unidas, para la lucha contra el Terrorismo, se ha entendido que tanto actores independientes como las organizaciones terroristas poseen la capacidad de utilizar el Internet, las redes y el ciberespacio, para llevar a cabo sus operaciones, que permitan hacer colapsar los sistemas políticos, económicos, sociales, de transporte o a través de la explotación directa de ingeniería social, que le permita obtener informaciones al respecto de blancos específicos.[206]

---

[205] STUXNET. Este gusano podría parecer uno más si no se le analiza en detalle. Sin embargo, ha sido descrito como "prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentística mundial"

[206] UN, Consejo de Seguridad, CTC. (2019). Information and communications technologies (ICT).

De otro lado, las redes pueden está siendo utilizadas para la captación, reclutamiento, incitación, difusión, comunicaciones y financiamiento de operaciones criminales y delictivas, en sus actividades para generar un caos mundial. Para abordar toda esta problemática que involucra el uso de tecnologías de información y Comunicación (TIC´s) para fines vinculados al terrorismo, su financiamiento y proliferación, el Consejo de Seguridad ha adoptado varias resoluciones las cuales se resumen de la manera siguiente:

Normativa existente y fecha de aprobación	Objetivos que persigue
Resolución 1373 (2001)	Insta a todos los Estados Miembros a encontrar formas de intensificar y acelerar el intercambio de información operativa sobre el uso de las TIC por parte de grupos terroristas y de reprimir el reclutamiento de terroristas
La resolución 1624 (2005)	Insta a todos los Estados Miembros a legislar localmente en la prohibición de la incitación a cometer un acto terrorista y prevenir esa conducta. Identifica la importancia de la colaboración internacional para impedir el uso de las TIC,s y los medios de libre acceso para captar, incitar o financiar actos terroristas.
La resolución 2129 (2013)	Consejo de Seguridad ordena a la Dirección Ejecutiva del Comité contra el Terrorismo (CTED) que consulte a los Estados Miembros sobre el uso de las TIC en actividades terroristas, las organizaciones internacionales, regionales y subregionales, el sector privado y las organizaciones civiles. Sociedad civil.
La resolución 2178 (2014)	Sobre el respeto a los Derechos humanos y las libertades fundamentales en virtud del Derecho Internacional, de los combatientes terroristas extranjeros, instando a los Estados miembros que actúen de manera cooperativa cuando toman medidas nacionales para evitar

	que los terroristas exploten la tecnología, las comunicaciones y los recursos para incitar el apoyo a los actos terroristas.
Marco de acción del CTED	Centrado en cuatro pilares: 1. La incorporación de las TIC en su evaluación de la implementación por los Estados miembros de las resoluciones 1373 (2001), 1624 (2005) y 2178 (2014); 2. La promoción de la autorregulación de la industria; 3. Fortalecimiento de la asistencia legal mutua en materia de contenidos digitales; y 4. Promover técnicas de contra-mensajería, e incluso electrónica.

A partir de la incorporación del Marco de acción común para el Comité contra el Terrorismo, las acciones corporativas en lo que corresponde al uso de los medios electrónicos e internet posteriormente han sido dirigidas para fines auténticos. En este orden, el Consejo de Seguridad de Naciones Unidas aprobó el diseño de un Marco Integral para poder enfrentarse de conformidad con el Derecho Internacional, así como las formas en que el ISIS, Da,esh, Al-Quaida y otros grupos terroristas utilizaban nos medios comunes de libre acceso para motivar, reclutar y hasta ordenar la ejecución de actos de terror en el mundo.

En este sentido el Comité ha centrado su acción el llevar a cabo políticas y normas nacionales entre los estados miembros enfocadas en limitar o entorpecer la capacidad de los terroristas y grupos para utilizar las redes y en la difusión de su doctrina y acciones. Esto puede observarse en las orientaciones que han desarrollado cada año vinculadas a los temas de: Protección de la Organización política del estado, Uso de medios electrónicos y tecnología para fines de terror y financiación, Participación público privada en la seguridad de las redes, Diseño de marco legal que permita tipificar y sancionar los delitos, y comunicación internacional.

7.4 ESTRATEGIAS DE USA.

Durante la administración del presidente de los Estados Unidos de Norteamérica Barack Obama, se pudo dar inicio a la Iniciativa Nacional de Seguridad Cibernética, donde se pudo determinar a la Ciberseguridad como uno de los mayores retos que enfrentaba la nación americana, en términos de la Seguridad Nacional, así como en la economía (Obama, 2008). Al asumir la presidencia en el 2009 se puso en vigencia la Política del Ciberespacio, involucrando en ello tanto a sector gubernamental, a los gobiernos locales y estatales e incluso a los actores públicos y privados, con la finalidad de poder enfrentarse de la forma más eficaz posible a cualquier amenaza cibernética.

Esta nueva iniciativa puso mucho énfasis en la investigación, desarrollo e innovación en todo lo referente a las nuevas tecnologías, además de propiciar un nuevo esfuerzo educativo con la finalidad de desarrollar una nueva fuerza laboral para el Siglo XXI. Esta Política de Ciberseguridad se basó principalmente en la Iniciativa Integral de Seguridad Nacional de Seguridad Cibernética mejor conocida por sus siglas en ingles CNCI (Comprehensive National Cybersecurity Initiative).

Los objetivos principales de esta política estuvieron enfocados en la necesidad de protección que precisaba los Estados Unidos de Norteamérica en el Ciberespacio en tres líneas de acción muy bien definidas y que fueron:

1) Establecer una primera línea de Defensa contra las amenazas cibernéticas del presente a la vez que mejora las condiciones para el futuro, permitiendo una capacidad de reacción ante los ataques y evitar las intrusiones.

2) Para defenderse de todas las amenazas al mejorar sus capacidades de contrainteligencia, y aumentar la seguridad de la información y las redes.

3) Promover la educación en ciberseguridad y en investigación y desarrollo de las tecnologías de información, a los fines de disuadir las actividades de las amenazas

Con estas tres líneas de acción, el estado se prepara para defenderse, responder, Estudiar y contraatacar. Así que en cierta forma el Gobierno del Expresidente Barack Obama, interpretaba los informes de sus asesores y agencias estatales, lo

que permitía predecir en líneas generales que estaba frente a una nueva problemática a nivel mundial.

Las iniciativas que se desprendieron de esta primera fueron las que se detallan en el siguiente cuadro que incluye las doce (12) iniciativas prioritarias con sus correspondientes responsabilidades y objetivos:

Título de la Iniciativa	Responsabilidades	Objetivos
Iniciativa 1: Manejar la red Federal como una red comercial con seguridad.	Establecer una red de comunicaciones de TIC segura, entre todos los actores federales.	Garantizar la comunicación segura entre todos los actores del gobierno.
Iniciativa 2: Instalar sensores pasivos	Desplegar una serie de sensores pasivos entre todos los actores de la red federal, con intentos no autorizados, bajo los protocolos del EINSTEN 2.	Identificar los intrusos al sistema en tiempo real y comunicar al CERT correspondiente.
Iniciativa 3: Perseguir mediante el despliegue de dispositivos.	Perseguir a los intrusos al sistema de la red federal a través del programa EINSTEN 3.	Identificar y caracterizar el tráfico de red malicioso para mejorar el análisis de ciberseguridad, y respuesta de seguridad. Con capacidad de detectar y responder automáticamente. a las amenazas cibernéticas antes de que se haga el daño, proporcionando un sistema de prevención de intrusiones que

		soporta Defensa dinámica. EINSTEIN 3 ayudará a DHS US-CERT a defender, proteger y reducir vulnerabilidades.
Iniciativa 4: Reenfocar la Investigación y Desarrollo.	Propiciar la inversión federal en I+D.	Incentivar la producción de las investigaciones de contratistas gubernamentales en herramientas y dispositivos que propicien mejores condiciones de seguridad.
Iniciativa 5: Conectar los centros de investigación.	Interconectar los centros de protección de información con los de operaciones estratégicas.	Mejorar las capacidades de respuesta a través de la integración de los recursos y la compartimentación de las informaciones.
Iniciativa 6: Desarrollar un Plan de CI Cibernética.	Coordinar las actividades en todos los estados federales. Agencias para detectar, disuadir y mitigar la amenaza de inteligencia cibernética patrocinada por extranjeros para los EE. UU. Y Sistemas de información del sector privado.	Desarrollo de las capacidades del personal de las agencias de CI
Iniciativa 7: Garantizar la seguridad de las redes.	Garantizar el flujo de información ininterrumpido en las redes entre las agencias estatales.	Proteger la información sobre diferentes amenazas e investigaciones.

Iniciativa 8: Ampliar la Educación cibernética	Propiciar la enseñanza relacionada con la Ciberseguridad.	Lograr mas recursos humanos con este conocimiento especializado.
Iniciativa 9: Diseñar estrategias en Ciberseguridad.	Establecer estrategias de ciberseguridad que conecte con el sector privado inclusive.	Mejorar las capacidades actuales en un lapso de 5 a 10 años.
Iniciativa 10: Definir y desarrollar programas de disuasión.	Establecer programas no tradicionales de ciberseguridad con miras a responder adecuadamente.	Disuadir a los adversarios, Intrusos o atacantes.
Iniciativa 11: Desarrollar vías alternas para negocios.	A los fines de asegurar el comercio y las transacciones electrónicas, se propone una red de vías alternativas.	Garantizar el flujo ininterrumpido de la información de negocios y comercio interconectado con el mundo.
Iniciativa 12: Proteger la infraestructura critica	A sabiendas de que EUA depende de infraestructura crítica pública o privada, es su interés protegerlas en su conjunto.	Garantizar el correcto funcionamiento del País, junto con la infraestructura vital para su permanencia y desarrollo, conjugando en esta iniciativa al sector privado.

Tabla 1: Iniciativas tomadas en cuenta para la formulación de la estrategia de Ciberseguridad en E.E.U.U a partir del 2009.

De lo reseñado anteriormente podemos identificar aspectos que marcan la importancia de estas iniciativas. Con ellas se pretenden identificar a las amenaza que opera por el ciberespacio como una realidad y, por consecuencia, identifica lo que son sus debilidades del momento, tales como, la capacidad del personal, la

interconexión entre las agencias, la identificación y persecución del delito, la capacidad de protección de las infraestructuras, la mejorar la capacidad al responder a los eventos, procurar la relación publico privada y especialmente la protección de la red de información vital para el país incluso en el ámbito de los negocios o el comercio.

7.5 ESTRATEGIA DE REINO UNIDO.

En el caso del Reino Unido el país ha asumido las iniciativas de la Unión Europea en materia de Ciberseguridad, pero para dar especial seguimiento a las actividades crea el Centro Nacional de Ciberseguridad (NCSC), cuya función más importante es la de mantener un ambiente más seguro en el campo de las redes y la información, procurando brindar un ambiente idóneo para trabajar en línea y sin riesgos.[207]

Este centro se dedica especialmente a apoyar a las personas, organizaciones públicas o privadas de Reino Unido, proporcionando respuestas efectivas para minimizar los daños y proporcionar la recuperación de los servicios, evitando la propagación a otros sistemas gubernamentales.

Creado en el 2016 el NCSC tiene su sede principal en Londres y apoyado en la experiencia del Centro para la Evaluación Cibernética (CESG), el CERT-Reino Unido y el Centro de protección de la Infraestructura Nacional. En este sentido el NCSC apoya, además de las organizaciones gubernamentales, a la industria y público en general, a las agencias de Defensa, Seguridad, de Inteligencia y de otras organizaciones internacionales.

La estrategia de Reino Unido denominada "Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space"[208] invita a todos los actores del gobierno, sector privado, socios, industrias e incluso al público en general, para que trabajen de forma conjunta en el mismo sentido con el objetivo de dar cumplimiento de los que denominan sus objetivos estratégicos. Estos

[207] Center., N. C. (2019). National Ciber Security Center.

[208] UK-GOB. (2019). Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. Reino Unido.

objetivos estan orientados a reducir el riesgo y aprovechar las oportunidades mediante la mejora del conocimiento y las capacidades de los individuos en base a la formación especializada en ciberseguridad procurando dotar al país de una ventaja competitiva en la toma de decisiones en materia cibernética.

La estrategia seguida por el Reino Unido utiliza a las herramientas que ofrece la Ciberseguridad para proteger los intereses del país y sus posesiones, permitiendo el uso y desarrollo de nuevas tecnologías sin que la búsqueda de la seguridad efectiva provoque el desaliento de los actores. La tecnología ofrece ventajas que le permitirán posicionarse como la principal economía a través de las garantías ofrecidas en el entorno digital.

Sin embargo, se entiende que este posicionamiento en el mercado también puede contribuir a exponer a la nación de una mayor forma. Sin embargo, considera viable la reducción del riesgo y el aprovechamiento de las oportunidades.

En este sentido, la reducción del riesgo del uso del espacio cibernético por parte del Reino Unido comprende las diversas formas en que sus estructuras e instituciones pueden defender sus sistemas mediante la prevención de ataques, la protección contra ataques y la reducción del impacto de los ataques.

En otro orden cuando deciden aprovechar las oportunidades en el espacio cibernético, lo llevan a cabo partiendo de la base necesaria para cubrir toda la gama de posibles acciones para apoyar la seguridad cibernética y los objetivos más amplios en materia de política de seguridad nacional, como, por ejemplo, en la lucha contra el terrorismo y contra la delincuencia organizada grave. En ambos casos persiguen mejorar su posicionamiento y aprovechar estas ventajas creando un ambiente mucho más seguro.

Para encabezar estas acciones cuenta con el Centro de Operaciones de Seguridad Cibernética donde convergen en una sola una unidad múltiple agencias para monitorear los desarrollos en el espacio cibernético además de proporcionar conciencia colectiva de la situación, analizar tendencias y mejorar la coordinación de la respuesta técnica a incidentes cibernéticos.

Como conclusión, se observa que en la estrategia seguida por el Reino Unido se reproducen en cierta forma todas las actividades desarrolladas por los

países en la búsqueda de proteger, restaurar y minimizar las acciones cibernéticas que puedan afectar sus estructuras. Países cada vez más interconectados quedan más expuestos a las amenazas ciber, por lo que, como tal, deben disponer de la capacidad tecnológica, de sus recursos humanos competentes y por qué no estructuras que de manera especializada mantenga una supervigilancia de todo el espectro nacional.

7.6 NUEVA CONCEPCIÓN DE CIBERDEFENSA DE LA OTAN.

En atención al concepto relacionado a la ciberdefensa podemos concebir a la Ciberguerra como una Acción ejecutada por un Estado con la finalidad de penetrar en los ordenadores o redes informáticas de otro, con el objeto de causar daños o interrupción de servicios. Sin embargo, subyace en esto la diferencia del campo de batalla porque se habla de un ambiente intangible.

El Pentágono reconoció, en 2009, al espacio cibernético como un potencial territorio donde podría librarse un ataque de otros Estados, que podría ir dirigido a infraestructuras críticas, pudiendo así bloquear servicios esenciales como agua, electricidad o transporte; causar daños económicos importantes, e interrumpir actividades cotidianas de ciudadanos, empresas y administraciones.[209]

Es evidente además al recordar los eventos de ciberataques que sufrió Estonia en 2007, muchos países han creado instancias contra guerra electrónica y han reforzado la protección de sus infraestructuras críticas.

Debido a ello el 10 de marzo del 2011, de acuerdo al documento informativo de la OTAN en materia de ciberdefesna, [210]los Ministros de Defensa de la OTAN aprobaron el Nuevo Concepto de Ciberdefensa de la Alianza, que permite asociar a eventos similares en el hemisferio occidental con las Cumbres de Ministros de Defensa de las Américas.

---

[209] Antonio Diaz Fernandez, Maria Teresa Cabre, Marcelino Elosa, Josefa Gomez Enterria. (2013). Diccionario LID de Inteligencia y Seguridad. Madrid: LID Editorial Empresarial.

[210] IEEE 09/2011 (2011): Nuevo concepto de ciberdefensa de la OTAN.

Los eventos de Estonia del 2007 pusieron en las agendas de la OTAN y evidentemente en el mundo, el tema cibernético y la seguridad, debido a que en ese momento fue la primera vez que un país solicitaba apoyo para restaurar sus sistemas luego que fuera atacado, generando un ambiente de impotencia ante estos eventos ya que la OTAN no disponía ni de un plan para los ciberataques ni los recursos para recuperar el sistema.

De la reunión de los Ministros de Defensa celebrada en ese mismo año se decidió adoptar un plan conjunto para todos los países aliados, así como la creación de una política común de ciberseguridad.

De estas reuniones se concluyó un esquema que debía incluir: La coordinación y asesoramiento en ciberdefensa; asistencia a las Naciones; investigación y formación; y cooperación con los socios.

En la Coordinación y asesoramiento instaba bajo el marco Cyber Defence Management CDMA[211], como el responsable de propiciar la política de ciberdefensa a implementarse a través de las autoridades políticas, militares y técnicas de la OTAN, así como por las naciones.

La asistencia a las naciones, provista a través de equipos de asistencia rápida a emergencias, además de instar a la creación de CSIRT nacionales además de los sectoriales.

La investigación y formación en ciberdefensa, a través del Centro de Excelencia OTAN de Ciberdefensa Cooperativa (Cooperative Cyber Defence Centre of Excellence -CCDCOE) en Tallinn, Estonia fue acreditado en 2008. Este centro se encarga de la investigación y formación en ciberguerra con personal experto de los diez países que lo patrocinan. [212]

[211] NATO Cyber Defence Management Authority-CDMA

[212] CESEDEN-IEEE. (s.f.). DOCUMENTO INFORMATIVO DEL IEEE 09/2011. NUEVO CONCEPTO DE CIBERDEFENSA DE LA OTAN. Ministerio de Defensa España.

Con esto se perciben 3 ejes fundamentales:

1.- La Creación de la infraestructura física y tecnológica para enfrentar ataques cibernéticos con un marco legal común,

2.- La Creación de equipos de reacción ante eventos,

3.- La formación académica en temas de ciberseguridad a través de centros de excelencia y formación especializada.

Sin lugar a dudas estos eventos permitieron considerar el espacio cibernético como un nuevo espacio de batalla cuya característica principal se basa en la falta de delimitación territorial espacial, donde no solamente sería afectados los blancos u objetivos militares, sino que además se estaría contemplando el hecho de que estas acciones afectaban además al conglomerado civil incluso provocando la pérdida de vidas humanas y recursos de inocentes.

7.7 GRUPOS CON ORIGEN EN RUSIA

En la última década, Rusia destaca como una de las principales fuentes de la tipología de las diferentes ciberamenazas. Los diferentes ataques realizados a lo largo de los últimos años han venido motivados por las decisiones políticas de este país, como ejemplo, la participación de Rusia en el conflicto bélico sirio.

Según las fuentes consultadas, señalan a los siguientes grupos como los más activos de este país:

- SNAKE
- FANCY BEAR
- APT28
- SOFACY
- COZY DUKE
- COZY BEAR
- SANDWORM

Características de los grupos rusos

Los ciberataques de estos grupos presentan unas características generales, que hacen posible que se vinculen su origen entre ellas. Una de estas características sería la utilización de herramientas y tácticas, las cuales se actualizan permanentemente, y que han sido diseñadas específicamente contra objetivos muy concretos. Estas herramientas se caracterizan por su diseño para evitar la detección y que se le atribuya la autoría del ciberataque.

Por otra parte, el conocimiento técnico sobre Windows y otros sistemas operativos es muy elevado, así como que la mayoría de los ataques han sido realizados contra entidades Gubernamentales y Administraciones Públicas de los países atacados. Esta compleja técnica se ha ido incrementando en las últimas décadas, por lo que han usado mecanismos de ocultación de su actividad tanto en el tráfico interno como en el de salida.

Mantienen protocolos para la extracción de la información, usando técnicas de exfiltración muy depuradas, por otra parte, tienen técnicas que dificultan el análisis del código por los investigadores de seguridad y que dificultan las tareas de investigación.

7.8 GRUPOS CON ORIGEN EN CHINA

Al igual que Rusia, China ha mostrado claramente ser unos de los orígenes más significativos de los ataques de ciberespionaje de los últimos años.

Las características generales de las campañas de ciberespionaje que han tenido su origen en China responden a una decisión mayormente política que estableció el uso de Internet para recolectar información de interés nacional para China, en diferentes ámbitos como el político, económico, industrial, militar y comercial. Estos grupos muestran un especial interés por la propiedad intelectual de empresas que tienen un alto conocimiento y caudal tecnológico.

Existen diferentes grupos los cuales mantienen diferentes niveles y conocimientos técnicos, con un denominador común en todos sus ataques, al predominar el uso de herramientas comerciales. Estas técnicas han ido evolucionando y mejorándose para evitar la detección y la atribución de los ciberataques, a la vez que han implementado medidas para mejorar la seguridad en sus operaciones.

A diferencia de Rusia, existen organismos del gobierno chino que supuestamente se han encontrado detrás de los ciberataques de estos últimos años, a saber:

- MINISTERIO DE SEGURIDAD DEL ESTADO (MSS).

- EJERCITO DE LIBERACIÓN CHINO.

- OFICINA DE RECONOCIMIENTO TÉCNICO.

Por otra parte, se le pueden atribuir ataques a China y sus diferentes grupos más activos[213] utilizadas por los sujetos activos fueron desarrolladas en chino, lo que indica una posible atribución a dicho país.

Aunque Rusia y China son dos de los actores más activos en materia de ciberespionaje hay otros países, como Corea del Norte e Irán, que están tomando cierta relevancia en este campo, donde en Corea del Norte se ubica el grupo DARK SEOUL como el más activo, mientras en Irán se encuentra el Grupo ROCKET KITTEN.

Uno de los directores del FBI, Robert Mueller, Abogado y funcionario público estadounidense que fue el 6º director del FBI del 2001 al 2013, afirmó a la Comisión de la Cámara de Inteligencia, que el Ciberespionaje "constituía una de las amenazas más importantes y complejas a las que se enfrenta la nación", cuando se le preguntó el nombre de los peores delincuentes de todo el mundo que representa una seria amenaza a los Estados Unidos, Mueller dijo: "hay países como Rusia y China, y otros tal vez como Corea del Norte e Irán que tienen capacidades, y donde estamos en continua alerta".

213 http://researchcenter.paloaltonetworks.com/2016/05/operation-ke3chang-resurfaces-with-new-tidepool- malware

7.9 LA SITUACIÓN EN LA REPUBLICA DOMINICANA.

Dentro del marco legal, la República Dominicana, en función a la seguridad de las comunicaciones y las tecnologías, se basa en el marco de referencia, las siguientes en función a su ámbito de competencia y las necesidades en función de las amenazas percibidas al momento de su creación. Estas pueden ser identificadas en el siguiente cuadro:

Número y fecha de creación	Denominación	Aspectos que regula
LEY No. 126-02	Sobre comercio electrónico, documentos y firma digital.	Facilitar el comercio electrónico entre y dentro de las naciones, validar las transacciones entre las partes. Admisibilidad como prueba del documento digital, Uso y validación de la Firma Digital,
LEY No. 310-14	Sobre la regulación del envío de correos electrónicos no solicitados (SPAM)	Tipificación del delito informático, y de los daños causados por los correos masivos provocando denegaciones de servicios o disminución del ancho de banda.
Ley No. 53-07	Sobre Crímenes y Delitos de Alta Tecnología.	Tipifica como acciones criminales o delictivas el divulgar, generar, copiar, grabar, capturar, utilizar, alterar, traficar, desencriptar, decodificar o de cualquier modo descifrar los códigos de acceso, información o mecanismos similares, a través de los cuales se logra acceso ilícito a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, o falsificar cualquier tipo de dispositivo de acceso al mismo. Delitos de propiedad intelectual, pornografía, acoso, sustracción de dinero o

		información.
2015	Constitución de la República Dominicana	La Constitución de la República Dominicana establece los derechos y deberes fundamentales de los ciudadanos entre los que se encuentra la libertad de expresión, la integridad e inviolabilidad de la correspondencia y demás documentos privados;
Ley No. 155-17	Ley contra el lavado de activos y el financiamiento del terrorismo	Vinculada a la persecución y uso de recursos mal habidos, utilizados para el blanqueo de capitales y/o su uso con propósito de proporcionar apoyo financiero a organizaciones criminales o de terroristas.
Decreto 230-18	Estrategia Nacional de Ciberseguridad 2018-2021.	Establece la estrategia de ciberseguridad para la nación así como la creación de un CERT para la República Dominicana.

Basado en el marco legal establecido con anterioridad a la promulgación del Decreto Presidencial 230-18, la República Dominicana asume su compromiso de garantizar la seguridad de los sistemas de información, así como de las infraestructuras críticas (Gobierno_Domincano, 2018).

El objeto de su creación es establecer y regular la estrategia nacional en materia de Ciberseguridad del 2018-2021, con la misión de establecer los mecanismos necesarios para la protección del estado, sus habitantes y el aseguramiento del desarrollo y seguridad nacional, con el objetivo principal de

considerarse en el año 2021 como un país más seguro en cuanto al ciberespacio y las actividades de sus ciudadanos.[214]

Para su aplicación, la citada estrategia contempla un desarrollo en función de 4 pilares fundamentales:

1.- Marco legal y fortalecimiento institucional,

2.- Protección de infraestructuras Críticas e Infraestructuras TI del Estado,

3.- Educación y cultura nacional en ciberseguridad,

4.- Alianzas nacionales e internacionales.

El objetivo del pilar número 1 se fundamenta en el Marco legal y fortalecimiento institucional tenido como prioridad fortalecer el marco legal que permita a las unidades competentes y especializadas en esta materia de estudio desarrollar sus actividades para mejorar sus capacidades para prevenir, investigar y actuar en casos de delitos de alta tecnología. Este pilar se deriva en diferentes objetivos específicos y líneas de acción de las cuales se podrán evidenciar en el cuadro elaborado para tales fines, las cuales se vinculan a las Fuerzas Armadas.

En cuanto al Pilar 2 va referido a la protección de Infraestructuras Criticas Nacionales e Infraestructuras TI[215] del estado, cuyo objetivo general se enmara en asegurar el funcionamiento y la protección de la información almacenada en las infraestructuras críticas y de TI del Estado. Este pilar enmarca una gran responsabilidad en cuanto a las FFAA y su participación, ya que es el principal garante de la protección de la mayoría de las instalaciones gubernamentales.

En cuanto al Pilar 3: La educación y cultura nacional en ciberseguridad. En este pilar se persigue fomentar principalmente una cultura de seguridad cibernética, además de fomentar la inclusión en los programas educativos de todos los niveles formación especializada y la inclusión como tema transversal.

---

214 Gobierno_Domincano. (2018). Estrategia Nacional de Ciberseguridad 2018-2021. Decreto 230-18 Estrategia Nacional de Ciberseguridad 2018-2021. Santo Domingo, Republcia Dominicana.

215 La infraestructura de TI se define como un conjunto de dispositivos físicos y aplicaciones de software que se requieren para operar la empresa.

Así por último el Pilar 4: La Formación de Alianzas Nacionales e Internacionales, procurando establecer alianzas duraderas entre el sector público y privado y la sociedad civil con organismos e instituciones naciones e internacionales para fomentar lazos en procura de mejores alternativas de propiciar una ciberseguridad.

PILAR	Objetivo especifico	Líneas de acción
I Marco legal y fortalecimiento institucional	1: Fortalecer el marco jurídico que facilite un ciberespacio seguro en RD.	1.1 Desarrollar un plan de actualización y reforma del marco jurídico. 1.2 Establecer un plan de actualización del marco regulatorio, dados los cambios
	2: Fortalecer las capacidades de los órganos de investigación de crímenes y delitos de alta tecnología.	2.1. Realizar una evaluación de las capacidades de los cuerpos de investigación. 2.2. Incluir en el plan de estudios programas de investigación y seguimiento a evidencias. 2.3 Fortalecer la relación de la policía con la ciudadanía en la mejora de la confianza para hacer denuncias.
2.- Protección de infraestructuras Criticas e Infraestructuras TI del Estado	1.- Identificar las Infraestructuras criticas y de TI de la nación.	1.- Establecer los criterios para la evaluación. 2.- Catalogar las Infraestructuras Criticas y de TI. 3.- Efectuar el análisis de riesgo de las Infraestructuras críticas y de TI e identificar su vulnerabilidad.
	2.- Elaborar y poner en ejecución un plan para	1.- Considerara las mejores prácticas en ciberseguridad.

	robustecer la seguridad de la infraestructura critica.	2.- Analizar y mejorar las normas emitidas en ciberseguridad.
	3.- Mejorar la Coordinación intersectorial	1.- Establecer un Equipo se respuesta ante incidentes cibernéticos (CSIRT-RD) 2.- Promover la creación de equipos sectoriales de respuestas a incidentes cibernéticos y ayudar al CSIRT-RD. 3.- Definir y aplicar un protocolo de comunicación entre los Equipos sectoriales y el CSIRT-RD 4.- Hacer cumplir los requisitos mínimos de seguridad y recuperación de las Infraestructuras críticas y de TI del estado.
	4.- Elaborar un plan de respuesta ante incidentes	1.- Identificar las entidades relevantes para la actuación. 2.- Definir el protocolo de activación y actuación de las instituciones ante incidentes de ciberseguridad. 3.- Coordinar y monitorear las actividades de recuperación de incidentes hasta la normalidad. 4.- Crear un plan de ejercicios periódicos y prácticas en incidencias cibernéticas, del estado y del sector privado.

Pilar 3: Educación y cultura nacional en ciberseguridad	1.- incorporar el manejo de los temas fundamentales en seguridad informática.	1.- Incluir planes de capacitación en materia de ciberseguridad al personal docente del nivel básico y medias escuelas públicas. 2.- adecuar los planes de estudio de educación básica y media.
	2.-Adecuar los planes de estudio básica, grado y postgrado a ciberseguridad y cibercivismo.	1.- Planes de capacitación a docentes de grado y posgrado en ciberseguridad.
	3.- Crear un marco de coordinación académica en ciberseguridad.	1.- Propiciar la investigación en ciberseguridad. 2.- Desarrollar un programa de caza talentos en ciberseguridad. 3.- Establecer un programa de formación continua para los servidores públicos. 4.- Sensibilizar a la población civil.
Pilar 4: Alianzas Nacionales e Internacionales	Fomentar mecanismos de cooperación nacional con los sectores público, privado y sociedad civil.	1.- Establecer alianzas para la creación de una plataforma de seguimiento conjunta. 2.- Asegurar la participación de la República Dominicana en foros y eventos internacionales en materia de ciberseguridad. 3.- Fomentar el intercambio de información nacional e internacional.

Tabla: Identificación por pilares de las vinculaciones de las FFAA a la Estrategia de Ciberseguridad RD 2018-2021.

Con el estudio más profundo de los aspectos establecidos como pilares fundamentales para la Estrategia de Ciberseguridad de la República Dominicana del 2018 al 2021, se evidencia la necesidad de implementar algunas acciones como la creación del CERT-MIDE, a los fines de cumplir con el mandato de esta, así como poder dentro del Ministerio de Defensa responder ante eventos de naturaleza informática que puedan trastornar la seguridad y la paz de la nación.

-LA SEGURIDAD DEL CIBERESPACIO EN ESPAÑA. -

VIII .LA SEGURIDAD DEL CIBERESPACIO EN ESPAÑA

8.1 INTRODUCCIÓN

La ciberseguridad es el conjunto de actividades centradas en mecanismos defensivos (ciberdefensa) y ofensivos (ciberataques) empleados tanto para proteger el ciberespacio contra el uso indebido del mismo, para defender su infraestructura tecnológica, así como los servicios que prestan y la información que manejan; como para utilizar las capacidades del ciberespacio como arma de ataque por razones de seguridad o actividad militar. En esta dirección, la ciberseguridad se puede utilizar para propósito de espionaje, de sabotaje o de subversión, entre otras actividades.

La ciberseguridad y la ciberdefensa son dos áreas que se están convirtiendo en prioridades las agendas de los distintos estados, la causa principal es el auge del ciberespionaje y las amenazas híbridas. El ex presidente de los EE.UU., Barak Obama ya situó la seguridad del ciberespacio y su defensa en primera línea de la agenda política de su país en el año 2015. El desencadenante más relevante de que la ciberseguridad pase a un puesto prioritario en la seguridad de los diferentes países se debe principalmente a dos sucesos, por una parte, el ciberataque sufrido por Sony Pictures Enterntainment en el año 2014 y por otra parte, los ataques terroristas de París (Francia) en noviembre del 2015.

Otro de los conceptos relacionados es el CSIRT el cual de acuerdo a la Agencia de la Unión Europea para la seguridad de las redes y la información (ENISA), el CSIRT proviene del inglés Computer Security Incident Response Team, y se asocia al mismo concepto que el CERT, sin embargo, estos últimos fueron asociados a una estructura capaz de reaccionar ante la ocurrencia de un evento, siendo el CSIRT algo más preciso que implica incluso los servicios de prevención, alertas y avisos para los servicios de prevención de la seguridad pública o privada. Como resultado, el nuevo término CSIRT se estableció al final de los años 90 En este momento, ambos términos (CERT y CSIRT) se utilizan de manera sinónima, siendo CSIRT el término más preciso.

En cuanto a la Infraestructura critica son definidas como aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de los gobiernos de los Estados miembros.[216]

En este punto de la investigación, aunque en las infraestructuras criticas abarcan una serie de instalaciones físicas vitales para la nación, no cabe duda que la mayoría de estas, se encuentran interconectadas por redes y sistemas informáticos que permiten su monitoreo y control a distancia, lo que a su vez las expone de las amenazas de individuos, grupos terroristas y cibercriminales, empresas y estados interesados.

Por último, la gestión de riesgos se basa de acuerdo a la norma ISO 27001 en Actividades coordinadas para dirigir y controlar una organización, con respecto al riesgo. En este sentido se favorece la identificación de las amenazas, la probabilidad de sus ocurrencias y por último la decisión administrativa de cómo y dónde invertir los recursos para la seguridad, en función a las vulnerabilidades y riesgos.

8.2 DEBILIDADES DE LOS SISTEMAS DE PROTECCIÓN Y PROBLEMAS PARA LA LUCHA CONTRA EL CIBERDELITO

Tras el análisis de los ataques más reseñables que ha sufrido España, las medidas de protección de los sistemas españoles presentaban las siguientes debilidades:

- Falta de concienciación y desconocimiento del riesgo por parte de la jefatura, esto unido a un sistema con vulnerabilidades, con escasa configuración de seguridad y seguridad reactiva, lo que hace que los sistemas de ciertas empresas y AAPP se conviertan en "objetivos fáciles", que pueden ser atacados por sujetos activos con herramientas sin demasiada capacitación técnica.

---

[216] CCN, Centro Criptológico Nacional. (2015). Guia de Seguridad (ccn-stic-401) Glosario y abreviaturas. Madrid: Editor y Centro Criptológico Nacional.

- Poco personal de seguridad y escasa vigilancia de tráfico de red, de la actividad de usuarios externos, del empleo de recursos de red o de equipos críticos. Asimismo, se detecta una nula vigilancia del tráfico interno de la red.

- Ausencia de herramientas que faciliten la investigación de cualquier anomalía o incidente de seguridad.

- Mayor superficie vulnerable, ya que la mayoría de las organizaciones y empresas son muy permisivos con el uso de redes sociales, telefonía móvil y servicios en la "nube" a sus empleados, lo que facilita el ciberataque por diversas vías. Las políticas de seguridad de las diferentes empresas y organismos públicos no tratan el asunto de la implementación de las TIC's y su correcto empleo.

- Las organizaciones/empresas afectadas no comparten información y no comunican información técnica de incidentes que pueden afectar a otras organizaciones y/o empresas.

El primero de los problemas a los que se enfrenta los diferentes países para combatir el ciberespionaje, es la dificultad de identificar a los ACTORES de los ciberataques. El acceso, comunicación y acción a través de internet es barato, simple y efectivo. Y el alcance masivo de cualquier ciberdelito es otro problema principal. Un problema añadido, al del acceso masivo, es el ANONIMATO en internet, que es una ventaja significativa del sujeto activo para cometer tales crímenes.

Otro gran problema que se presenta al respecto en la lucha contra el ciberdelito es el continuo debate sobre cómo combatir el cibercrimen y el ciberespionaje, el cual actualmente tiene puesta ahora todas sus miras en el compromiso entre la seguridad y la privacidad. De hecho, la ENCRIPTACIÓN, proceso para volver ilegible información considera importante para que sólo pueda leerse aplicándole una clave, es una de las principales estrategias para evitar intrusiones no autorizadas en sistemas por parte de ciberdelincuentes, se enfrenta a la oposición de algunos gobiernos debido a sus programas de vigilancia.

Para la Protección del ciberespacio, Inicialmente, la ciberseguridad estaba enfocada a la protección de la información, donde únicamente se salvaguardaba la información a accesos, usos, revelaciones, interrupciones, modificaciones o destrucciones prohibidas[217].

Hoy en día, este enfoque está cambiando hacia la gestión de riesgos del ciberespacio, donde la ciberseguridad se basa en "la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basándose en los estándares internacionalmente aceptados"[218]. Por este motivo, la ciberseguridad debe expresarse como un proceso permanente de análisis y gestión de los riesgos vinculados al ciberespacio[219].

En este sentido, la ejecución de ciberataques, el robo de información, el ciberespionaje industrial, los ciberdelitos patrimoniales, la difusión de códigos maliciosos y la captación indebida de datos de carácter personal se constituyen como "enemigos" constantes en este "campo de batalla" llamado ciberespacio24. Dichas ciberamenazas, a pesar de perpetrarse con cierta regularidad, a veces ni siquiera son advertidas, ni tampoco son tratadas de manera adecuada.

Para poder hacer frente a dichas amenazas en el ámbito del ciberespacio, se requiere medir y gestionar los riesgos manifestados de forma objetiva y repetible. En este sentido, es fundamental contar con una estrategia de ciberseguridad apoyada en herramientas y metodologías que permitan realizar un análisis pormenorizado de cada uno de los riesgos. Por ello, es recomendable contar con catálogos de activos, amenazas y vulnerabilidades, capaces de adaptar las metodologías a las particularidades del ciberespacio.

---

[217] Martínez Atienza, G. (2016), "Seguridad y delitos tecnológicos", en Seguridad Pública y Privada., p. 200

[218] Instituto Nacional de Ciberseguridad, (2015) "Análisis y caracterización del mercado de la Ciberseguridad".

[219] Martínez Atienza, G. (2016), "Seguridad y delitos tecnológicos", en Seguridad Pública y Privada.p. 201

Asimismo, la estrategia de ciberseguridad debe responder a un proceso de mejora continua, a cuyo efecto conviene implementar:

En primer lugar, herramientas de monitorización que permitan medir la seguridad a través de indicadores alineados con los objetivos de la organización;

Y segundo lugar unos sistemas adecuados para descubrir y gestionar los incidentes, que permitan inspeccionar tanto las vulnerabilidades expuestas, como el procedimiento para manejar su respuesta.[220]

El gobierno británico "amenazó con 'prohibir la encriptación' porque "no debería haber 'medio de comunicación' que 'no podamos leer'". En este escenario, la ONU se ha manifestado en un informe para el Consejo de Derechos Humanos de 2015 a favor del uso de encriptación y anonimato en comunicaciones digitales, como modo de protección de los derechos y libertades del ciudadano. El Open Technology Institute de EE.UU. (OTI) esboza cuatro razones por las que el cifrado reforzado es positivo:

- La encriptación reforzada es buena para la seguridad de internet.

- La encriptación reforzada protege la privacidad individual.

- La encriptación reforzada supone un apoyo para la libertad de expresión.

- La encriptación reforzada promociona el crecimiento de la economía de la información.

Desde un punto de vista legal, el ciberespionaje y, en general cualquier tipo de ciberdelito "comporta cuestiones de procedimiento y jurisdicción", en un contexto en el que la aplicación de la ley no está adaptada a los crímenes por la novedad y el requerimiento de conocimientos avanzados del mismo. De hecho, muchos países no disponen de leyes que persigan los cibercrímenes.

---

[220] Écija Bernal, Á. (2014), "El Ciberespacio: una herramienta de poder", Editorial Aranzadi, Cizur Menor.

Para finalizar, desde un punto de vista económico, está claro que para el cibercriminal los beneficios superan los costes. Muchas fuentes explican cómo el cibercrimen crece debido a incentivos económicos dentro de la tecnología de la TIC's, la globalización de los mercados y una ley inadecuada. Un caso representativo es el de los estudiantes en Rusia y Europa oriental que son buenos en matemáticas e informática y no pueden encontrar trabajos fácilmente porque las economías de sus países son demasiado pequeñas para absorber el talento informático. Los grupos de crimen organizado pagan hasta 10 veces más que en los trabajos legítimos de TIC's a los mejores graduados.

8.3 ESQUEMA NACIONAL DE SEGURIDAD

España, a diferencia de otros países de nuestro entorno, no ha definido todavía una legislación específica y completa en materia de ciberseguridad. Sí existe legislación distribuida en distintos ámbitos ministeriales, pero que no ha sido desarrollada a partir de una política común que refleje el ámbito nacional y estratégico de la ciberseguridad.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, constituye un buen punto de partida, pero, como su propio nombre indica, cubre únicamente el sector de las administraciones públicas, dejando fuera los otros sectores relevantes para la gestión de la ciberseguridad: otras infraestructuras críticas, las empresas y los ciudadanos. Además del citado Real Decreto existen leyes nacionales, europeas e internacionales que abordan la cuestión de la ciberseguridad. Entre estas, se encuentran la Ley Orgánica de Protección de Datos, la Ley General de Telecomunicaciones y la Ley de la Sociedad de la Información y Comercio Electrónico.

A pesar de la existencia de este marco normativo, su grado de cumplimiento, en algunos casos, es preocupantemente bajo, lo cual supone un aumento del riesgo de nuestro ciberespacio. Las competencias relacionadas con la gestión de la ciberseguridad están repartidas entre un conjunto de organismos e instituciones, que dependen de diferentes ministerios del gobierno. Entre los más relevantes se encuentran:

- El Centro Criptológico Nacional (CCN), dependiente del CNI que tiene, entre sus misiones, la gestión de la seguridad del ciberespacio dependiente de cualquiera de los tres niveles de las administraciones públicas: estatal, autonómico y local. El CCN-CERT es el centro de alerta nacional que coopera con todas las administraciones públicas para responder rápidamente a los incidentes de seguridad en su parte del ciberespacio y, además, es el responsable último de la seguridad de la información nacional clasificada.

- El Instituto Nacional de Tecnologías de la Comunicación (INTECO), dependiente del Ministerio de Industria, Turismo y Comercio, es responsable de gestionar a través de su CERT la defensa del ciberespacio relacionado con las PYMES españolas y los ciudadanos en su ámbito doméstico.

- El Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC), dependiente del Ministerio del Interior procura la ciberseguridad relacionada con estas infraestructuras.

- El Grupo de Delitos Telemáticos de la Guardia Civil y la Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional, dependientes ambos del Ministerio del Interior son responsables de combatir la delincuencia que se produce en el ciberespacio.

- La Agencia Española de Protección de Datos (AEPD), dependiente del Ministerio de Justicia, responsable de hacer cumplir la normativa en materia de protección de datos personales.

Además, en la administración autonómica existen centros homólogos a los referidos a nivel estatal como el CSIRT-CV de la Comunidad Valenciana y las Agencias de Protección de Datos de la Comunidad de Madrid y de la Generalitat de Cataluña, que igualmente tienen responsabilidades en la gestión de la ciberseguridad en su ámbito autonómico. En resumen, si bien existen organismos con responsabilidades claras en distintos ámbitos de las administraciones públicas, España no dispone de un órgano único, al más alto nivel, que asuma el valor estratégico que la ciberseguridad tiene para nuestro país y ejerza el liderazgo necesario para que todos esos organismos actúen según una única política nacional.

En cuanto a lo referido a la industria española relacionada con la ciberseguridad, está se encuentra en pleno proceso de crecimiento y maduración, tal y como refleja el último "Catálogo de empresas y soluciones de seguridad" del INTECO42, cifrando en más de 1.000 las empresas españolas que se dedican a la ciberseguridad. En 2009, las principales empresas del sector se agruparon en el Consejo Nacional Consultor sobre Ciber-Seguridad (CNCCS) con el objetivo de fomentar la defensa del ciberespacio, poniéndose a disposición de entidades gubernamentales o privadas para asesorar en materias de ciberseguridad, y potenciar la innovación tecnológica y el crecimiento económico consiguientes.

Las empresas reconocieron pronto el valor estratégico del ciberespacio, tanto del propio como del concebido globalmente, y así aparecieron los departamentos de seguridad en sus organizaciones y las agrupaciones como el CNCCS. Sin embargo, apenas existen iniciativas desde el lado de la administración pública que fomenten la colaboración entre el Estado y la industria. Una relación que debería ser bidireccional: las empresas necesitan crear valor alrededor del negocio de la ciberseguridad y el Estado precisa de tecnología que le permita disponer de una capacidad solvente y vanguardista de ciberseguridad.

Es importante destacar que España forma parte de organizaciones internacionales que promueven la defensa del ciberespacio. Destaca nuestra participación en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN y en organismos como European Network Information Security Agency (ENISA)44 el Antiphising Working Group (AWG)45 y el Art.29 Data Protection Working Party.46 Nuestra presencia y colaboración en organismos internacionales no sólo permiten compartir experiencias y conocimientos sobre los riesgos y las soluciones, sino que corroboran que ningún ciberespacio nacional podrá ser gestionado eficazmente si el resto de porciones del ciberespacio global no se encuentran en un nivel de riesgo similar. Uno de los principios no escritos de la seguridad de las TIC afirma que la cadena siempre se rompe por el eslabón más débil. De poco o nada le sirve a una nación implementar una ciberseguridad muy avanzada, si el resto o alguno de los países que intervienen en el ciberespacio no se encuentran en un nivel parecido.

8.4 LA ESTRATEGIA DE ESPAÑA

En el caso del Reino de España en el año 2013 se promulga su Estrategia de Ciberseguridad Nacional y queda definida como un modelo integral que persigue la vinculación, coordinación y uso de los actores y recursos del Estado, contando con la colaboración público-privada, así como con la ciudadanía como uno de sus principales activos.[221]

Al igual que la estrategia definida por otros países, hace una referencia importante a las características que ofrecen los ciber destacando de ella los siguientes aspectos:

•Bajo Costo: Llama la atención que la mayoría de los recursos y herramientas que utilizan los ciber atacantes, pueden obtenerse libremente en el mercado incluso de manera gratuita. Basta con señalar que en el momento de la publicación de esta estrategia los recursos y las capacidades, además de los desarrolladores dedicados a la fabricación de softwares, eran mínimos, mientras que en la actualidad se habla incluso de manejo de Big Data y de inteligencia artificial que puede provocar algún tipo de afectación o daño sin necesidad de ninguna manipulación por parte de los seres humanos.

•La ubicuidad y la fácil ejecución: Esto revela que los atacantes pueden estar en cualquier lugar del mundo y acceder a través de diferentes redes informáticas logrando interconectarse en breves segundos. El crecimiento de las tecnologías de comunicación y el uso de redes no alámbricas para la interconexión facilita diferentes vías para que un atacante pueda llevar a cabo sus actividades, sin ser descubierto rápidamente y en tiempo real, lo que facilita enormemente su anonimato y las posibles consecuencias de su ataque.

---

[221] Gobierno de España, Gabinete de la Presidencia-Departamento de Seguridad Nacional. (2014). Estrategia de Ciberseguridad Nacional. Obtenido de Departamento de Seguridad Nacional www.dsn.gob.es.

•Efectividad e impacto: La puesta en marcha de un ataque en el ciberespacio genera de seguro un intento efectivo para lograr sus objetivos, sin embargo se destaca que el hecho de que el mismo pueda ser identificado, generara algunos impactos negativos en términos de respuesta, aseguramiento, identificación de patrones y vulnerabilidades a la infraestructura existente y además en cuanto a la resiliencia.

•Bajo riesgo para el atacante: La versatilidad que exhiben los sistemas informáticos en la actualidad, le garantizan una baja exposición a los atacantes, ya que en algún caso el mismo puede estar a kilómetros de distancia del ataque generado, o bien pueden tratarse de acciones pre programadas para su ejecución en fechas determinadas que harán prácticamente imposible determinar dónde o cuando se originó la infestación.

Estas características comunes implican que los individuos aislados, grupos u organizaciones criminales o dependientes de naciones extranjeras, pueden fácilmente utilizar los recursos a la mano para provocar algunos daños en el Ciberespacio, atendiendo a las motivaciones de la baja exposición, acceso a redes cada vez más accesibles en el mercado, y los bajos niveles de exposición para ser detectados, frente a la posibilidad de agenciar beneficios económicos de manera directa o a través de competidores comerciales o de países que compitan en algún sector de los negocios internacionales.

Es por esta razón la visión española pretende general el consenso entre los sectores Público y Privados ya que ambos comparten responsabilidad en las infraestructuras críticas, y además, bajo el convencimiento de que el fracaso de una parte puede dar en gran medida el fracaso de todos.

De estas precisiones la propia Estrategia española establece como principios básicos:

a.- La existencia de un liderazgo nacional que permita coordinar todos los esfuerzos.

b.- Una Responsabilidad compartida entre todos los sectores públicos y privados.

c.- Proporcionalidad y racionalidad en el uso de los recursos dando lugar a e una acción responsable.

d.- Propiciar la Cooperación internacional dado el carácter transfronterizo de la ciberseguridad. Muchas de las medidas que deberán aplicarse solo serán efectivas si se aplican en diferentes países de manera simultánea o conjunta.

Para que pueda ser efectiva esta estrategia se requiere del cumplimiento de objetivos generales y específicos además de algunas consideraciones adicionales. Este objetivo general que se persigue es "Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques".[222]

De este objetivo general se desprende una visión española que asegura la creación de la legislación correspondiente que permita un uso adecuado de todos los agentes, instituciones y recursos para garantizar las capacidades preventivas, de Defensa, de investigación y el análisis de las amenazas e intrusiones, la detección, la recuperación, la respuesta y persecución de aquellos que como individuos o grupos atenten contra las estructuras cibernéticas individuales, de instituciones públicas o privadas, además de la debida protección a la industria y la economía nacional.

Otros objetivos específicos que se persiguen son garantizar que los sistemas gubernamentales así como los privados vinculados a las infraestructuras criticas posean los sistemas de información y telecomunicaciones, prevenir y contrarrestar el terrorismo y la delincuencia cibernética, llevar a cabo una extensa campaña de sensibilización a la población y a las empresas en términos de Ciberseguridad y entornos preventivos, elevar y mejorar el conocimiento en tecnologías de Información y telecomunicaciones procurando extender su participación internacional en ámbitos de cooperación.[223]

---

[222] Gobierno de España, Gabinete de la Presidencia-Departamento de Seguridad Nacional. (2014). Estrategia de Ciberseguridad Nacional. Obtenido de Departamento de Seguridad Nacional www.dsn.gob.es

[223]. Idem.

Para cada uno de estos objetivos específicos pretende seguir con una línea de acción que operativiza cuya finalidad es el cumplimiento de cada uno de estos objetivos.

Así que puede describirse una relación que vincula la política, con la estrategia, los principios, los objetivos con las líneas de acción en cada uno de estos, además de conjugar para todos los casos la participación individual, publica, privada e internacional. Esto constituye un referente para una mejor colaboración y coordinación con otros países en materia de ciberseguridad, ya que este modelo entra en consonancia con las estrategias de diferentes países del entorno europeo en materia de seguridad del ciberespacio.

La primera de las líneas de acción favorece la cooperación de los organismos con responsabilidades en ciberseguridad, en España contamos con el CERT y la Administración Pública del Centro Criptológico Nacional (CCN-CERT), el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas (MCCD) y el CERT de Seguridad e Industria. Se incluye además la cooperación de los CERT de las Comunidades Autónomas, los de las entidades privadas y otros servicios de ciberseguridad, permitiendo tomar las decisiones adecuadas a cada situación o momento y de naturaleza conjunta.

En esta iniciativa española, se crea el Mando Conjunto de Ciberdefensa (MCCD) como una estructura operativa, dependiente del Jefe de Estado Mayor de la Defensa (JEMAD), siendo este organismo el responsable del planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa.[224]

Entre sus actividades, el MCCD establece un protocolo para dar las respuestas adecuadas en el Ciberespacio a todas aquellas amenazas o ataques que puedan afectar la Defensa Nacional. De aquí surge el ESP DEF CERT siendo denominado como Centro de Respuesta ante Incidentes del Ministerio de Defensa. Su ámbito de actuación son las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y

[224] EMAD-Mando Conjunto de Ciberdefensa. (2019). Estado Mayor de la Defensa.

sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional.

Al igual que los demás Centro de respuestas ante incidentes informáticos, hay una prioridad en lo que respecta la realización de las siguientes acciones:

a.- Garantizar el libre acceso a todas las dependencias de las FFAA al ciberespacio.

b.- Garantizar la integridad, disponibilidad e integridad de la información, así como los servicios críticos que puedan ser afectados por accidentes, incidentes o ataques.

c.- Ejercer respuesta y seguimiento a los ciberataques, y dirigir los centros de respuesta de incidentes de los demás componentes (Ejercito y Armada) y el de Seguridad de Información del Ministerio de Defensa.

d.- Cooperar con los centros nacionales de respuesta a incidentes de seguridad de información.

e.- Dirigir el entrenamiento especializado en materia de ciberdefensa.

-CONCLUSIÓN-

IX CONCLUSIONES

Conclusión primera.

La investigación doctrinal que concluye con estas páginas ha consistido en el estudio y análisis de las nuevas amenazas híbrida desde el punto de vista de la ciberseguridad y los ataques de las organizaciones terroristas. Se ha analizado de forma pormenorizada la forma en que estas nuevas amenazas actúan en el campo físico y plano virtual para generar los efectos locales y globales que atentan a la seguridad nacional e internacional.

Los nuevos conflictos bélicos de este siglo, y concretamente las amenazas híbridas se ha constituido como un fenómeno muy complejo donde la simple definición está siendo de gran controversia y donde encontramos diversas interpretaciones doctrinales.

A pesar de ello si se puede comprobar que todos los enfoques coinciden en el fin que se persigue con estas amenazas, siendo este el aprovechamiento de las vulnerabilidades que presentan los sistemas a los que pretenden atacar y con ello debilitar al adversario. Para ellos utilizan diversas combinaciones de los llamados" instrumentos de poder". Por todo lo investigado puedo llegar a la conclusión que las amenazas híbridas son una nueva combinación entre la criminalidad organizada, o concomida como criminalidad común, con los actuales episodios de violencia política, siendo estos nuevos conflictos el objeto de estudio de esta tesis.

Conclusión segunda.

Si atendemos a la definición dada en el punto anterior se observa que existen múltiples amenazas híbrida en la actualidad, debiendo llevar a cabo una estructuración de las mismas para llegar al fin que se pretende en esta tesis. La existencia de un modelo tan dinámico de las mismas está construida en tres fases bien definidas.

La primera de ellas hace referencia a las relaciones de intercambio y reciprocas entre las organizaciones políticas y criminales. En una segunda fase, estas relaciones avanzan a un segundo estado de convergencia donde ambas partes utilizan una técnica de imitación, avanzando finalmente a un estado de mutación de las entidades, donde se produce una fusión de las entidades que al mismo tiempo son políticas y criminales, estado en el cual tanto los estados como los criminales tienden a defenderse y a justificarse mutuamente. Uno de los ejemplos que encontramos en esta tesis se describe en el capítulo cuarto donde el terrorismo yihadista, principalmente en los enclaves terrorista, "no go Zone", los integrantes pasan de ser simples criminales del derecho común a convertirse en actores de un panorama no únicamente criminal sino también geopolítico y de gran relevancia.

En la última de estas tres fases, nos encontramos en un momento donde ya no se puede distinguir que parte de la estructura son criminales y que parte de ella son políticas, confundiendo modelos operacionales y donde las justificaciones de las actividades tienen como única finalidad la depredación.

Conclusión tercera.

Las vigentes aproximaciones doctrinales llegan a la conclusión de la existencia de un componente exterior en todas las amenazas híbridas y que constituye el verdadero motor de estas; bien sea porque los autores del conflicto achacan al enemigo el diseño o ejecución de tal amenaza como una forma de atacar sus respectivos intereses geoestratégicos. Sin embargo, una amenaza híbrida puede tener un origen interno, sin necesidad, al menos inicialmente, de poderosos apoyos exteriores.

Esta amenaza de origen interno es profundamente adaptativa y tiene como misión explotar las debilidades del bando contrario en los entornos desde un punto de vista social y de la información, del ámbito diplomático y político, y no renuncia a utilizar y sincronizar dichas acciones con otras propias de los entornos económico o de seguridad si fuera necesario, dejando el terreno "investigativo" listo para el análisis de otra serie de conflictos que diversos autores.

Conclusión cuarta.

Otro de los objetivos de la investigación está basado en el efecto que produce el uso de las TIC´s en los conflictos del siglo XXI principalmente por la Yihadismo islámico.

Si se llevamos a cabo un estudio de los textos publicados por las bandas terroristas evidencian la existencia de procesos destinados a la captación y radicalización que son inteligentes y adaptivos. Para la confección de estos, el personal encargado de la captación y reclutamiento escuchan y analizan las necesidades y vulnerabilidades de cada sujeto. Tras confeccionar un perfil del mismo, elaboran un mensaje con la suficiente fuerza para poder captar su atención e implantar en ellos la necesidad de entender el yihadismo como su nuevo modelo de vida donde vea cubierta las necesidades que no disfrutan en la actualidad.

Conclusión quinta.

Tras un análisis empírico de estos individuos, se observa que no existe un perfil potencial terrorista determinado y que el proceso de radicalización por el cual el individuo para a ser captado y adopta la determinación de unirse a grupo terroristas no tiene un periodo temporal determinado. Por lo tanto, aunque el proceso de captación se pueda dividir en una serie de etapas más o menos, identificables, este varia en intensidad y duración según la forma de influenciar y de actuar del agente reclutador y de la receptividad propia del individuo.

Tras un estudio más profundo de estos individuos, a través de las evidencias documentales existentes, podemos observar que en la mayoría de estos individuos muestran ciertas carencias afectivas personales, personales o vitales. La interacción virtual con estos individuos, así como le revisión bibliográfica referente a este tema, cconstatan que las bandas terroristas están haciendo un uso proactivo e intensivo de la web en los procesos de radicalización y reclutamiento de los individuos. Dentro del capítulo cuarto de esta tesis se lleva a cabo un análisis de las zonas donde una vez reclutados se concentran estos individuos en mayor medida, las conocidas como “No Go Zones”.

Conclusión sexta.

Otro de los puntos importantes de mi tesis y que es objetivo de la misma consiste en destaca la complejidad ya reseñada anteriormente de los procesos de reclutamiento donde es importante poner mucho énfasis en la creciente importancia que tiene en ellos las mujeres. Estas bandas terroristas son conscientes de la necesidad de incrementar su ejército para poder conseguir el fin que persigue potenciando el papel de la mujer como un verdadero y eficiente interlocutor que aumenta considerablemente el existo de la radicalización. Estas mujeres, a través del proceso de empatía, reclutan a otras jóvenes puesto resulta más eficiente cuando se interactúan dos personas del mismo sexo. En varios de los atentados llevados a cabo ha quedado demostrado el papel de la mujer que pasa de tener un rol pasivo a tener un papel activo en la expansión del yihadismo bélico como captadoras de nuevas integrantes en la organización terrorista.

Conclusión séptima.

EL siguiente de los objetivos planteados viene definido por el ciberespacio como nueva forma de amenaza existente, configurado como una nueva dimensión virtual en los nuevos conflictos del siglo XXI.

En el capítulo siete de mi trabajo doctoral se lleva a cabo el análisis y estudio de la relación de los grupos terroristas con el uso del ciberespacio, lo que se conoce por la mayoría de los expertos como "Ciberespacio y Terrorismo: Yihadismo 2.0".

Las investigaciones llevadas a cabo durante los años de estudio de mi tesis he observado una gran mutabilidad del ciberespacio que ha permitido que tanto la delincuencia común como los grupos terroristas han trasladado gran parte de sus operaciones a las nuevas TIC´s haciendo un gran uso de internet debido a las características intrínsecas que posee el mundo del ciberespacio. Entre las características más importantes, destacare la instantaneidad, el anonimato y la fácil accesibilidad al mundo del ciberespacio, lo que conlleva una enorme dificultad para defenderse o prevenir este tipo de amenaza híbrida. La guerra de la información queda definida como las acciones tomadas por las fuerzas para mantener la integridad del trabajo de los sistemas de información, redes de comando, control, y prevenir la explotación o destrucción por parte del enemigo,

tomando todas las medidas que pueden ser explotadas o destruidas y que se usan para proporcionar información a las fuerzas con el fin de lograr la victoria.

Conclusión octava.

El resultado obtenido en mi trabajo doctoral en relación con las mafias y las bandas terroristas demuestran que los integrantes de estas hacen uso del ciberespacio como un nuevo campo donde diversificar sus acciones bélicas, y en el caso de las bandas terroristas, para llamar la atención de los ataques terroristas y para ampliar sus canales de captación. El papel de los medios de comunicación y las TIC´s ha quedado demostrado a la hora de la captación utilizada por parte de las organizaciones terroristas. Para conseguir estos resultados las personas que encabezan esos movimientos hacen uso de la propaganda como medio para conquistar las voluntades de las personas utilizando dos características del lenguaje como son la persuasión y la manipulación necesarias para producir un cambio en las creencias y en la ideología de los individuos. También hemos podido comprobar que la información compartida no es al azar, sino que, antes de que llegue a internet ha pasado por uno o varios programas de tratamiento de imagen para hacerla más atractivos.

Con el nuevo mundo del ciberespacio se pone de relieve que el uso de este facilita todas las operaciones y se amplía en eco mediático aumentando el impacto psicológico y sembrando en el individuo de a pie la sensación de inseguridad, tanto de ser atacado como de hacer el uso de las mismas. La aparición de internet y la utilización del este canal de comunicación como nuevo instrumento de ataque permite al atacante ser más dañino a la par que más resiliente ya que necesita de muchos menos recursos para conseguir sus objetivos.

Como conclusión de este punto nos lleva a pensar que la red es interpretada por estos grupos como un medio de permite facilitar la consecución de sus objetivos a menor coste y con mayor anonimato.

Conclusión novena.

En el capítulo siete y ocho de este trabajo doctoral se analiza la situación actual de varios países en materia de ciberseguridad y cómo afrontan las amenazas híbridas. Según el estudio llevado a cabo podemos afirmar que resulta necesario continuar trabajando en materia de seguridad en el ciberespacio e

investigando en diferentes campos como la cooperación internacional en materia de inteligencia, coordinación de todas las Fuerzas y Cuerpos de Seguridad y de los ejércitos de cada país. En ciberseguridad es esencial la prevención y la identificación de posibles irregularidades y brechas de seguridad antes de que se produzcan de manera efectiva, por el ahorro económico y de esfuerzo humano que supone.

Podemos comprobar la imperiosa necesidad de incrementar la cooperación estatal internacional y un intercambio rápido y eficaz de toda la información que se tenga conocimiento de este tipo de amenazas híbridas. Muchos de los países han creado organismo con una de las funciones principales es la coordinación en materia de ciberseguridad, pero es cierto que en la actualidad está muy lejos de conseguir la eficiencia necesaria. Uno de los ejemplos lo encontramos si analizamos los últimos atentados terroristas en Europa, donde los componentes de la cedulas terroristas de estos ataques han transitado sin problema alguno por diferentes países de la unión europea a pesar de estar perseguidos por la fuerzas y cuerpos de seguridad de los Estados. Con estos hechos queda demostrado que el intercambio de información entre los estados no está siendo todo lo efectivo que se necesita para evitar estos ataques.

Conclusión decima.

En el contexto actual es necesaria una importante labor de autocrítica que llegue a la conclusión por parte de los estados que las nuevas amenazas híbridas globales no pueden combatirse de una forma eficaz si siguen existiendo trabas en el intercambio de la información. Todo elemento o circunstancia que impida el flujo constante entre los servicios destinados al intercambio de información se transforma en un factor que favorece considerablemente este tipo de amenazas híbridas.

A pesar de lo reseñados, la experiencia nos ha demostrado la importancia de esta cooperación como sucedió en el caso de la cooperación bilateral entre España y Marruecos. Por lo tanto, debemos concluir con la certeza de que cuando existe una cooperación eficiente en materia de información, la lucha contra este tipo de amenazas es muy efectiva. Los Estados deben salir de su individualidad y abandonar el sistema de ámbito nacional para crear y diseñar una respuesta

común y coordinada que puede hacer frente a cualquier tipo de amenaza de manera eficiente y eficaz.

Para ello debemos mejorar el control del ciberespacio como nuevo campo de acción donde este tipo de amenazas se hace más fuerte y por tanto más peligrosa. Con este nuevo medio consiguen expandirse y operar con mayor facilidad aumentando y acelerando, en el caso de la amenaza terrorista, la captación de un mayor número de individuos. Los resultados de la investigación llegan a la concusión que el control del ciberespacio debe ser más férreo, siendo esto posible si se potencia la implicación ciudadana y se lleva a cabo una cultura en materia de ciberseguridad.

Conclusión undécima.

Otro de los aspectos a tener en cuenta para mejorar la respuesta ante este tipo de amenazas es la formación del personal encargada de la seguridad de cada Estado y una mejora en las dotaciones y los medios materiales necesario para llegar a alcanzar el fin que se persigue. Del estudio llevado a cabo en esta tesis deducimos que si de verdad queremos hacer frente a este tipo de amenazas debemos comprender al Estado como un engranaje en el cual todas las piezas que actúan en la defensa del mismo deben estar en perfecto estado y muy bien coordinadas. Si encontramos deficiencias en los mecanismos de defensa pasamos a ser muy vulnerables frente a este tipo de ataques.

Conclusión duodécima.

De lo investigado en el capítulo 8 podemos llegar a la conclusión que el Proyecto CERT destaca de manera contundente el hecho de querer mejorar la cooperación en inteligencia entre Estados Miembro de la Unión Europea y resto del mundo para proteger las infraestructuras críticas, haciendo uso de ciberinteligencia. Es decir, mediante la ciberinteligencia se mejoraría la cooperación e intercambio de inteligencia. Debido al carácter internacional del ciberterrorismo y de las APTs, este proyecto aplicado a estos ámbitos sería de gran utilidad.

A través de la investigación se ha podido concretar que la ciberinteligencia puede dar apoyo en la prevención del ciberterrorismo de manera proactiva. En el

caso concreto de España y la Unión Europea y a nivel de Seguridad Nacional, la ciberinteligencia es considerada frente al ciberterrorismo. En el instante en que se publica la presente investigación, no hay una concepción unánime de Seguridad Nacional ni de ciberterrorismo, varios Estados u organizaciones exponen definiciones a su entender. Existen claras discrepancias en acordar y acotar qué es el ciberterrorismo, si ataques a infraestructuras críticas o también el uso de Internet como medio de propagando y/o reclutamiento.

-REFERENCIAS BIBLIOGRÁFICAS. -

X REFERENCIAS BIBLIOGRAFICAS.

10.1. FUENTES BIBLIOGRÁFICAS

Abdel Hamid, Mohamed (2012): Guerra sin lucha, Dar Anglo publicación y distribución, El Cairo, P.22.

Abu-Warda, N. (1999) 'Las Relaciones Internacionales en la concepción islámica'. Estudios Internacionales de la Complutense.

Alonso, R. (2015) 'El Terrorismo Yihadista: una amenaza hibrida'. Cuadernos de Pensamiento Político. Fundación FAES [en línea] (45), 61-80.

Alonso, R. (2009) 'Procesos de radicalización y reclutamiento en las redes de terrorismo yihadista'. en La inteligencia, factor clave frente al terrorismo internacional. ed. por Instituto Español de Estudios Estratégicos & Centro Nacional de Inteligencia. España: Ministerio de Defensa, 21-68

Al-Uyayri, Y. (2000-2003) The role of the women in fighting the enemies.

Antonio Diaz Fernandez, Maria Teresa Cabre, Marcelino Elosa, Josefa Gomez Enterria. (2013). Diccionario LID de Inteligencia y Seguridad. Madrid: LID Editorial Empresarial.

Aubrey, S. (2004) The new dimension of international terrorism. Zúrich: Vdf Hochschulverlag AG

Avilés, J. (2017) Historia del terrorismo yihadista: de Al Qaeda al Daesh. Madrid: Editorial Síntesis.

Balañá, J. (2011) 'El uso de las nuevas tecnologías por parte de los grupos terroristas islámicos (yihadistas), en relación a: propaganda y entrenamiento'. en La seguridad y la defensa en el actual marco socio-económico: nuevas estrategias frente a nuevas amenazas. ed. por Instituto Universitario General Gutiérrez Mellado de Investigación sobre la Paz, la Seguridad y la Defensa. Madrid: IUGM, 649-676

Bauman, Z. (2006) Miedo Líquido. La sociedad contemporánea y sus temores. Barcelona: Editorial Paidós Ibérica, S.A.

Banasik, M. (2015). How to Understand the Hybrid War. Sicuritologia, pp. 2829

Ben Jelloun, T. (2002) El Islam explicado a nuestros hijos. Barcelona: RBA Libros Ben Jelloun, T. (2015) El Islam que da miedo. Madrid: Alianza Editorial

Berner, B. (2008) Yihad. Habla Bin Laden. Declaraciones, entrevistas y discursos. Madrid: Editorial Popular, S.A.

Brumiller, E. (2011) 'Panetta Warns of Dire Threat of Cyberattack on U.S.' The New York Times.

Burgat, F. (2006) El Islamismo en tiempos de al-Qaida. Barcelona: Ediciones Bellaterra.

Caballero velasco, m.á., (2015) "Ciberdelincuentes: la gran amenaza", Gerencia de Riesgos y Seguros, núm. 122, p. 66.

Cabanelas, L. y Calero, F. (2017) «Las canteras europeas de la yihad». ABC Internacional. Consultado en: https://www.abc.es/internacional/abci-canteras-europeas-yihad- 201511291847_noticia.html.

Calduch, R. (1988) Métodos y técnicas de investigación internacional. Madrid: Universidad Complutense de Madrid

Calduch, R. (1991) Relaciones Internacionales. Madrid: Ediciones Ciencias Sociales

Calvo albero, J.L. (2009) La Evolución de las Insurgencias y el concepto de Guerra Híbrida. Revista Ejército , vol. 822, p. 6-13.

Calvo, S. (2013) 'De la web 1.0 a internet invisible vulnerabilidades, amenazas y delitos'. en Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.

Caro, M.J. (2010), 'Alcance y ámbito de la seguridad nacional en el ciberespacio'. en La seguridad un concepto amplio y dinámico. V Jornadas de Estudios de Seguridad. ed. por Instituto Universitario General Gutiérrez Mellado de Investigación sobre la Paz, la Seguridad y la Defensa. Madrid: IUGM, 47-82

Castells, M. (2009) Comunicación y poder. Madrid: Alianza Editorial

Carlini, A. (2018) 'Las redes sociales como factor de desestabilización'. Instituto Español de Estudios

Clarke, R. & Knake, R. (2011) Guerra en la red. Los nuevos campos de batalla. Madrid: Editorial Ariel

Cockburn, P. (2015) ISIS El retorno de la Yihad. Barcelona: Editorial Planeta

Cohen-Almagor, R. (2017) 'Jihad Online: How Do Terrorists Use the Internet?' en Media and Metamedia Management. ed. por VV.AA. Suiza: Springer International Publishing, 55- 66

Cortés, J. (ed.) (2005) El Corán. Barcelona: Herder Editorial

Center., N. C. (2019). National Ciber Security Center.

Chehadé (2015), Fadi Chehadé at the Senate Commerce Committee, pag. 38

Conway, M. (2006) 'Terrorism and the Internet: ¿New Media-New Threat?' Parliamentary Affairs

Conway, M. (2011) 'Privacy and Security against cyberterrorism. Why cyber-based terrorist attacks are unlikely to occur'. Communications of the ACM [en línea] 54 (2) 26-28.

Cullen, P. y Reichborn-Kjennerud, E. (2017). Understanding Hybrid Warfare. Pag. 3.

Cusumano, E. y Corbe, M. (eds.) (2018). A Civil-Military Response to Hybrid Threats. Palgrave Macmillan

DeLong-Bas, N. (2004) Wahhabi Islam. From Revival and Reform to Global Jihad. Londres: Oxford University Press - I.B. Tauris

De la Corte, L. & Jordán, J. (2007) La Yihad terrorista. Madrid: Editorial Síntesis

De la Corte, L. (2006) La lógica del terrorismo. Madrid: Editorial Alianza Editorial, S.A. Debord, G. (2003) La sociedad del espectáculo. Valencia: Pre-Textos

De la Corte, Luis. (2015), « ¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla», Revista de Estudios en Seguridad Internacional, Vol. 1, No. 2 pp. 1-34.

De la Corte, Luis. (2018). «La yihad de Europa. Desarrollo e impacto del terrorismo yihadista en los países de la Unión Europea». Informe del Centro Memorial de las Víctimas del Terrorismo. Nº4.Pp. 1-76

De Vega, Luis. (2015) «La convivencia agoniza en el barrio ceutí del Príncipe». ABC España.

Dershowitz, A. (2004) ¿Por qué aumenta el terrorismo? Para comprender la amenaza y responder al desafío. Madrid: Ediciones Encuentro

Devji, F. (2007) Paisajes del Yihad. Militancia, moralidad, modernidad. Barcelona: Ediciones Bellaterra

Díaz, C.M. (2006) 'El marco jurídico-internacional de la lucha contra el terrorismo'. en Lucha contra el terrorismo y Derecho Internacional. ed. por Instituto Español de Estudios Estratégicos. Madrid: Ministerio de Defensa, 51-77Dogrul, M., Aslan, A. & Celik, E. (2011) 'Developing an International Cooperation on Cyber Defense and Deterrance against Cyber Terrorism'. International Conference on Cyber Conflict. Tallinn, Estonia 2011 [en línea] 2 de julio

Dogrul, M., Aslan, A. & Celik, E. (2011) 'Developing an International Cooperation on Cyber Defense and Deterrance against Cyber Terrorism'. International Conference on Cyber Conflict. Tallinn, Estonia 2011 2 de julio

Droogan, J., & Peattie, S. (2017). Mapping the thematic landscape of Dabiq magazine. Australian Journal of International Affairs, 71(6), 591-620.

Duva, J. (2014) 'El 95% de los ciberdelitos cometidos quedan impunes'. El País.

Echevarría, A. (2005): Cuarta generación de la guerra y otras leyendas, pag 34

Écija bernal, Á., (2014) "El Ciberespacio: una herramienta de poder", Editorial Aranzadi, Cizur Menor.

Écija bernal, Á., (2017) "Principales conductas antisociales de Internet. Análisis y propuestas de solución (I)", Diario La Ley, núm. 8956.

Elzbieta Bienkowska, (2016) Comisaria de Mercado Interior, Industria, emprendimiento y Pymes.

El-Rouayheb, K. (2010) 'From Ibn Hajar al-Haytami (d.1566) to Khayr al-Din al-Alusi (d.1899): Changing Views of Ibn Taymiyya among non-Hanbali Sunni Scholars'. en Ibn Taymiyya and his times. ed. por Rapoport, Y. & Ahmed, S. Pakistán: Oxford University Press, 269-318

EMAD-Mando Conjunto de Ciberdefensa. (2019). Estado Mayor de la Defensa.

Etsivaria, Antonio (2008): Las guerras asimétricas son guerras desiguales, P. 61.

Federica Moggherini, (2016). Alta Representante de la Unión Europea en asuntos Exteriores y Política de Seguridad

Faksh, M. (1997) The Future of Islam in the Middle East: Fundamentalism in Egypt, Algeria and Saudi Arabia. Estados Unidos: Praeger Publishers

Ganuza, N. (2010) 'La situación de ciberseguridad en el ámbito internacional y en la OTAN'. en Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. ed. por Ministerio de Defensa. Madrid: Ministerio de Defensa, 165-214

García Yuste, Tamara. (2017) «Si es usted cristiano no ponga los pies en estos cinco barrios europeos controlados por islamistas».

Garriga, D. (2015) Yihad ¿Qué es? Barcelona: Editorial Comanegra.

Gazapo, M. (2017) 'Ciberespacio: el nuevo campo de actuación del crimen organizado en América Latina'. El crimen organizado en América Latina: manifestaciones, facilitadores y reacciones. ed. por Sampó, C. & Troncoso, V. Madrid: Instituto Universitario General Gutiérrez Mellado, 335-361

Gazapo, M. (2017) 'Daesh o el secuestro y deformación de una religión. Islam y terrorismo: conceptos (des)vinculados'. Los estudios militares y de seguridad en los albores del siglo XXI. ed. por Durán, M. & González, R. Granada: Universidad de Granada, 133-148

Gazapo, M. (2017) 'El Yihad y sus ideólogos: la tergiversación del concepto en el terrorismo contemporáneo'. en Análisis de la seguridad internacional desde perspectivas académicas. ed. por Payá, C. Navarra: Editorial Thomson Reuters Aranzadi, 577-609.

Gazapo, M. (2017) 'Terrorismo e inteligencia: capacidades, fallos y posibilidades'. en Inteligencia aplicada a la seguridad del siglo XXI. ed. por Payá, C. España: ePraxis - Wolters Kluwer, 93-103

Gazapo, M. (2018) 'Internet como catalizador del terror: el uso del ciberespacio por parte de organizaciones terroristas'. en Conflictos y diplomacia, desarrollo y paz, globalización y medio ambiente. ed. por Giner, G. & Delgado, J. Navarra: Editorial Thomson Reuters Aranzadi, 371-388

Gazapo, M. (2018) 'La inteligencia como instrumento clave en la lucha contra el terrorismo'. en La inteligencia y su actual relación con la seguridad. ed. por Payá, C. & Sillari, G. Madrid: Wolters Kluwer, 57-83

Giles, K. (2015). "Conclusion: Is Hybrid Warfare Really New?" En Lasconjarias, G. y Larsen, J. (eds.) (2015). Nato's Response to Hybrid Threats. NATO Defense College Forum Paper, 24, p. 337.

Goldzhier, I. (1981) An introduction to Islamic Theology and Law. New Jersey: Princeton University Press

Graham, E. (2015) 'Could Isis's 'cyber caliphate' unleash a deadly attack on key targets?

Guidère, M & Morgan, N. (2007) Manual de Reclutamiento de Al-Qaeda. Barcelona: Editorial Base

Hafez, M. (2007) Suicide Bombers in Iraq: The Strategy and Ideology of Martyrdom.

Hesham, Halaby (2017): Estrategia militar de cuarta generación de guerras, Dar Bairut publicación y distribución, Lebanon, P. 43

Hidalgo, Carlos. (2007) «Los sindicatos policiales exigen que se atajen los brotes radicales en la Cañada Real».

Hoffman, F. (2007). Conflict in the 21st Century: The Rise of Hybrid War. Arlington: Potomac Institute for Policy Studies.

Hoffman, F. (2009). Further Thoughts on Hybrid Threats. Small Wars Journal.

Hoffman, Frank G, 2010, «"Hybrid threats": Neither Omnipotent Nor Unbeatable,volumen 4 p 441-445.

Iriarte, D. (2015) 'Califatobook`, la red social de los seguidores del Estado Islámico'. ABC [en línea] 16 de marzo. IT Digital Security, 2017

Jacobs A., Lasconjarias G. (2015). NATO's Hybrid Flanks: Handling Unconventional Warfare in the South and East. NDC Rome Research Paper, 112.

Juergensmeyer, M. (2003) Terror in the Mind of God. The Global Rise of Religious Violence. California: University of California Press

Kahwagi, R. (2016): "Guerra híbrida: la evolución de las tácticas guerrilleras y la guerra revolucionaria en la era de la digitalis".

Kamal,Salah (2009): Objetivos de guerra de cuarta generación Dar Algazaer publicación y distribución Algeria, P. 23

Kepel, G. (2016) El terror entre nosotros. Una historia de la yihad en Francia. Barcelona: Ediciones Península

Küng, H. (1999) En busca de nuestras huellas. La dimensión espiritual de las religiones del mundo. Barcelona: Círculo de Lectores S.A.

Küng, H. (2001) El Judaísmo. Pasado, presente, futuro. Madrid: Editorial Trotta

Küng, H. (2004) El Islam. Historia, presente, futuro. Madrid: Editorial Trotta

Küng, H. (2006) Proyecto de una ética mundial. Madrid: Editorial Trotta

Laqueur, W. (2003) La guerra sin fin. El terrorismo en el siglo XXI. Barcelona: Editorial Destino S.A.

Lanz raggio, M., y López alfranca, Mª. d. V.,(2015) "Ciberespionaje y derecho internacional", Retos del derecho ante las nuevas amenazas / coord. por María Susana de Tomás Morales, p. 145.

Lesaca, J. (2017) Armas de seducción masiva. La factoría audiovisual de Estado Islámico para fascinar a la generación millenial. Barcelona: Editorial Península

Liang Q. y W. Xiangsui (1999): Guerra sin restricciones: plan maestro de China para destruir América, pag 4

Liang, C. S. (2015). Cyber Jihad: understanding and countering Islamic State propaganda. GSCP Policy Paper, (2), 4.by TAPSTRI Media. (March 1, 2015).

Liang, Q. y Xiangsui, W. (1999). Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House.

Liang, Qiado and Xiangsui, Wang (1999): University Warfare, Beijing, PLA Literature and Arts Publishing House.

López, Esteban. (2017) «La quinta columna actúa en Cataluña». Defensa.com. Consultado en: https://www.defensa.com/en-abierto/quinta-columna-actua-cataluna.

López, J. (2012) 'La evolución del conflicto hacia un nuevo escenario'. en El ciberespacio. Nuevo escenario de confrontación. ed. por Ministerio de Defensa. Madrid: Ministerio de Defensa, 117-166

Luis De la Corte, (2015), "¿Enclaves yihadistas? Un estudio sobre la presencia y el riesgo extremistas en Ceuta y Melilla", Revista de Estudios en Seguridad Internacional, Vol. 1, No. 2 ,pp. 1-34.

Mahmud, Atia (2017): Las guerras de cuarta generación, Dar El hoda publicación y distribución, Cairo, P. 32.

Marín avella, v., (2015), "Delitos informáticos", Colegio Nuestra Señora de la Presentación-Centro, p. 18.

Martín, E., Bordas, J. & Yitzhak, E. (2015) Objetivo: Califato Universal. Claves para comprender el yihadismo. Barcelona: La Vanguardia Ediciones

Martín, E. (2015) 'El Estado Islámico capta terroristas en dos meses'

Martín, M. Á. B. (2017). La estrategia del DAESH a través de su revista Dabiq. bie3: Boletín IEEE, (7), 338-353.

Martínez atienza, G., (2016) "Seguridad y delitos tecnológicos", en Seguridad Pública y Privada, p. 200.

Masuda, Y. (1981) The Information Society as Post-industrial Society. Washington: World Future Society

Mattis, J. (2008). USJFCOM Commander's Guidance for Effectsbased Operations. Parameters, pp. 18-25

McConnell, M. (2010) 'How to win the cyber-war we're losing'. The Washington Post [en línea] 28 de febrero.

Metz, S. y D. Johnson. II (2014): Asymmetry and U.S. Military Strategy: Definition, background and strategic concepts, Instituto de Estudios Estratégicos del ejército de EE. UU.

Miró llinares, F., (2012) "El cibercrimen", Marcial Pons, p. 25

Miró llinares, F., (2012) "La criminalidad en el ciberespacio: la cibercriminalidad", Marcial Pons,p. 37. Este campo es unejemplo de la utilización en el ámbito científico de negoologismos derivados de la traducción al castellano de conceptos de otras palabras.

Miró llinares, F (2012) "Tipos de cibercrimen y clasificación de los mismos", en El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio, 2012, pp. 50-51.

Miró, F. (2012) El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid

Moghadam, A. (2008) The globalization of martyrdom. Al Qaeda, Salafi Jihad, and the Diffusion of Suicide Attacks. Baltimore: Johns Hopkins University Press

Morán, S. (2017) 'La ciberseguridad y el uso de las tecnologías de la información y la comunicación (tic) por el terrorismo'. Revista Española de Derecho Internacional, 195-222.

Moro, M. (2011) 'Posibilidades terroristas del empleo de armas NBQ-R'. en Las armas NBQ-R como armas de terror. ed. por Ministerio de Defensa. Madrid: Ministerio de Defensa, 23-82

Munaser, Said (2006): Las guerras y su concepto, el Colegio de líderes de Egipto, Cairo, P.121.

Münkler, H. (2005) Viejas y nuevas guerras. Asimetría y privatización de la violencia. Madrid.

Münkler, H. (2005) Viejas y nuevas guerras. Asimetría y privatización de la violencia. Madrid

Muñoz, P. (2015) 'Los ataques ciberterroristas aumentan y cada vez son más especializados'. ABC [en línea] 27 de enero

Murad, M. (1990) The Life & the Aqeedah of Muhammad Bin Abdul-Wahhab. Arabia Saudi: Printed as donation on behalf of His Royal Highness Price Abdulah Ibn Abdulaziz Al-Saud

Nance, M. (2016) Defeating ISIS: Who They Are, How They Fight, What They Believe. Nueva York: Skyhorse Publishing.

Pablo VI (1965) Declaración Nostra Aetate: Sobre las relaciones de la Iglesia con las religiones no cristianas. Concilio Vaticano II.

Puime maroto, J., "El ciberespionaje y la ciberseguridad", La violencia del siglo XXI. Nuevas dimensiones de la guerra, 2009, p. 48.

Qutb, S. (2007) Justicia social en el Islam. España: Editorial Almuzara Qutb, S. (2015) Milestones. Nueva Delhi: Islamic Book Service (P) Ltd.

Quincoces, A. (2015) 'Eugene Kaspersky: La amenaza ciberterrorista, al albur ya sólo de voluntades'.

Rafiq, H. & Malik, N. (2015) Caliphettes: Women and the Appeal of Islamic State [en línea] Londres: Quilliam Publications.

Ramadan, T. (2000) El reformismo musulmán. Desde sus orígenes hasta los Hermanos Musulmanes. Barcelona: Edicions Bellaterra

Ranstorp, M. (2004) 'Al Qaeda en el ciberespacio: desafíos del terrorismo en la era de la información'. en El nuevo terrorismo islamista. Del 11-S al 11-M. ed. por Reinares, F. y Elorza, A. Madrid: Editorial Temas de Hoy S.A., 201-221

Rapoport, D. (2004) 'Las cuatro oleadas del terror insurgente y el 11 de septiembre'. en El nuevo terrorismo islamista. Del 11-S al 11-M. ed. por Reinares, F. y Elorza, A. Madrid: Editorial Temas de Hoy S.A., 45-74

Rapoport, Y. & Ahmed, S. (2010) Ibn Taymiyya and his times. Pakistán: Oxford University Press

Rumman, A. & Hanieh, H. (2017) Infatuated with Martyrdom: Female Jihadism from Al- Qaeda to the Islamic State. Amman: Friedrich-Ebert-Stiftung Jordan & Iraq

Raska, M. (2015). Hybrid Warfare with Chinese characteristics. Singapur: Nayang Technological University.

Reichborn-Kjennerud, E. y Cullen, P. (2016). What is Hybrid Warfare? Norwegian Institute of International Affairs Policy Brief,.

Reinares, F. y Elorza, A. (2004). El nuevo terrorismo islamista del 11S al 11M. Temas de Hoy. Madrid.

Reinares, F. (2006) 'Dimensiones del terrorismo internacional'. en Lucha contra el terrorismo y Derecho Internacional. Cuadernos de Estrategia 133. ed. por Instituto Español de Estudios Estratégicos. Madrid: Ministerio de Defensa, 41-50

Reinares, Fernando y García-Calvo, Carola. «Actividad yihadista en España, 2013-2017: de la Operación Cesto en Ceuta a los atentados en Barcelona». 2017, Real Instituto el Cano, documento de trabajo 13/2017.

Rodríguez Blanco, Patricia y Díaz Matey, Gustavo.(2015) «La Unión Europea y el terrorismo islamista». UNISCI, No 39 , Pp. 1-14.

Roy, O. (2017) Jihad and Death. The Global Appeal of Islamic State. Londres: Hurst & Co.

Shakhtourra, R. (2014): "Guerra asimétrica: El arma más débil también puede ser utilizado por el poderoso", pp. 6-12.

Saleh, W. (2007) El ala radical del Islam. El Islam político: realidad y ficción. Madrid: Ediciones Siglo XXI

Singer, P. & Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Nueva York: Oxford University Press

Smith, R. (2008): La utilidad del poder y el arte de la guerra en el mundo contemporáneo, Casa Árabe de las Ciencias, Beirut

Smith, R.G.., grabosky, P., y Urbas, G., (2004) "Cyber criminals on trial", Cambridge, Cambridge University Press p. 5.

Taylor, P. (1997) Global Communications, International Affairs and the Media Since 1945. Nueva York: Routledge

Thomas Edward Lawrence, el famoso Lawrence de Arabia (1888 – 1935), pag. 44

Torres, M. (2009) El eco del terror: ideología y propaganda del terrorismo yihadista. Madrid: Plaza y Valdés

Torrecuadrada, S. (2013) 'Internet y el uso de la fuerza'. en Ciberseguridad global. Oportunidades y compromisos en el uso del ciberespacio. ed. por Universidad de Granada. Granada: Universidad de Granada, 91-118

Torres, M. (2009) 'Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda'. Real Instituto Elcano. [en línea] (ARI 110) 1-9.

Torres, M. (2009) El eco del terror: ideología y propaganda del terrorismo yihadista. Madrid: Plaza y Valdés

Treverton, G.; Thvedt, A.; Chen, A.; Lee, K. y McCue, M. (2018) pag 74. Addressing Hybrid Threats. Centro de Excelencia sobre Amenazas Híbridas y Swedish Defense University.

Sageman, M. (2017) Misunderstanding Terrorism. Philadelphia: University of Pennsylvania Press

Sánchez Moreno, G., (2013) "El ciberespionaje", Nueva Época, p. 115

Sánchez, Álvaro. «Molenbeek, año I: más radicales, más vigilados». El País, Internacional, 2017.

Schmidt, E. (2010) 'From the archives. Washington Ideas Forum. 1 de octubre de 2010 en el The

Schneier, B. (2015) 'NSA doesn´t need to spy on your calls to learn your secrets'. Wired, marzo de 2015.

UK-GOB. (22 de abril de 2019). Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. Reino Unido.

Von Clausewitz, K. (1980): De la guerra, traducido por Akram Deere y Haitham al Ayoubi, Fundación árabe para los estudios y la publicación, Beirut, 312 páginas.

Vacas, F. (2011) El terrorismo como crimen internacional. Definición, naturaleza y consecuencias jurídicas internacionales para las personas. Valencia: Editorial Tirant Lo Blanch

Wales Summit Declaration, Press Release, (2014), p. 13 – 104.

WALL, D., (2007) "Cybercrime: the transformation of crime in the information age", Cambridge, Polity Press, pp. 44 y ss

Warldan, G. (1986) Terrorismo Político. Teoría, táctica y contramedidas. Madrid: Colección Ediciones Ejército, Servicio de Publicaciones del E.M.E.

Warren, M. (2007) 'Terrorism and the internet'. en Cyber Warfare and Cyber Terrorism. ed. Por Janczewski, L. & Colarik, A. Nueva York: IGI Global - Information Science Reference, 42-49

Wignell, P., Tan, S., O'Halloran, K. L., & Lange, R. (2017). A mixed methods empirical examination of changes in emphasis and style in the extremist magazines Dabiq and Rumiyah. Perspectives on Terrorism, 11(2), 2-20.

Wolf, K. (2017) 'Cyber Jihadists Dabble in DDoS: Assessing the Threat'

YAR, M (2006), "Cybercrime and society", Sage, London, p. 9.

Yárnoz, C. (2015) 'Francia ha sufrido 19.000 ciberataques en cinco días'. El País 15 de enero.

Zaid Al-Marhoun, A. (2008): "La guerra desequilibrada del Cáucaso", Al Riyadh, La Fundación Al Yamamah, (14662), pp. 48-56.

Zerzri, M. (2017) 'The Threat of Cyber"

Žižek, S. (2015) Islam y modernidad. Reflexiones blasfemas. Barcelona: Herder Editorial

Zineb Hosny, Ezz El Din (2016): El impacto de las guerras de cuarta generación en la seguridad nacional árabe, El Centro Democrático Árabe, P.62 - 63.

Zuloaga, J.M. (2009) «Los Mossos desarticulan una célula yihadista en Barcelona con voluntad de atentar».

10.2. OTRAS FUENTES.

Físico y astrónomo estadounidense, experto en ordenadores y escritor. (1950) Stoll participo en la captura del hacker alemán Markus Hess durante los años 1986 y 1987, cuando trabajaba en el Lawrence Berkeley national Laboratory en California, sobre ello escribió en el libro "El huevo del cuco".

Veterano de la Armada de los EE.UU. (1968), rastreó un anillo de ciberespionaje chino que tenía el

Consultor tecnológico estadounidense, informante, antiguo empleado de la CIA y la NSA. (1983)

Agencia Europea de Seguridad (2016) Plan de acción para intensificar la lucha contra la financiación del terrorismo [en línea] Disponible en <http://eur- lex.europa.eu/resource.html?uri=cellar:e6e0de37-ca7c-11e5-a4b5- 01aa75ed71a1.0016.02/DOC_1&format=PDF> [3 de octubre de 2018]

Audiencia Nacional (2012) Diligencias Previas 26/2011-W. Juzgado Central de Instrucción Nº5, Madrid [en línea] Disponible en

<https://ep00.epimg.net/descargables/2012/03/30/d61bac3fc1fa90da6d87e2edd6e1fbe4.pdf

CIBER ELCANO del Real Insituto Elcano y la conferencia (2013) "Trojan Horse: The Widespread Use of International Cyber-Espionage as a Weapon RSA Conference 2013" de Mark Russinovich.

IV Congreso de CiberSociedade 2009, "Internet: Un espacio para el cibercrimen y el ciberterrorismo", 2009. Disponible en: http://www.cibersociedad.net/congres2009/gl/coms/internet-un-espacio-para-el-cibercrimen-y-el-ciberterrorismo/610/

Center., N. C. (2019). National Ciber Security Center.

CCN. Centro Criptológico Nacional, (2017) "Ciberamenazas y tendencias", CCN-CERT IA-16/17, 2017, p. 12.

CCN, Centro Criptológico Nacional. (2015). Guia de Seguridad (ccn-stic-401) Glosario y abreviaturas. Madrid: Editor y Centro Criptológico Nacional.

CESEDEN,(2012).Los Estados canallas "no sólo cuestionan o atacan abiertamente el orden internacional, sino que lo hacen apoyando y patrocinando a grupos armados irregulares (guerrillas, grupos terroristas, organizaciones criminales internacionales, etc.) que desencadenan o refuerzan los conflictos híbridos."

CESEDEN (2012), op.cit., pp. 26 y ss

CESEDEN-IEEE. (s.f.). (2011) Documento informativo del ieee 09/2011, nuevo concepto de ciberdefensa de la otan. Ministerio de Defensa España.

CESEDEN De 365 conflictos en el 2009.(2012), sólo 31 fueron guerras, mientras que los demás fueron solo crisis, como ataques terroristas, revueltas populares, golpes de Estado, etc.

Comisión de las Comunidades Europeas (2005) Terrorist recruitment: addressing the factors contributing to violent radicalisation

Consejo de la Unión Europea (2005) Estrategia de la Unión Europea de lucha contra el Terrorismo.

Consejo de la Unión Europea (2016) Declaración conjunta de los ministros de Justicia y Asuntos de Interior de la UE y los representantes de las instituciones de la UE con motivo de los atentados terroristas perpetrados en Bruselas el 22 de marzo de 2016.

Consejo Europeo (2004) Declaración sobre la lucha contra el terrorismo.

Directorate-General for External Policies of the Union (2013) The Involvement of Salafism/Wahhabism in the Support and Supply of Arms to Rebel Groups around the World.

Directorate-General for Internal Policies (2012) Europe´s crime-terror Nexus: links between terrorist and organised crime groups in the European Union.

Eurojust (2016) Brussels terrorist attack of March 2016.

Europol (2018) European Union Terrorism Situation and Trend Report 2018.

Elzbieta Bienkowska, (2016) Comisaria de Mercado Interior, Industria, emprendimiento y Pymes.

EMAD-Mando Conjunto de Ciberdefensa. (2019). Estado Mayor de la Defensa.

Gobierno de España (2013) Estrategia de Seguridad Nacional.

Gobierno de España, Gabinete de la Presidencia-Departamento de Seguridad Nacional. (2014). Estrategia de Ciberseguridad Nacional. Obtenido de Departamento de Seguridad Nacional www.dsn.gob.es.

Gobierno_Domincano. (2018). Estrategia Nacional de Ciberseguridad 2018-2021. Decreto 230-18 Estrategia Nacional de Ciberseguridad 2018-2021. Santo Domingo, Republcia Dominicana.

http://researchcenter.paloaltonetworks.com/2016/05/operation-ke3chang-resurfaces-with-new-tidepool- malware

http://theconversation.com/terroristas-en-la-red-el-modelo-de-comunicacion-digital-que-hace-temblar-las-democracias-116443

http://www.ieee.es/Galerias/fichero/docs_analisis/2018/DIEEEA21-2018_Al_Qaeda-Daesh_IFC.pdf

https://www.politicaexterior.com/articulos/afkar-ideas/foreign-fighters-europeos realidades-y-retos/

https://www.semana.com/mundo/articulo/estado-islamico-como-llego-ser-tan grande/450566-3

https://www.upf.edu/antenas/resultados/ndm/2016.03.neo_esp.html.

IEEE 09/2011(2011) titulado: Nuevo concepto de ciberdefensa de la OTAN.

Igor Koruchenko, experto militar y miembro del Consejo Social del Ministerio de defensa de Rusia, redactor jefe de la revista de defensa nacional de Rusia.

Incidente de Ransomware de Sony Pictures Entertainment.

INSTITUTO NACIONAL DE CIBERSEGURIDAD, (2015) "Análisis y caracterización del mercado de la Ciberseguridad".

NATO Cyber Defence Management Authority-CDMA

NATO (2015) keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar, Washington, DC. https://www.nato.int/cps/en/natohq/opinions_118435.htm?selectedLocale=n

NATO (2017) Secretary General statement. 20 October.

NATO Warsaw Summit Communiqué, op. cit. 13th Point. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO, (2016) Joint statement of the NATO-Ukraine Commission at the level of Heads of State and Government,9 july https://www.nato.int/cps/en/natohq/ofçficial_texts_133173.htm?selectedLocale=en

NATO, (1949): The North Atlantic Treaty, Article V. https://www.nato.int/cps/en/natohq/official_texts_17120.htm

NATO, Wales Summit Declaration, op. cit. 13th point. https://www.nato.int/cps/en/natohq/official_texts_112964.htm

Nota de prensa de la Comisión Europea de seguridad: La UE refuerza su respuesta a las amenazas Híbridas, en (Bruselas 6 de abril de 2016).

Nota de prensa de la Comisión Europea de seguridad: La UE refuerza su respuesta a las amenazas Híbridas, en (Bruselas 6 de abril de 2016).

Para un análisis exhaustivo de estas opiniones vea: CESEDEN. (2012). El Enfoque Multidisciplinar en los Conflictos Híbridos. Documentos de Seguridad y Defensa, 51. Ministerio de Defensa de España.

Presidencia del Gobierno. Estrategia de Seguridad Nacional. Departamento de Seguridad Nacional, 2017.

Resolución AG/RES. (2004) estrategia de seguridad cibernética.

Unión de Comunidades Islámicas de España. «Estudio demográfico de la población musulmana». Observatorio Andalusí, 2019. Págs. 1-18

Unión de Comunidades Islámicas de España. «Estudio demográfico de la población musulmana». Observatorio Andalusí, 2019. Págs. 1-18.