Artículo

*Jorge Gómez Sevilla*

# Ciberespacio y ciberterrorismo. Una aproximación a los nuevos campos de batalla inmateriales

## Cyberspace and Cyberterrorism: An Approach to the New Fields of Immaterial Battle

**Resumen**

Las profundas transformaciones en cuanto a las tecnologías de información y comunicación (TIC) acontecidas en el pasado siglo han provocado una verdadera revolución de los asuntos militares pues, a los tradicionales dominios a los que se destinaba el uso de la fuerza (tierra, mar y aire) se ha añadido el ciberespacio. Un nuevo dominio dotado de un carácter inmaterial que carece de una regulación legal propia, que permite actuar desde el absoluto anonimato produciendo grandes daños y dificultando una coherente respuesta. A ello, se añade que paralelamente con la democratización de las TICs y la masiva interconexión del siglo XXI, cualquiera, ya sea persona, estado u organización, puede hacer uso de ellas lo cual supone un nuevo reto tanto en materia de seguridad nacional como para la comunidad internacional en su conjunto, y genera nuevos fenómenos y amenazas como el ciberterrorismo. Será objetivo de este trabajo analizar este nuevo dominio, sus formas de uso y los actores que se servirán de ellas, centrándose especialmente en la viabilidad práctica del ciberterrorismo.

**Palabras clave:** TIC, Ciberespacio, Seguridad Nacional, Comunidad Internacional, Ciberterrorismo

**Abstract**

The profound transformations in terms of information and communication technologies (ICTs) that have taken place in the last century have provoked a true Revolution in Military Affairs, since cyberspace has been added to the traditional domains to which the use of force was intended (land, sea and air). A new domain endowed with an immaterial character that lacks its own legal regulation, which allows us to act from absolute anonymity, causing great damage and hindering a coherent response, to which it is added that, with the democratization of ICTs and the massive interconnection of the 21st century, anyone, whether person, State or organization, It can make use of them, which poses a new challenge for National Security and the international community as a whole, in addition to generating new phenomena such as cyberterrorism. The aim of this paper will be to analyse this new domain, its forms of use and the actors who will use them, focusing especially on the practical viability of cyberterrorism.

**Keywords:** ICT, Cyberspace, National Security, Internacional Community, Cyberterrorism

**Jorge Gómez Sevilla,** Grado de Derecho de la Universidad Complutense de Madrid, colaborador en medios de comunicación especializado en Seguridad Nacional y Defensa.

**Para citar este artículo:** Gómez Sevilla, J. (2024), Ciberespacio y ciberterrorismo. Una aproximación a los nuevos campos de batalla inmateriales, Revista Internacional de Estudios sobre Terrorismo, nº11, pp.51-60.

**Recibido** 02/04/2024

**Aceptado** 30/04/2024

## 1. Introducción

El ciberespacio es un término creado, definido y popularizado por William Gibson en su novela de ciencia ficción "Neuromante" del año 1984. En ella haciendo alusión a este término, describe una realidad virtual donde unos sujetos llamados "cowboys" proyectan su conciencia a través de una consola como una suerte de mercenarios que navegan a través de flujos de datos, eludiendo sistemas de seguridad, con el objetivo de robar información a grandes corporaciones. Paradójicamente, esta visión se acabó transformando en realidad, la pugna por el dominio de ciberespacio entre las antiguas y nuevas potencias es una nueva variable que se une a los intereses permanentes de los actores que participan en la esfera internacional.

En el ámbito de los estados, el ciberespacio ha constituido un nuevo medio para desarrollar nuevas estrategias, tanto ofensivas como defensivas, que se materializan principalmente en dos ámbitos.

Por un lado, las operaciones en el ámbito cognitivo, es decir, aquellas que afectan al ámbito inteligible inherente al ser humano, considerándolo de forma individual, socializada u organizada, y es consustancial a su capacidad de juicio y toma de decisiones. Estas tienen como objetivo aprovechar la coyuntura estructural social de la era tecnológica, caracterizada por el uso de metodologías analíticas irreflexivas basadas en prejuicios y premisas epistemológicas sencillas que junto a la sobreexposición de cantidades de información excesivas en su mayor parte en una plataforma electrónica provocan una saturación y desatención social que genera una percepción debilitada de la realidad, dando lugar a una mayor efectividad de las operaciones de corte psicológico o ingeniería social. Todo ello destinado a modificar la opinión pública, arremeter contra los pilares del sistema democrático y orientar la voluntad política hacia los intereses de otros, desfavoreciendo así en definitiva los propios (Instituto Español de Estudios Estratégicos, 2020).

Por otro lado, el desarrollo de las nuevas tecnologías ha tenido como consecuencia un proceso de restructuración estatal basado en sistemas automatizados de tratamiento de datos que han propiciado el paso de almacenamiento en soporte físico al soporte digital creando una nueva forma de gestión informatizada de los servicios básicos e infraestructuras críticas que, de forma indirecta, generan una nueva brecha en el aparato estatal de seguridad.

La centralización de servicios a través de su interconexión provoca una grave desventaja a ojos de la defensa. Esto se debe principalmente a que cualquier brazo del estado puede ser una puerta de acceso para la infiltración entidades maliciosas que provoquen una verdadera catástrofe. En este sentido, el Departamento de Seguridad Nacional del Gabinete de Presidencia del Gobierno español en su informe anual de seguridad nacional de año 2022 identifica la vulneraciones del ciberespacio como una de las principales amenazas para la seguridad nacional, habiendo detectado el Centro Criptológico Nacional (CCN) un total de 55.695 incidentes, el instituto nacional de Ciberseguridad (INCIBE) un total de 111.197 incidentes y el Ministerio de defensa un total de 2035 incidentes dándole de este modo, una intensidad de riesgo en una escala de 0-26 de 19,61. Una intensidad de riesgo con una tendencia a empeorar en un periodo de cinco años (Departamento de Seguridad Nacional, 2023). No es casualidad que esto ocurre en un periodo convulso en la dimensión internacional que, junto con la introducción de terceros actores no legítimos a ojos del Derecho Internacional Público, la

progresiva privatización de la guerra, y la nueva variable del ciberespacio, los estados aprovecharán para continuar con sus clásicas pugnas de una manera más eficiente y barata. Muestra de ello es la propia codificación de nuevos delitos redactados en base a un sustrato material específico pero que siguen teniendo al menos en España la forma de una subtificación bajo el paraguas de un tipo genérico (Departamento de Seguridad Nacional, 2023), mostrando que, en la actualidad, la única manera de luchar de forma efectiva contra estas amenazas procede de la esfera interna de los estados.

En este contexto, la incorporación de nuevos actores que eluden la categoría clásica de entidad soberana pero que, tienen en ocasiones más influencia que muchos de los actores tradicionales plantea un nuevo dilema para la seguridad nacional que ve en el panorama estratégico nuevos riesgos y, por tanto, nuevos retos para su buen y efectivo funcionamiento. La *pax americana* del mundo unipolar quiebra en sus cimientos y las escenas costumbristas pasan a nueva dimensión de oscuridad que poco o nada tiene que hacer ante el inexorable paso del avance tecnológico.

Será objetivo de este trabajo analizar estas nuevas dinámicas propias del siglo XXI centrándose en la utilización del ciberespacio como nuevo espacio de conflicto, e intentar establecer una categorización de estos nuevos actores que intervienen en él, teniendo especial importancia el ciberterrorismo como novedad teórica.

## 2. La zona gris; el paso previo hacia la guerra

La zona gris (GZ, por sus siglas en inglés)[1] es un concepto relativamente reciente en el mundo de los estudios estratégicos que hace referencia a una posible situación anterior a la guerra declarada. En otras palabras, se trata de un tipo de paz que se caracteriza principalmente por estar basada en la mala fe (Baques, 2021). Analizando desde una perspectiva realista la esfera de intereses que rige la dimensión internacional, no sorprende que la institución jurídica que lo gestiona de facto se torne cada vez más inservible, pues las grandes potencias han roto su compromiso para con el respeto al Derecho. La invasión de Ucrania, la quietud de la Corte Internacional de Justicia respecto de los plausibles crímenes lesa humanidad y de guerra cometidos en la actual guerra palestino-israelí, o la famosa intervención de Estados Unidos en Irak en el año 2003, son solo unos de los pocos síntomas que prevén una futura muerte ex natura del ordenamiento jurídico internacional pero, paradójicamente, gracias a la lógica de costes políticos los conflictos armados desde el final de la Guerra Fría son más excepción que regla y, ante la necesidad de suplir esta vulnerabilidad surge la GZ como nueva punta de lanza tanto, para países revisionistas respecto al statu quo, como para las grandes potencias que prefieren mantener una imagen impecable que no afecte a su legitimidad, aunque también existe la posibilidad de que el actor que la ejercita no sea soberano. Se trata entonces de una realidad con una doble dimensión donde lo que es ficción a ojos del Derecho se transforma en un asesino silencioso que no tendrá piedad cuando muestre su rostro.

Siguiendo esta lógica, la GZ tendrá como pilar fundamental la ambigüedad ya que, su principal

1 La zona gris (GZ), se configura como un nuevo método de uso de la fuerza y la amenaza pero que, a diferencia de las categorías clásicas, actúa bajo el umbral de la agresión formal de acuerdo con el Derecho Internacional. De este modo, se puede afirmar que se trata de un nuevo tipo de paz basada en una competición entre los distintos entes que componen la esfera internacional, y, que tiene como principal característica la mala fe. Si bien es cierto que su conceptualización es nueva, es una realidad con un desarrollo histórico extenso como muestra la "Marcha Verde" en el marco de las aspiraciones del Reino de Marruecos respecto al Sáhara Occidental, la conocida como Leyenda Negra como una de las primeras operaciones psicológicas a gran escala, o el actual conflicto entre China y Japón por las Islas Senkaku.

función es evitar el enfrentamiento directo por medio de operaciones que enmascaren u oculten su autoría dificultando la toma de decisiones del adversario, además de tener como finalidad obtener objetivos estratégicos en un periodo de medio-largo plazo (Baques, 2021) sin la necesidad de acudir a un conflicto armado o preparando uno futuro. Por ello, se servirá de herramientas que se podrían categorizar como híbridas en el sentido de que mezclan medios convencionales y no convencionales, tales como guerra electrónica, operaciones de información, la instrumentalización de movimientos civiles contrarios al estado, la utilización del ciberespacio para amplificar lo anterior o realizar nuevas acciones dentro de este.

*2.1 El ciberespacio como elemento de hibridación en la zona gris*

Cabría decir, que el ciberespacio se ha proclamado por méritos como el nuevo campo de batalla del siglo XXI. Su amplitud, flexibilidad y anonimato han permitido que sea el terreno preferido para grandes potencias, pequeños estados, y actores de otros indoles como empresas privadas, organizaciones terroristas o criminales donde tienen la posibilidad de desarrollar acciones que puedan poner en jaque determinados intereses, sectores e incluso la propia integridad de la entidad afectada, sea soberana o no. Por el contrario, aunque parezca sorprendente, no se puede afirmar a día de hoy que haya existido una situación análoga al conflicto armado en el ciberespacio, es decir, una ciberguerra, aunque para certificarlo habría que determinar que se debe entender por este término.

Por ciberguerra habría que entender un tipo de agresión hacia un estado realizada o incitada por un ente que puede ser soberano o no, con el objetivo de interferir o neutralizar el funcionamiento normal de dicho ente a través de acciones promovidas por medios convencionales o no convencionales que afecten a nivel estratégico, político, y social. Limitar la ciberguerra a las desavenencias entre estados es un craso error puesto que la introducción de nuevos actores en la esfera internacional dirige inevitablemente hacia una anacronía que pone más límites de actuación que respuestas ante ofensas de estos nuevos actores, como podrían ser grandes las corporaciones u organizaciones criminales trasnacionales que, en muchos casos tienen más poder que pequeños estados y mucha influencia en los grandes. Casos como el del Banco Santander son paradigmáticos, puesto que, sus ingresos en el año 2017 serían equivalentes al PIB de Panamá (Belinchón, 2018), quebrando uno de los aspectos que determinan la existencia de soberanía: el poder.

Por otra parte, existen casos donde organizaciones criminales se constituyen como un poder paralelo al estado a través del ejercicio de monopolio de la violencia, como es el caso de los cárteles mexicanos donde el estado ya ha tenido que recurrir en varias zonas a negociar en igualdad de términos con estas organizaciones criminales, generando incluso un problema de alcance geopolítico (Manrique, 2019). Por tanto, teniendo las capacidades tecnológicas, los medios humanos y financieros adecuados cualquiera de estos entes podría trasladar una suerte de hostilidades al ciberespacio, creando una amenaza que podrá ser crítica para el estado según la propia intensidad que logre crear.

Sin embargo, la ciberguerra no será habitual dentro de las estrategias híbridas, sino que, serán los ciberataques los que tomen el protagonismo[2]. Estos ciberataques representan agresiones aisladas con

2 Los ciberataques son según el glosario del Centro Criptológico Nacional (CCN) la *"Acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan."*

diversos objetivos limitados que pueden ir desde el robo de cierta información, la propaganda o la propia desestabilización del sistema. Sus características revisten una naturaleza similar a las llamadas operaciones de *small footprint* debido a su difícil rastreabilidad y su flexibilidad de comisión. Son estas facilidades las que hacen atractivas el uso de este tipo de acciones por determinados actores que prefieren jugar bajo el paraguas de la baja visibilidad, o que por el contrario prefieren evitar el enfrentamiento directo generando una suerte de disuasión al mostrar las debilidades que afloran con el éxito de un ciberataque.

Es en este contexto donde se introduce el fenómeno de la privatización de ciertos servicios operacionales debido a las grandes ventajas que ofrecen respecto del uso de los propios medios empezando por el coste económico, la posibilidad de conseguir personal cualificado de forma inmediata y, lo más importante, mantener la ambigüedad de las acciones a través del desdibujamiento de la autoría. Por ello, no será extraño encontrarse a entidades y organizaciones legales e ilegales que ofrezcan sus servicios con cuestionables parámetros éticos para quien pueda y quiera adquirirlos, como si de una suerte de mercenarios del siglo XXI se trataran.

Siguiendo este razonamiento, distinguiremos entre empresas militares y de seguridad privadas, hackers o hacktivístas y, las organizaciones criminales que se especializan en la venta de Ransomware como servicio (RaaS).

### 2.1.1 Empresas de seguridad y militares privadas (ESMP)

Las empresas de seguridad y militares privadas no son algo nuevo en la historia, sin embargo, sí hay que destacar que existe un progresivo proceso de privatización de determinados servicios que tradicionalmente han sido estatales, pasando desde la propia seguridad nacional, el desarrollo I+D, mantenimiento y gestión logística, hasta la política exterior. Es debido a estas circunstancias donde determinados servicios que requieren de una alta especialización o de tomar decisiones con un alto coste político sean propicias para la intervención de las ESMP, puesto que el coste económico podrá ser más bajo, las facilidades de contratación y negociación serán mayores que en el sector público, y a nivel internacional pueden no tener tanta repercusión debido al efecto "hombre de paja" que pueden llegar a provocar (Damián, 2024). A su vez, entre las ventajas del uso de este tipo de entidades encontramos la nula regulación internacional que existe sobre la actividad que pueden llegar a desarrollar, aunque, si bien es cierto que existen declaraciones internacionales en este sentido, no pasan de ser documentos no vinculantes que instan a los estados partes a regular de forma interna la actividad empresarial y, los principios éticos que deben de seguir.

A efectos de este análisis cobran importancia las ESMP tecnológicas, o lo que es lo mismo, las que se centran en el desarrollo de herramientas de software y hardware para ofrecer soluciones tecnológicas a los estados sobre diversas materias como pueden ser herramientas de seguridad de sistemas, acceso a satélites, o incluso ciberinteligencia. En apariencia, suponen una buena solución para estados que no tienen la capacidad para el desarrollo de estas capacidades, pero, por el contrario, en determinados sectores pueden suponer un verdadero reto para la seguridad en el caso de que sus parámetros éticos sean de dudosa validez, o el control que ejerza el estado donde reside la sede sea bastante laxo. Existen diversos ejemplos bastante sonados en recientes acontecimientos que conducen a plantearse diversas cuestiones sobre la existencia y la actividad que desarrollan. Uno de ellos es caso de NSO Group.

Fundada el 25 de enero de 2010 con sede central en Israel, y con una actividad mercantil centrada en el desarrollo de ciberinteligencia solo para gobiernos, supone uno de los grandes gigantes que ofrece soluciones tecnológicas a distintos gobiernos con el objetivo en teoría de combatir el terrorismo y el crimen organizado. El producto que más ha trascendido a la opinión pública ha sido el "software Pegasus" que según su manual de utilización se define como:

*"Pegasus es una solución de ciberinteligencia* ***líder en el mundo que permite a las fuerzas de seguridad y a las agencias de inteligencia extraer de forma remota y encubierta información valiosa de prácticamente cualquier dispositivo móvil. Esta innovadora solución fue desarrollada por veteranos de agencias de inteligencia de élite para proporcionar a los gobiernos una forma de abordar los nuevos retos de interceptación de comunicaciones en el campo de batalla cibernético altamente dinámico de hoy en día. Al capturar nuevos tipos de información de dispositivos móviles, Pegasus salva una importante brecha tecnológica para ofrecer la inteligencia más precisa y completa para sus operaciones de seguridad****.*[3]

Es decir, se trata de un software espía que tiene como finalidad la captación de inteligencia a través de dispositivos que permiten la comunicación por medios electrónicos destinado a ser usado para combatir el crimen y el terrorismo pero que, por el contrario, su utilización ha estado salpicada por varias polémicas puesto que ha sido usado para fines distintos a los previstos inicialmente, llegando al punto de ser usado para espiar a altos cargos de gobiernos europeos como muestra la recomendación del Parlamento Europeo de 15 de junio de 2023[4] sobre el *"Examen del uso del programa espía de vigilancia Pegasus y otros programas equivalentes"*, donde se admite que varios altos cargos de gobiernos europeos han sido espiados a través de este programa y, se alerta sobre la posible utilización para actuar contra opositores políticos.

Todo ello genera algunas cuestiones El primer planteamiento que suscita es: ¿por qué existe una ausencia total de una regulación internacional que armonice el estatus jurídico de estas empresas? Las respuestas podrían ser variadas, aunque lo evidente es que la propia naturaleza del Derecho Internacional exige por una parte la cooperación entre los estados para llegar a un acuerdo, y por otra la necesidad de consentimiento de estos, en virtud del principio de soberanía, para someterse a esta regulación, lo cual ya plantea limitaciones pues, llegar a acuerdos en estas cuestiones suele ser tedioso y largo. No hay más que ver que la práctica internacional demuestra que los mayores hitos tardan años en fraguarse, lo cual nos lleva a la segunda cuestión: que deban ser los propios estados los que regulen de manera interna estas empresas de acuerdo a intereses propios que no tienen por qué estar inspirados en el respeto a los derechos fundamentales o sigan parámetros éticos de dudosa validez que posibiliten facilidades para la venta de este tipo de herramientas y servicios a grupos criminales u organizaciones terroristas.

3 Manual NSO software Pegasus P.7. Disponible en: https://ia801005.us.archive.org/1/items/nso-pegasus/NSO-Pegasus.pdf

4 Procedimiento Parlamento Europeo 2023/2500(RSP)

### 2.1.2 Hackers y Hacktivísmo

El hacktivismo es una nueva forma de activismo ideológico que se materializa en el mundo digital trayendo a escena una nueva forma de desobediencia civil electrónica. Se entiende por desobediencia civil electrónica la acción por la que se trata de desestabilizar o cambiar el orden prestablecido a través de actuaciones que pueden ir desde la pasividad, hasta el propio sabotaje digital a través de ciberataques. Su razón de ser proviene de la propia digitalización que, inevitablemente ha provocado también un cambio en los movimientos ideológicos antisistema, pasando de tener una tradicional estructura jerarquizada como la de un partido político, a modelos encuadrables dentro de la "netwar" (Jordán, 2004) que permiten llevar a cabo determinados ciberataques de difícil atribución debido al amplio espectro de células interconectadas que implica la propia netwar, además de ampliar sus capacidades operativas sin poner en riesgo la propia estructura de dicha organización. Por el contrario, no siempre habrá organizaciones políticas que reivindiquen intereses ideológicos detrás pues, no será novedad que determinadas agencias de inteligencia instrumentalicen esta clase de movimientos con el fin de desarrollar estrategias híbridas o en el espectro de la zona gris. Siguiendo este razonamiento, casos como el del grupo "Fancy bear" son recurrentes.

Presuntamente asociado al GRU ruso, es usado como proxy para cometer diversos ciberataques hacia países OTAN y relacionados con el objetivo realizar labores de propaganda pro kremlin, espionaje o robo de información. Su modus operandi, se centra en la explotación de vulnerabilidades emergentes a través del uso de diversos tipos de malware (Junquera, 2023). De esta manera, se consigue una ambigüedad que atiende a la necesidad de conseguir logros estratégicos a largo plazo evitando una escalada que pueda conducir a un conflicto convencional.

Resulta importante añadir que un hacktivísta no es un ciber delincuente o, en principio no tiene por qué serlo, pues cuando hablamos de hacktivísmo nos referimos a un fenómeno puramente ideológico que, si bien es cierto que puede cometer acciones que puedan ser encuadradas dentro de tipos penales, su principal finalidad es conseguir logros colectivos que van más allá de la simple vulneración de bienes jurídicos protegidos, pues estos quedan en un segundo plano respecto a sus fines principales.

Por otra parte, el concepto de ciberdelincuente es una construcción puramente criminológica para hacer referencia a los autores de los delitos informáticos de manera formal, a la cual le es indiferente que el *mens rea*[5] tenga fundamentaciones políticas o reivindicativas pues la propia categoría carece de un requisito de dolo especial que permita calificar al ciberdelincuente como tipo especial en el Código Penal, como podría pasar en otros casos.[6]

### 2.1.3 Ransomware as a service (RaaS)

Se tratan de organizaciones criminales que, al igual que las ESMP tecnológicas se centran en otorgar soluciones tecnológicas a ciberdelincuentes a través del desarrollo de malware para explotar vulnerabilidades. En sí, no se trata de una nueva adaptación del concepto referido a la organización criminal tradicional, sino, a un nuevo modelo de negocio ilícito que se ha adaptado a las nuevas

5 Se refiere a la voluntad o intención de querer cometer el delito.

6 Por ejemplo, en el crimen de genocidio el Estatuto de la Corte Penal Internacional exige un dolo especial pues, el elemento subjetivo que determina la existencia del *dolus specialis* es la protección del grupo (art.6.a).

tecnologías. Sus modelos de financiación se adaptan al propio perfil del cliente y van desde: el pago de mensualidades para acceder a las herramientas, el pago de una cuota única que otorga la "licencia de uso" del ransomware, e incluso, en colaboraciones para la distribución de beneficios a través de programas de afiliados o asociaciones entre los dos interesados. Normalmente van acompañados de servicios de mantenimiento y asistencia técnica, llegando al punto en algunos casos a proporcionar personal técnico especializado. Normalmente, la oferta se distribuirá en la Darkweb, sin embargo, es posible contactar con estas organizaciones a través de plataformas de comunicación electrónica como Telegram.

El problema que genera el surgimiento de esta nueva forma de delincuencia es la nueva posibilidad que tienen tanto los ciberdelincuentes como los ciberterroristas, de adquirir herramientas especializadas para cometer acciones que pongan en peligro la propia seguridad tanto colectiva como individual, pues pueden ser empleadas tanto, para realizar extorsiones a personas naturales y jurídicas o atacar a las instituciones estatales como una forma de desestabilización de bajo coste que implica la necesidad de destinar recursos estatales tanto para la protección y la persecución de estas organizaciones sometiendo a más presión a la propia arquitectura de seguridad en torno a la cual se sustenta el estado.

## 3. ¿Terrorismo en el ciberespacio?

El terrorismo entendido como un fenómeno social que instrumentaliza la violencia para conseguir fines políticos por su propia naturaleza parte de una situación de debilidad donde, la instrumentalización de la violencia para crear una atmosfera de terror se transforma en su principal arma y las estrategias hibridas son su medio. En este sentido, la concepción de la guerra como un equilibrio de fines y medios se abandona, ya que con la distribución y el uso masivo de las nuevas tecnologías ese equilibrio se ha roto pues con medios de coste relativamente bajo se pueden producir daños que, en un pasado no tan remoto, solo eran alcanzables con medios convencionales. Por esta razón, se ha popularizado el término ciberterrorismo, aumentando la difícil problemática que ya existía para definir el concepto originario y generando una preocupación excesiva en determinados casos pues, aún no se ha producido ningún atentado usando medios electrónicos que haya tenido una gran repercusión, lo cual parece concluir en principio que las organizaciones terroristas no tienen los medios para desarrollar operaciones que impliquen ciberataques a una gran escala y que, en definitiva, pongan en riesgo la propia integridad de la arquitectura estatal, aunque esto no puede obligar a descartar la posibilidad de que se den nuevas formas de ataques terroristas que puedan llegar a causar víctimas mortales, ya que, por ejemplo, basta con que se interfiera la infraestructura que controla los semáforos para generar un verdadero desastre. Por el contrario, parece constatable que el ciberespacio se ha centrado por el momento en ser una nueva herramienta para la difusión masiva de acciones consistentes en propaganda, reclutamiento, recolección de inteligencia, apoyo de operaciones, comunicaciones o, para el uso de Ransomware como una nueva forma de extorsión. En otras palabras, el ciberespacio se vuelve una herramienta complementaria para desarrollar y potenciar las capacidades de este tipo de organizaciones sin que estas lleguen a ser decisivas. Otra cuestión distinta es teorizar que en algún momento sea posible que una organización terrorista tenga

las capacidades para llevar a cabo acciones a gran escala que supongan un verdadero peligro para un estado, lo cual resulta poco probable desde el momento en que ni siquiera los propios países han sido capaces de desarrollar capacidades que permitan vislumbrar el peligro inmediato de una ciberguerra. Esto, queda certificado con el ejercicio realizado por la US Naval College, denominado Digital Pearl Harbor, donde se arrojaron resultados poco alentadores para los que estuvieran esperanzados con esta posibilidad pues quedó certificado que, para construir una "ciberarma" que pueda conseguir dañar de manera masiva la estructura estatal, se necesitaría un presupuesto mínimo de 200 millones de dólares y cinco años de trabajo de laboratorio, siendo algo que pocos países pueden llegar a permitirse. (Nieto, 2018).

## 4. Conclusiones

Es evidente que la introducción del ciberespacio en el conflicto propiamente dicho ha provocado una revolución de los asuntos militares, lo cual ha tenido como consecuencia lógica inmediata una profunda transformación del conflicto armado que no ha dejado indiferente a nadie. Esto se manifiesta en nuevas oportunidades económicas, que han ido desde el aumento de la presencia de EMSP especializadas en otorgar soluciones tecnológicas para gobiernos, hasta nuevas formas de crimen organizado basados en modelos de negocio RaaS, y que en la práctica funcionan de la misma manera que una EMSP, pero para ciberdelincuentes.

Del mismo modo, a nivel estratégico también se ha producido una profunda transformación doctrinal que, inevitablemente, ha abocado a un cambio de la arquitectura de seguridad tanto estatal como a nivel operacional, dando lugar a nuevos tipos de estrategias como la llamada "guerra multidominio"[7], adoptada por las fuerzas armadas de EEUU en la última década, donde el ciberespacio y las comunicaciones entre las diversas plataformas ocupan un nivel privilegiado.

Por ello, podemos concluir que nos encontramos en una era de inestabilidad donde la paz se paga con ambigüedad, confusión e inseguridad, lo cual es aprovechado por actores no estatales que, para conseguir sus fines, se han ido actualizando y han incorporado estas novedades a su propia naturaleza, determinando, por tanto, un nuevo paradigma mundial. Por el contrario, tampoco tiene sentido caer en un alarmismo exagerado pues actualmente el tradicional modelo se mantiene, y siguen siendo los estados los que tienen más facilidades para ejercer una violencia de gran entidad, por lo que la actual existencia de conceptos como el de ciberterrorismo solo tiene sentido cuando estas organizaciones sean instrumentalizadas por estados y estos sean los que les provean de los medios necesarios para llevar acciones que puedan tener el mismo efecto que un atentado tradicional. Algo que, aunque por ahora sea poco probable, no debe de ser impedimento para desarrollar sistemas de protección efectivos que ejerzan un nuevo tipo de estrategia de disuasión que permita enfrentar a este nuevo tipo de amenazas y, a su vez, desarrollar políticas proactivas consistentes en sistemas de alerta temprana, formación especializada en ciberseguridad. Todo ello con el fin de afrontar las posibles

7 Se trata de una nueva doctrina que han adoptado las Fuerzas Armadas de Estados Unidos en la última década, donde se entremezclan de manera conjunta, en el desarrollo de operaciones, todos los dominios de la guerra, es decir, tierra, mar, aire, espacio, ciberespacio, electromagnético y cibernético como consecuencia de los retos que supone la nueva realidad del teatro de operaciones contemporáneo.
Véase obras relacionadas como: Pulido. G (2021) *Guerra multidominio y mosaico; el nuevo pensamiento militar estadounidense* 1º ed. Catarata

brechas de seguridad que puedan producirse de manera eficaz y eficiente, además de contar con la necesaria e imprescindible colaboración y cooperación entre todas las instituciones estatales.

## 5. Bibliografía

Baqués, J. (2021), *De las Guerras híbridas a la Zona gris; La metamorfosis de los conflictos en el siglo XXI*, 1º ed. UNED.

F. Belinchón (18 de julio de 20189, *Apple, Netflix, Zara, Mercadona y otras 21 grandes empresas son tan grandes que superan el PIB de estos países",* Business Insider.

Departamento de Seguridad Nacional (2023), *Informe de seguridad nacional 2022*.

IBM, *¿Qué es el Ransomware como servicio?*

Jordán, J. (coord.) (2004), *Los orígenes del terror; indagando en las causas de terrorismo*, 1º ed., Biblioteca Nueva, Madrid.

Instituto Español de Estudios Estratégicos (2020), *Límites Jurídicos de las operaciones actuales; nuevos desafíos,* Cuadernos de estrategia nº201, Ministerio de Defensa, pp. 60-62.

Instituto Español de Estudios Estratégicos (2020), *Límites Jurídicos de las operaciones actuales; nuevos desafíos, IEEE, Cuadernos de estrategia nº201, Ministerio de Defensa.*

Junquera, A. *(28 de marzo de 2023), Fancy Bear y dónde encontrarlo,* Tarlogic.

Manrique, L.E. (12 de diciembre de 2019), "*El narco, poder paralelo en México",* Política Exterior.

Manual NSO software Pegasus.

Nieto, I. (2018), *La letalidad del ciberterrorismo*, Revista general de la marina Vol.275.

Procedimiento Parlamento Europeo 2023/2500(RSP)

Rubio, F. (2024), *Guerra S.A; La privatización de los conflictos armados,* 1º ed., Espasa, Madrid.