# Introducción a la guerra no cinética

**Javier Vea Remacho**
***Comandante del Ejército del Aire***

En 2013, el jefe del Estado Mayor General de Rusia, general Valery Gerasimov, publicaba un artículo[1] en el que plasmaba su percepción predictiva sobre las futuras operaciones de combate. Ocho años después, algunas de las características que incluía en dicha perspectiva podrían servir perfectamente como preámbulo a este texto, cuyo objetivo no es otro que ofrecer una perspectiva general de la guerra no cinética, también conocida por sus siglas en inglés: NKW[2].

Gerasimov pronosticaba que las guerras del futuro ya no se declararían y que una vez iniciadas, su evolución proseguiría un patrón desconocido. Que veríamos un amplio uso de herramientas cinéticas y no cinéticas en estrecha coordinación. Que la distinción entre los dominios militares y civiles se volvería aún más borrosa. Y que además del espacio físico, las batallas tendrían lugar en el espacio de la información. Un abanico descriptivo que nos presentaba una Guerra Híbrida en la que cabía cualquier acción diseñada intencionadamente para debilitar al oponente, incluidas las políticas, económicas y culturales. La hibridación en la contienda es comparable a un «botón del caos» que actúa como un ecualizador, combinando operaciones cinéticas y no cinéticas para maximizar el efecto deseado. Puede graduar la intensidad, seleccionando la letalidad del arsenal disponible (desde interferencias radio hasta armas de destrucción masiva) y también el equilibrio (su capacidad más sutil), precisando la línea de acción más eficiente mediante la combinación de acciones cinéticas y no cinéticas. La eliminación selectiva de emisoras de radio unida a una sólida campaña informativa por las redes sociales puede ser un ejemplo de cómo modificar la opinión del adversario, abocándolo a los intereses propios.

## HALLANDO UN LUGAR ENTRE LA TAXONOMÍA Y LA SEMÁNTICA

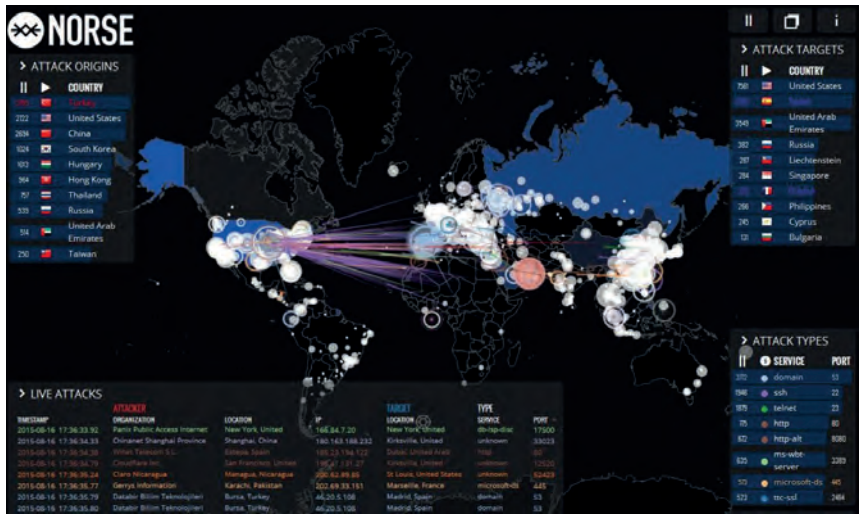
El término «no cinético» no lo inventó un general ruso. Lleva usándose más de una década en el entorno militar, pero la constante evolución en el estudio del espectro electromagnético[3], así como la incorporación del entorno digital y el espacial a las operaciones militares, han dado lugar a cambios constantes en su definición, causando cierta confusión.

*Non-kinetic* se usa en el entorno militar para referirse a operaciones bajo el paraguas de la guerra electrónica[4], la guerra ciberespacial[5], la guerra de la información[6] y la guerra espacial[7], la última y más moderna incorporación a la lista. Una variedad disciplinar cuya acción combinada ofrece resultados acordes a la amenaza actual, sobre todo en las fases iniciales de conflictos de baja intensidad, en los que la mediación precisa el uso del bisturí en lugar del sable.

A falta de una definición ampliamente consensuada, la guerra no cinética podría definirse como «el uso de herramientas informativas, psicológicas, diplomáticas, económicas, sociales y tecnológicas del Estado para lograr intereses y objetivos nacionales, ya sea aceptando o perjudicando la voluntad nacional del adversario»[8].

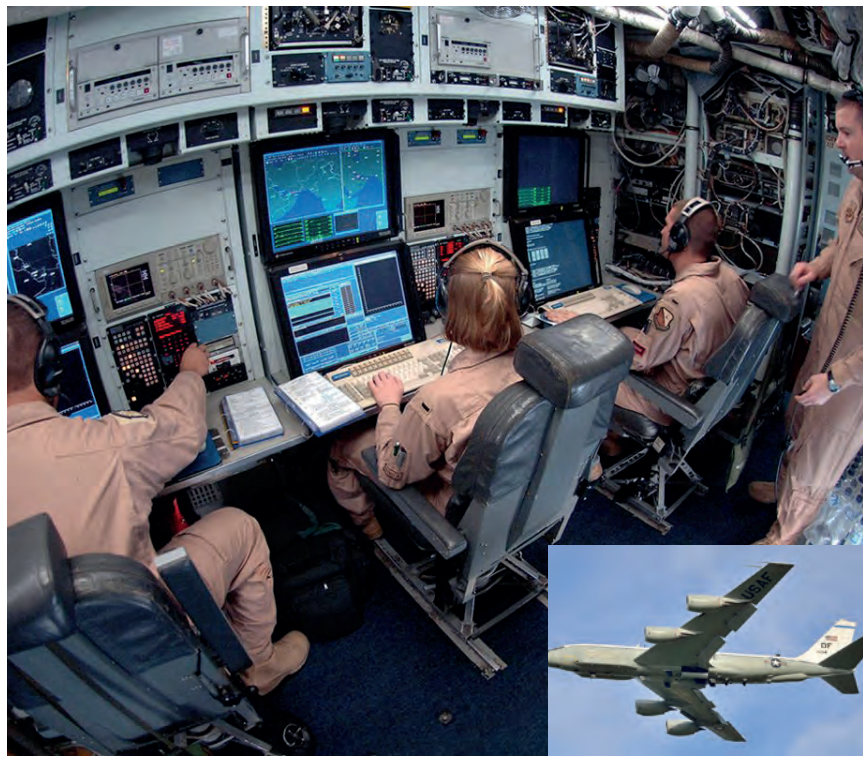
## LA ADAPTACIÓN A LA AMENAZA HÍBRIDA EN EL ENTORNO NO CINÉTICO

La expansión y difusión de la tecnología avanzada hacen que el acceso al entorno de la NKW resulte cada vez más asequible. Es sencillo adquirir capacidades que den acceso al ciberespacio y a la información más competitiva que antes solo estaban al alcance de los países más desarrollados, lo cual erosiona su ventaja tecnológica. Esto favorece el veloz crecimiento de la amenaza híbrida, especialmente la que proviene de actores no estatales haciendo uso indiscriminado e ilegal de acciones no cinéticas.

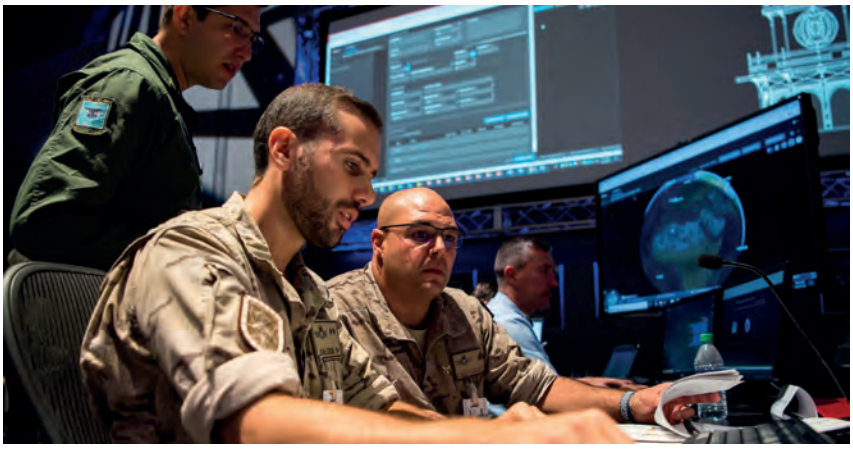



*La actividad ilegal en la red es lucrativa y prolífica, engrosando la amenaza con actores no estatales, pero no por ello menos peligrosos o capaces que los estatales*

La actividad ilegal en el entorno no cinético es lucrativa y disputada, agravando la amenaza y llegando a plantear un auténtico desafío al Derecho Internacional, que requiere un enfoque adecuado para actuar. Algo parecido a unas gafas bifocales con las que obtener una visión nítida del cuerpo normativo de cada nación en particular y del entorno multinacional en general. Solo así podríamos adaptarnos a la amenaza y diseñar una respuesta acorde, proporcionada[9], ética, y sobre todo legal.




*El RC135 Rivet Joint es una de las plataformas usadas por los EE.UU. en operaciones de guerra electrónica, dotada de una excelente capacidad SIGINT (inteligencia de señales)*



*La adaptación al entorno no cinético por parte del Ejército del Aire es un hecho. La operatividad del RQ9 del Ala 23 y la creación del Centro de Operaciones de Vigilancia Espacial (COVE) son dos de los hitos destacables más recientes*

El aporte de la amenaza híbrida a la guerra moderna está íntimamente relacionado con la tecnología. Tanto que la Red, en el amplio sentido de la expresión, y el Espectro Electromagnético constituyen su entorno. Un espacio de maniobra concreto y altamente disputado, donde la energía se propaga por cable o por el espacio, de manera trasversal a los tradicionales dominios físicos terrestre, marítimo, aéreo o espacial. De ahí que la cuádruple respuesta no cinética (EW, IW, CW y SW) forme un conjunto basado en redes.

La USAF[10] lleva más de catorce años trabajando en la adaptación: «Las acciones cinéticas son llevadas a cabo con medios físicos y materiales como bombas, balas, cohetes y otras municiones. Las acciones no cinéticas son lógicas, electromagnéticas o conductuales, como un ciberataque a un sistema enemigo o una operación psicológica dirigida a tropas adversarias. Si bien las acciones no cinéticas tienen un componente físico, los efectos que provocan son principalmente indirectos: funcionales, sistémicos, psicológicos o conductuales[11]».

## NKO[12]: LAS OPERACIONES NO CINÉTICAS

Una operación (o una acción) no cinética sirve de facilitador para conseguir algo. Ya sea atravesar un sistema integrado de defensa aérea[13], localizar un objetivo de alto valor[14], explotar medios de comunicación del adversario, o proteger la propia infraestructura de red. Esa operación generará un efecto, generalmente no cinético, y acabará provocando un estado final deseado. Ejemplo: «Interrumpir de manera selectiva una línea telefónica (acción) incomunicará temporalmente el terminal de un HVT (efecto). Privarle de este medio le forzará a optar por otro que resulte más vulnerable a nuestros propósitos (estado final deseado)».

Las NKO no se perciben dando un paseo por la calle. Sus efectos son difíciles de atribuir a un autor, y suele ser el usuario de la tecnología el primero en advertir que algo está pasando. Estas operaciones no suelen dejar un agujero humeante en el suelo, no producen sonidos violentos, y no ocasionan derramamiento de sangre civil colateral. Son operaciones precisas, discretas y esquivas, pero con una contundente capacidad de influencia que no debe subestimarse.

Infravalorar el poder de la guerra no cinética es no entender las operaciones integradas. La sincronización de operaciones de EW, IW, CW y SW, entre ellas o combinadas con otras de tipo cinético, pondrá en un serio aprieto a unas fuerzas armadas que no estén adaptadas para combatir en esta arena. De ahí surge la necesidad de un cambio de paradigma en el moderno tratamiento de asuntos militares y la constante preparación y adaptación al entorno no cinético de los ejércitos modernos.

***Las NKO no suelen dejar un agujero humeante en el suelo, ni tampoco producen sonidos violentos, ni derramamiento de sangre civil colateral. Son operaciones precisas, discretas y esquivas, pero con una contundente capacidad de influencia que no debe subestimarse***

## EL PLANEAMIENTO DE LAS NKO

Durante la preparación previa a una operación militar, el elemento de planeamiento debe definir parámetros como la plataforma física apropiada para llevar a cabo una determinada misión. Pero ¿qué le lleva a optar en primer lugar por una capacidad cinética? Una primera respuesta podría ser por su familiaridad con determinados sistemas de armas, pero una reflexión más profunda podría mostrar que por desconocimiento de las opciones no cinéticas. Más allá de la elección de un tipo de aeronave, un misil o una táctica, queda patente que el elemento de planeamiento NK no solo requiere un buen conocimiento de las capacidades del componente que representa: aeroespacial, marítimo, terrestre o conjunto, sino una conciencia situacional[15] de los elementos esenciales en NKO: el espectro electromagnético y la red.

*La integración del elemento no cinético debe ser una máxima en el planeamiento y ejecución de operaciones militares. Tan importante es la selección de la plataforma y el armamento convencional, como su combinación con los facilitadores que provienen del espectro electromagnético y la red*

Conociendo las posibilidades del entorno no cinético y adaptándolas a la preparación de inteligencia del entorno operativo[16], aparecen nuevas opciones militares, favoreciendo la inserción y sincronización de acciones cinéticas y no cinéticas. Las NKO requieren plena integración con el elemento de inteligencia, cuyos planificadores ISR[17] deben estar adaptados al nuevo entorno, para ajustarse a los requerimientos priorizados de inteligencia[18] con nuevas opciones que aseguren un flujo bidireccional de inteligencia durante la ejecución.

***Al principio de la guerra en Afganistán, las fuerzas de la coalición atacaron los nodos de comunicaciones del adversario que previamente habían sido fuentes de obtención para inteligencia. Tras la eliminación de estos nodos mediante acciones cinéticas no se pudo recopilar más información por dicho canal, causando un grave daño al dejar una brecha para la obtención de información muy valiosa***

No serviría de mucho tener la capacidad de influir en las comunicaciones telefónicas del adversario sin conocer perfectamente su red de telefonía. ¿Es terrestre, digital o por satélite? ¿Dónde están los nodos de comunicaciones? ¿Están controlados remotamente? ¿Tienen salida a Internet? La acción del elemento de inteligencia reduciría la incertidumbre, concretando nuestras opciones:

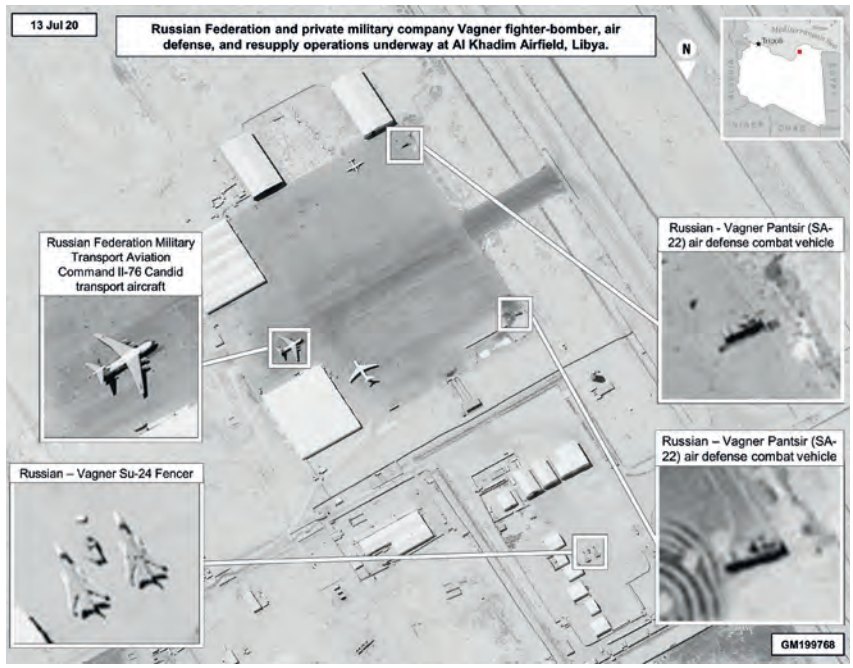
interferir la señal, denegar el servicio del teleoperador, limitar el acceso a las comunicaciones satélite o introducir un software malicioso en la red. En definitiva, acciones que causarían impedir, retrasar o corromper las comunicaciones del objetivo dejándolo en un estado final deseado, de manera poco o nada atribuible, y sin daños colaterales lamentables.

Otra «bondad» del planeamiento es que permite escalar la eficacia o el rendimiento de nuestra acción NK durante su ejecución, añadiendo acciones por capas. Volvamos al ejemplo: Queremos incomunicar un HVT (estado final deseado) y desde una aeronave operando en zona lanzamos un ataque que interfiere su línea de microondas (acción), privándole de ese medio (efecto). El adversario decide continuar operando mediante telefonía móvil. Advertimos que sus comunicaciones aún son efectivas y añadimos un ataque por denegación de servicio. El objetivo ha quedado aislado, viendo limitadas sus posibilidades de enviar/recibir órdenes.

## EL *TARGETING* EN LAS NKO

*Targeting* es un término usado en doctrina militar para describir el modo en que se utilizan los medios disponibles para influir en un objetivo con el fin de lograr los fines políticos y/o militares impuestos por el Mando, sincronizándolo con el resto de la operación[19].

El *targeting* cinético se refiere a la aplicación específica de la fuerza militar basada en la liberación o concentración de energía cinética contra fuerzas u objetos del oponente con (principalmente) efectos letales en el dominio físico. El *targeting* no cinético describe la aplicación de capacidades (militares y no militares) contra objetivos para generar efectos no cinéticos (adicionales) en el dominio físico y no físico principalmente dirigidos a la telefonía, los ordenadores y las redes de objetivos dentro y fuera del campo de batalla tradicional[20].




*El targeting es esencial para la selección de objetivos militares y los métodos para influir en ellos, ya sea por medio de la destrucción, la degradación o simplemente su anulación temporal. Las alternativas no cinéticas permiten alcanzar objetivos en el dominio no físico*

Debemos tener presente que lo que hace del *targeting* no cinético un elemento vital en las operaciones militares contemporáneas es precisamente su carácter complementario. Por sí mismo puede alcanzar algunas metas a nivel táctico, pero si queremos obtener resultados precisos y completos al nivel operacional o incluso estratégico, lo ideal es encontrar la combinación adecuada de *targeting* cinético y no cinético, complementándose unos a otros.

El aporte no cinético, propio del siglo XXI, permite involucrar actores adicionales (aliados, neutrales u oponentes), alcanzar efectos menos devastadores (incluso efectos constructivos) aportando medios adicionales para llevar a cabo las operaciones, haciendo hincapié en el papel crucial de elementos no cinéticos como la comunicación, la información, la percepción, la cohesión, la comprensión, y la voluntad[21].

Entender el *targeting* no cinético puede resultar desconcertante. Somos herederos de un patrón de guerra convencional que nos lleva a ver límites difusos entre lo cinético y lo no cinético cuando usamos métodos o herramientas que se salen del arsenal militar tradicional y que desencadenan efectos más allá del campo de batalla que ya conocíamos. Pero nadie dijo que la respuesta a una amenaza tan compleja vendría de la mano de una solución simple.

## *NON-KINETIC FIRE* (NKF): EJEMPLOS DE ATAQUE NO CINÉTICO

Tal como veíamos antes, los ataques no cinéticos son facilitadores. Generan un efecto que desencadena un estado final deseado, casi siempre haciendo uso del Espectro Electromagnético y la Red. Con ejemplos se ve más fácil:

Guerra Electrónica (EW): Interferir la frecuencia de radio (acción) que usa un objetivo puede degradar suficientemente sus comunicaciones (efecto), forzándole a optar por la vía telefónica móvil. La utilización del teléfono móvil revelaría su

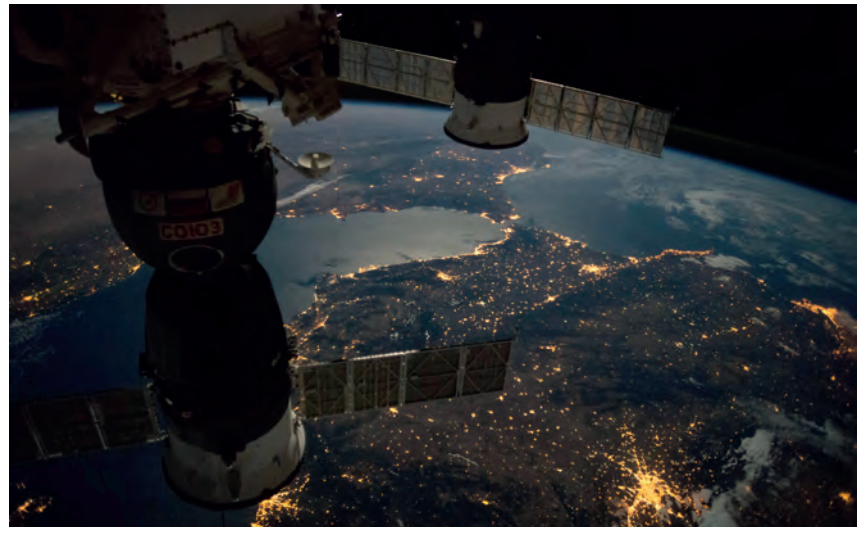
*El Krasuja-4 es uno de los sistemas más avanzados utilizados en el ámbito de la guerra electrónica por Rusia. Su capacidad para interferir drones, aeronaves, misiles y satélites a cientos de kilómetros lo colocan en la vanguardia de las operaciones no cinéticas*

posición con cierta precisión, incrementando su vulnerabilidad (estado final deseado) ante un hipotético ataque aéreo.

Guerra de Información (IW): Insertar en redes sociales imágenes de altos cargos en actitud inadecuada (acción) podría influir en una audiencia objetivo, produciendo desconfianza en la cadena de mando (efecto). Eso fomentaría la degradación en el liderazgo y el deseo de no entablar combate obedeciendo a un mando incompetente (estado final deseado).

Ciberguerra (CW): Inocular *malware* en un sistema de emisión de imagen radar (acción) podría corromper la imagen difundida (efecto) a otras instalaciones y aeronaves con una apariencia deformada, aparentando un cielo limpio, saturado, o con falsos objetivos, provocando respuestas no adecuadas al oponente (estado final deseado) según nuestras necesidades.

Guerra Espacial (SW): Introducir modificaciones selectivas en la tecnología GPS (acción), provocaría el mal funcionamiento de sistemas dependientes de esa tecnología (efecto), sumiendo en un caos tecnológico al oponente (estado final deseado), dañando su disponibilidad financiera, su armamento guiado, o su capacidad logística, por mencionar algunos efectos.



*Las operaciones espaciales son lo último en la panoplia no cinética. Una ventaja tecnológica vuelve a desequilibrar la balanza a favor de actores más desarrollados*

***Las operaciones espaciales con satélites están lejos del alcance de muchos usuarios. Cuentan con una variada y resolutiva gama de ataques cinéticos y no cinéticos: congelación de efectivos financieros para bloquear la compra de armamento; denegación de señal GPS para limitar la precisión de municiones guiadas; privación de comunicaciones vía satélite para forzar al uso de medios más vulnerables; radiación de energía directa para destruir térmicamente medios espaciales o aéreos… llevan implícito un mensaje suficientemente disuasorio***


*Rusia es muy activa en el ciberespacio. Y a pesar de lo difícil que resulta atribuir su intervención en determinadas operaciones, ya nadie duda de su influencia en los ciberataques contra Georgia en 2008 o en la intromisión durante las últimas elecciones presidenciales de los EE.UU.*

## LA HISTORIA RECIENTE Y LAS OPERACIONES NO CINÉTICAS

Las operaciones no cinéticas no son nuevas y la historia contemporánea contiene evidencias de su existencia. Hace poco más de una década, la Oficina Federal de Investigaciones[22] de los EE.UU. ya consideraba a los ciberataques como la tercera mayor amenaza para su seguridad nacional, detrás de la guerra nuclear y las armas de destrucción masiva[23].

En el mundo del ciberespacio, la piratería informática quedó inmortalizada en 1988, con la infección de la red del Instituto Tecnológico de Massachusetts con el primer gusano de Internet, colocado allí por un estudiante[24]. Más de treinta años después, comprobamos que las operaciones espaciales y ciberespaciales han encontrado su hogar en el mundo de las operaciones militares, concretamente en el entorno no cinético.

Quizá el ejemplo más ilustrativo de ciberataque estratégico ocurrió el 27 de abril de 2007, cuando en cuestión de horas, los sitios web del gobierno de Estonia, los periódicos y los principales bancos habían caído. Las redes Estonias de Mando y Control militar se habían visto comprometidas. Un adversario había atacado cientos de objetivos en todo el país, pero no había carros de combate rugiendo, ni bombarderos haciendo pasadas, ni siquiera un disparo. Nada más y nada menos que una plaga zombi formada por ordenadores privados de todo el mundo[25] abriendo un frente en el ciberespacio.

Un año más tarde se repetía en Georgia un escenario casi idéntico, justo antes de que el ejército ruso les invadiera. Un ciberataque masivo inutilizó los sistemas en red de sus fuerzas armadas, afectando seriamente la operatividad de sus defensas aéreas y redes de Mando y Control en todo el país. Una operación


*El 2 de noviembre de 1988, Robert T. Morris (con 23 años en la imagen) liberó el primer gusano conocido en ARPANET (una precursora de internet) y tres días después se propagó a los ordenadores de todos los puntos vitales de los EE.UU.: la NASA, la RAND, el Pentágono, las principales universidades… fueron cayendo una tras otro*

no cinética que causó gran impacto en el ejército, el gobierno y el pueblo georgianos, antes de que se oyera silbar la primera bala[26].

Las redes invisibles que sirven de soporte al ciberespacio parecen intangibles, pero cuando las operaciones no cinéticas son llevadas a cabo eficazmente causan resultados sustanciales. Tal fue el caso en septiembre de 2008, cuando sitios web propagandísticos de al-Qaeda fueron atacados por infiltrados cibernéticos desconocidos. La acción era difícilmente atribuible, pero la mayoría de los analistas consultados orientaron sus sospechas hacia la figura de «ciberoperadores» occidentales no identificados. Esos sitios web de Al-Qaeda recibieron un claro mensaje: «su presencia en la Red, aunque virtual, es conocida y por tanto vulnerable»[27].

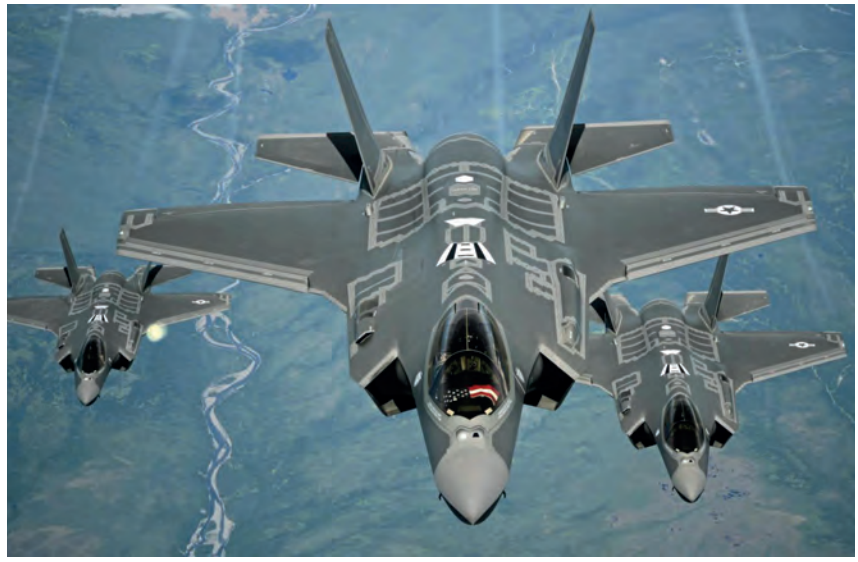
***Los eventos no cinéticos más significativos de la historia contemporánea pertenecen al ámbito de las operaciones en el ciberespacio, pero ponen de manifiesto la eficacia de las NKO. Especialmente si se combinan con operaciones cinéticas en un contexto temporal adecuado***

## NKW: EL SOLAPE TECNOLÓGICO

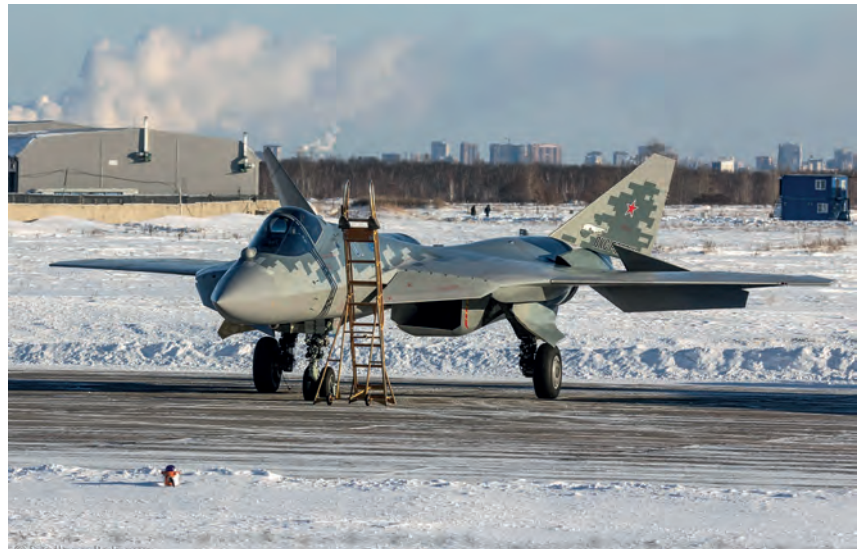
De acuerdo con el acta de la 15.ª Reunión Internacional sobre Guerra Ciberespacial y Seguridad[28] de 2020, «La NKW es un concepto operativo que se aplica sobre un entorno solapado que integran espectro electromagnético, espacio de información y ciberespacio para facilitar el logro de la superioridad en el entorno no cinético. El objetivo es crear un conocimiento compartido, acelerar el proceso de toma de decisiones y acciones, incrementar la eficacia de las misiones, mejorar la probabilidad de supervivencia en conjunto con fuerzas amigas, y elevar el nivel de sincronización en la ejecución de acciones»[29].

**Electronic Warfare (EW)**

La EW usa el EMS para detectar, proteger y comunicar en beneficio propio, o negar su utilización al adversario. El EMS es un área de actividades amplia, caracterizada por fenómenos físicamente observables (luz visible, y láseres) e invisibles (microondas y energía electromagnética)[30]. Su utilización minimiza el



*Lockheed Martin asegura que su modelo F-35 posee unas excepcionales capacidades para incrementar la alerta situacional del piloto, mejorar la identificación y uso de armamento, y compartir información con otras aeronaves y centros de mando y control, por no hablar de las de EW*



*Como aeronave de 5.ª generación, el Su-57 Felon es la contrapartida rusa al F-35 y al F-22. Existe una versión más moderna, el Su-75 Checkmate, de la cual se conocen pocos detalles, pero que señalan hacia un desarrollo electrónico como principal mejora en el ámbito de la EW*

riesgo del combatiente limitando su exposición, reduce costes por ahorro de munición y ofrece a los líderes militares una gama de opciones cuyos efectos se antojan inalcanzables a través de medios cinéticos.

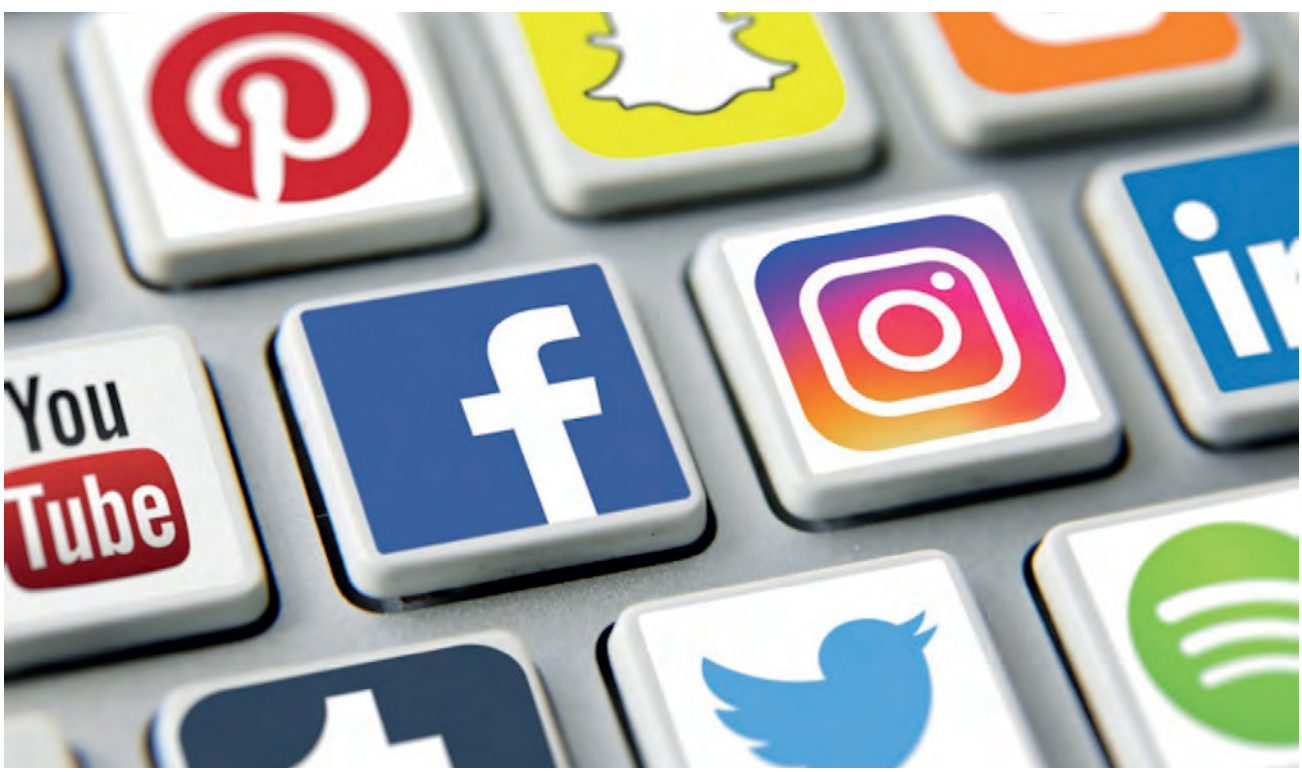
La doctrina militar define generalmente a la EW como una acción militar cuyo objetivo es el control del espectro electromagnético. Este objetivo se logra a través de acciones de ataque electrónico ofensivo[31], protección electrónica defensiva[32], recolección de inteligencia, y apoyo a la guerra electrónica por reconocimiento de amenazas[33]. Las capacidades de EW incluyen energía dirigida, señuelos e interferencias de radiofrecuencia[34] para negar, interrumpir o engañar la capacidad electromagnética de un adversario. Los medios propios de la guerra electrónica son el radar, las telecomunicaciones o la navegación.

Los sistemas de EW pueden dividirse en sistemas analógicos *front-end*, que detectan y reciben información, y sistemas de procesamiento de datos digitales *back-end,* cuya funcionalidad proviene del *software*. La unión de ambos sistemas proporciona capacidades modernas como el radar, las telecomunicaciones, la orientación de navegación de precisión PNT[35], los emisores de interferencia (*jammers*) y los señuelos[36].

**Information Warfare (IW)**

La guerra de información tiene un alcance cognitivo, cultural y social que incide sobre el conocimiento, la comprensión, la opinión, y en última instancia, las acciones del individuo en solitario, en un grupo o en una organización[37], afectando al ciclo lógico de toma de decisiones conocido por las siglas OODAA (observar, orientar, decidir, actuar y asesorar). Su objetivo es reunir, proporcionar y negar información para mejorar la propia toma de decisiones mientras daña la del enemigo a través de diversos medios de comunicación con campañas manipuladoras y operaciones psicológicas[38].

El poder de la información y los medios de comunicación está anulando todas las demás políticas e instrumentos de poder en el mundo actual. El desarrollo, la conformación y la gestión de la percepción se han convertido en el principal medio para fomentar actitudes, comportamientos y decisiones por parte de las audiencias objetivo[39]. Inundando las mentes de dichas audiencias objetivo con un gran volumen de información se nubla su capacidad de discernir entre lo que es real y lo que no lo es. Si se cree, ignora o desconfía de la información dependerá de la capacidad intelectual del receptor, así como de la credibilidad del remitente.




*La capacidad del «quinto poder» nunca ha pasado desapercibida, pero su transición al mundo digital y posterior inmersión en la Red han supuesto un inquietante trampolín para la política actual. Las redes sociales, diseñadas originalmente para fines menos trascendentes, son el vehículo perfecto para ejercer influencia de manera global*

Las operaciones de información[40] buscan la superioridad de la información combinando sus capacidades propias con otras líneas de acción para influir, interrumpir, corromper o usurpar la toma de decisiones de adversarios y/o potenciales adversarios, al tiempo que protegen nuestra propia información, sus procesos y sus sistemas. Las INFO OPS no son nada nuevo, pero la falta de comprensión de su potencial como herramienta ofensiva y las vulnerabilidades inherentes a dicho conflicto presenta amenazas estratégicas potencialmente graves para los países con una alta dependencia de las economías basadas en la información y la red.

***Las INFO OPS, también conocidas como operaciones de influencia, aprovechan profusamente el ciberespacio como multiplicador de fuerza, usando la propaganda y la desinformación en redes sociales para afectar la percepción pública, influir en su opinión, y catalizar de manera inmediata sus efectos (manifestaciones, violencia…), algo que a los tradicionales movimientos populares les llevaba meses o incluso años***

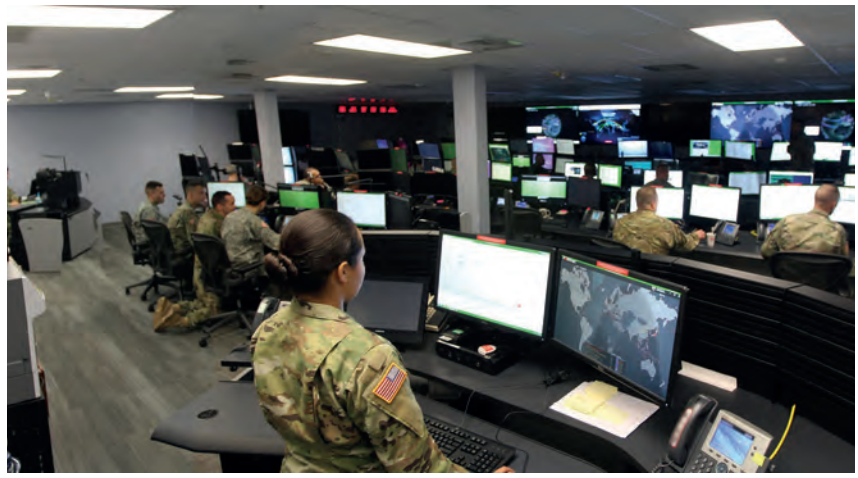
**Cyber Warfare (CW)**

La CW trascurre por un entorno artificial, hecho por el hombre y, por ende, diferente a los dominios naturales de tierra, mar, aire y espacio. El ciberespacio es más que internet, es un dominio en toda la regla que incluye no solo *hardware, software* y sistemas de información, sino también personas e interacción social dentro de estas redes.


La CW es el componente no cinético más reciente en conexión con EW e IW. Esta conexión es tan intensa, que las actividades en el ciberespacio inciden en la libertad de acción de los otros dominios, y las actividades en los otros dominios pueden crear efectos en, y a través, del ciberespacio[41]. La CW es ofensiva y defensiva: puede paralizar o destruir los sistemas basados en la tecnología ICT[42] del enemigo mientras mantiene los propios operativos[43].

La «caja de herramientas» de la CW evoluciona a una velocidad vertiginosa. Su repertorio, entre otras, incluye capacidades como denegar al enemigo servicios provistos por la Red (electricidad, información, comunicaciones, finanzas, acceso remoto a instalaciones industriales), influir en sus consumidores (campañas de información, decepción, espionaje), o proteger los nuestros (garantizar la disponibilidad, fiabilidad e interoperabilidad de activos de información).

Lanzar un ciberataque en lugar de uno tradicional/cinético crea más ambigüedad en términos de efectos, fuentes y motivos. Por lo tanto, si los ciberataques funcionan –y esto es un tremendo sí– cambian el perfil de riesgo de las misiones, transformándolas en opciones más atractivas[44]. A diferencia de la conducción de la guerra pasada, otros



*El amplio repertorio de la CW es «casi» tan grande como la lista de amenazas, pero permite librar batallas a gran distancia de manera eficiente y resolutiva. Los centros de operaciones como el de la foto son el presente en las instalaciones de mando y control*

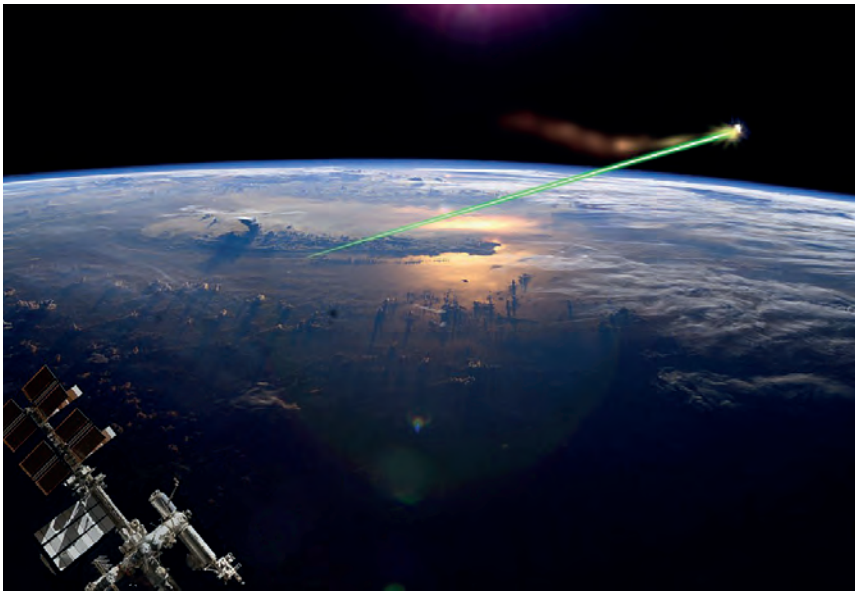
actores pueden librar una guerra cibernética desde lejanos confines del mundo de forma rápida, barata, anónima y devastadora.

**Space Warfare (SW)**

El espacio es un lugar de uso público, gratuito y abierto a todo usuario. Un medio poco convencional y conocido, pero tan amplio que constituye en sí mismo una gran vulnerabilidad. Su uso ya fue regulado por la ONU en 1967 mediante el tratado sobre el espacio ultraterrestre, un marco facilitador para la intervención del derecho internacional. Su texto establece básicamente que está reservado solo para uso pacífico, que debe permanecer libre de armas de destrucción masiva, que nadie puede reclamar sus territorios y que cualquier objeto a él lanzado debe ser conocido por la ONU.

La sociedad moderna depende del Espacio, sin paliativos. Cada día cuesta más encontrar actividades que funcionen de manera independiente, sin ayuda que provenga de él. Del espacio depende la tecnología GPS, el pronóstico meteorológico terrestre y espacial, el control financiero global, la radiodifusión, la navegación, el cultivo moderno, la aviación, las telecomunicaciones, la acción de sensores remotos, la Logística, la ciencia… Puede que la SW sea la última incorporación al equipo NKO, pero no cabe duda de la contundencia de sus capacidades. Así como decíamos de las NKO que actuaban de facilitador, el Espacio es un multiplicador.

Las operaciones militares espaciales nos mantienen alerta de las amenazas provenientes de la superficie terrestre y del espacio exterior, proporcionan comunicaciones vía satélite, posicionamiento y navegación, amplitud del entorno de detección, y por último y no menos importante, plataforma para medios ISR. No está mal como primer plato, si tenemos en cuenta la amenaza ligada al medio que abarca desde piratería, interferencias, encriptaciones de red, o ciberataques, hasta efectos climáticos espaciales y colisiones con basura espacial o meteoritos, sin dejarnos atrás los ataques con misiles, láser o pulsos electromagnéticos.



*El espacio es la última incorporación a la familia no cinética y constituye un dominio por sí mismo. En la foto se muestra una recreación de la capacidad DEW (Direct Energy Weapon) mediante láser*

Consciente de su trascendencia, la OTAN considera el Espacio un dominio en sí mismo desde diciembre de 2019, y desde 2020 cuenta con su propio plan de implantación. La capacidad espacial precisa del EMS y la Red como el resto de las capacidades no cinéticas, pero por suerte es bastante más cara y exclusiva, lo cual la aleja del alcance de muchos actores, estatales y no estatales, poco deseables en la lista de potenciales adversarios.

***La USAF ya cuenta con una organización centrada en la guerra de la información llamada 16ª Fuerza Aérea que combina operaciones de EW, CW, IW e ISR***

## CONCLUSIONES Y ANÁLISIS

Las NKO constituyen un elemento esencial en la guerra híbrida que ha permitido que actores no estatales reduzcan distancia con los países más desarrollados en la disputa por sus intereses. Son especialmente resolutivas cuando se usan de manera combinada con operaciones cinéticas, como muestra la historia reciente, actuando a modo de facilitador para conseguir un efecto, generalmente no cinético, que propicie un estado final deseado.

Son operaciones precisas y, a veces, tan sutiles que no pueden ser atribuidas claramente a un autor. Pero podría decirse que su mayor virtud reside en el carácter constructivo: permiten alcanzar metas mediante efectos menos devastadores, y reducen el riesgo a las fuerzas propias en determinadas misiones; involucran actores adicionales y aportan nuevos medios para llevar a cabo las operaciones de manera exitosa, convirtiéndose en un elemento de vital importancia en las operaciones militares contemporáneas.


*La evolución del componente no cinético en la guerra moderna afectará al futuro de las operaciones militares. Puede que la próxima vez que tenga lugar un conflicto militar, lo primero en oírse no sea un disparo*

EW, IW, CW y SW aprovechan el avance tecnológico y la dependencia cada vez mayor de sus elementos naturales, la Red y el Espectro Electromagnético, generando un cambio con nombre propio en las reglas del juego de la guerra moderna. Dicho cambio afectará no solo al cómo se resolverán las futuras operaciones militares, sino también al dónde tendrán lugar, y a quién encontraremos allí. ■

## REFERENCIAS


– Mason Clark: *Russian Hybrid Warfare*. Institute for the study of war (USA). 2020. https://www.scribd.com/document/490315726/Russian-Hybrid-Warfare-ISW-Report-2020-pdf

– Martti Lehto, Gerhard Henselmann: *Non-Kinetic Warfare, the new game changer in the battle space*. 15th International Conference on Cyber Warfare and Security (USA), 2020. https://www.researchgate.net/publication/339943524

– George Popp: *Kinetic and Non-Kinetic Tactics of Competing Powers over the coming decade*. NSI Analytic Services (USA), 2019. https://nsiteam.com/social/wp-content/uploads/2019/09/Future-of-Global-Competition-and-Conflict-ViTTa-Q2-Report_final.pdf

– Flemming Splidsboel Hensen: *Russian Hybrid warfare, a study of disinformation*. Danish Institute for International Studies (DEN), 2017. https://pure.diis.dk/ws/files/950041/DIIS_RP_2017_6_web.pdf

– Paul Ducheine, Michael N. Schmitt: *Targeting: The Challenges of Modern Warfare*. Asser Press (NED). 2016. https://link.springer.com/content/pdf/10.1007%2F978-94-6265-072-5.pdf

– Paul Ducheine: *Non-kinetic Capabilities: complementing the Kinetic Prevalence to Targeting*. Amsterdam Center for International Law, 2014. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474091

– Major Jeffrey C. Crivellaro (USAF): Combined arms in the Electromagnetic Spectrum: integrating non-kinetic operations. School of Advanced Military Studies (USA), 2013. https://apps.dtic.mil/sti/citations/ADA583814

– General Valeriy Gerasimov: *The value of science is in the foresight: new challenges demand rethinking the forms and methods of carrying out combat operations*. Voyenno-Promyshlennyy Kuryer (RUS), 2013. http://vpk-news.ru/articles/14632

– Colonel Erika R. Flanigan: Integrated non-kinetic operations: *the frontier of warfare in search of doctrine*. Faculty of the school of advanced air and space studies (USA), 2010. https://apps.dtic.mil/dtic/tr/fulltext/u2/1019178.pdf


## NOTAS

[1]The value of science is in the foresight: new challenges demand rethinking the forms and methods of carrying out combat operations. Voyenno-Promyshlennyy Kuryer (RUS), 2013.
[2]Non-Kinetic Warfare (NKW).
[3]Electro-Magnetic Spectrum (EMS).
[4]Electronic Warfare (EW).
[5]Cyber Warfare (CW).
[6]Information Warfare (IW).
[7]Space Warfare (SW).
[8]Farooq, 2014.
[9]La amenaza híbrida conlleva una respuesta híbrida que combina operaciones cinéticas y no cinéticas.
[10]Fuerza Aérea de los EE.UU.
[11]Air Force Doctrine Document 2, 03ABR2007.
[12]Non-Kinetic Operations.
[13]Integrated Air Defence System (IADS).
[14]High Value Target (HVT).
[15]Situational Awareness (SA).
[16]Intelligence Preparation of the Operational Environment (IPOE).
[17]Intelligence, Surveillance, Reconnaissance (ISR): Inteligencia, Vigilancia, Reconocimiento.
[18]Prioritized Intelligence Request (PIR).
[19]Paul Ducheine, 2017.
[20]Paul Ducheine, 2017.
[21]Paul Ducheine, 2017.
[22]Federal Bureau of Investigations (FBI).
[23]Rick C. Hodgin, 2009.
[24]Robert T. Morris demostró así la vulnerabilidad de la red ARPANET, explotando vulnerabilidades que había descubierto y siendo el primer condenado por la Ley de Fraude y Abuso Computacional de EE.UU.
[25]Shackelford: «Estonia Two-and-A-Half Years Later».
[26]Shackelford: «Estonia Two-and-A-Half Years Later».
[27]«Al-Qaeda Websites Hit by Western Cyber Attacks,» Daily Telegraph (22OCT2008).
[28]International Conference on Cyber Warfare and Security (ICCWS).
[29]Martti Lehto, 2020.
[30]Martti Lehto, 2020.
[31]Electronic Attack (EA).
[32]Defensive Electronic Protection (EP).
[33]Electronic warfare Support (ES).
[34]Radiofrequency Jamming (RFJ).
[35]Precision-navigation-targeting (PNT).
[36]Martti Lehto, 2020.
[37]JP 3-0, 2018.
[38]Psychological Operations (PSY OPS). También conocidas como Military Information Support Operations (MISO) cambiaron su nombre temporalmente para suavizar el carácter del término.
[39]IWP, 2019.
[40]Information Operations (INFO OPS).
[41]Erika R. Flanigan, 2010.
[42]Information and Communications Technology.
[43]Wooding, 2019; Wardrop, 2018.
[44]Libicki, 2011.