LA INFLUENCIA DE LA DIMENSIÓN CIBER EN LAS OPERACIONES MULTIDOMINIO

PLAN DE CARRERA Y CAPACITACIÓN DEL PERSONAL DEL EJÉRCITO DE ESTADOS UNIDOS INTEGRANTE DEL COMANDO CIBER

Por CL **OSCAR SANTIAGO ZARICH**

ARTÍCULO CON REFERATO

Marco teórico

Aproximadamente una década atrás, las Fuerzas Armadas de Estados Unidos de América comenzaron a investigar sobre nuevas teorías y formas para desarrollar las operaciones militares en el futuro. Así surgió el término conocido como *"Operaciones Multidominio"*. Si bien este es un viejo concepto, donde la primera campaña sobre el Golfo Pérsico en la denominada Operación Tormenta del Desierto, podría ser tomada como ejemplo, la concepción de esta operación en su esencia difiere de todo lo anterior si se toma en cuenta ciertas variables que se han implementado. En **primera medida**, las Operaciones Multidominio son aquellas que se desarrollan en un espacio tanto físico (dominio terrestre, marítimo, aéreo y espacio exterior) como intangible (dominio ciber: incluye el espectro electromagnético y el conocimiento), se entiende a este último como la información y la opinión que fluye en *"la nube"*[1]

Palabras Clave:
> Comando
> Ciberdefensa
> Ciberseguridad
> Integración
> Inteligencia estratégica

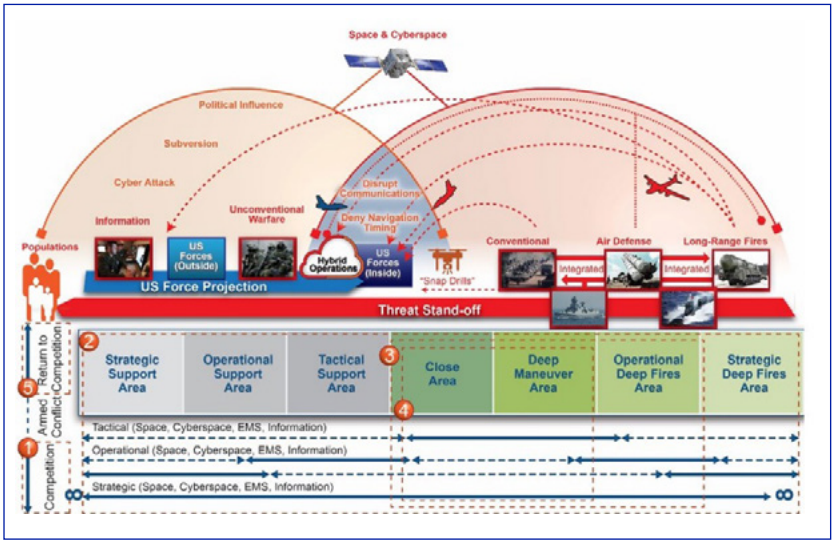
El objetivo final del Comando Ciber es lograr, en un plan de diez años, superar a sus adversarios en el espacio de la información, en combinación con otras operaciones de los distintos dominios.

(*cloud computing* según su versión en inglés) vertida por los medios de comunicación en los distintos portales de noticias y en las redes sociales. La **segunda variable** y más importante es que las Operaciones Multidominio comienzan a desarrollarse mucho antes del conflicto armado mismo, incluso anterior a su gestación durante la etapa de crisis, estando dirigidas hacia aquellos Estados o grupo de Estados considerados en posición de competencia. La **tercera condición** para desarrollar estas operaciones está dada en generar distintos dilemas (convertir debilidades del oponente en vulnerabilidades) sobre distintas áreas, zonas o espacios en forma simultánea, con la finalidad de generar caos y confusión en la toma de las decisiones. La **cuarta condición** está signada por la descentralización y disminución, hacia niveles subalternos, de la autorización para empeñar los fuegos de largo alcance sobre objetivos identificados como blancos de prioridad.

A su vez existen dos condiciones como consecuencia de la implementación de las anteriores; que es, por un lado, el desarrollo de la **inteligencia artificial** con el fin de reunir, procesar y analizar el gran volumen de información que se recibe, para disminuir exponencialmente el tiempo empleado en el ciclo OODA (observar, orientar, decidir y actuar) para la toma de la decisión[2] y, por otro lado, desarrollar la capacidad de **vuelo de aeronaves de elevación vertical tripuladas y no tripuladas**[3] con el propósito de influir en un corto período en la profundidad del dispositivo del oponente.

En resumen, básicamente este tipo de operaciones sienta sus bases sobre el control del dominio espacial y ciber, el desarrollo tecnológico y la inteligencia artificial. De esta forma, los distintos medios de obtención distribuidos tanto en tierra, mar, aire y espacio identificarán distintas amenazas aportando dicha información a *"la nube"*. A partir de allí, los sensores de superficie tripulados y no tripulados procesarán la información determinando qué plataforma o sistema de armas será el más conveniente para neutralizar la amenaza.

CONCEPTO ESQUEMÁTICO DE LAS OPERACIONES MULTIDOMINIO



Fuente: TRADOC Pamphlet 525-3-1. *The U.S. Army in Multi - Domain Operations* 2028.

1. "La computación en la nube es un modelo que permite el acceso a la red de forma conveniente y extendida, bajo una demanda compartida en red cajo un conjunto de recursos informáticos (hard y software) con capacidad para aprovisionar y liberar información rápidamente con un mínimo esfuerzo de gestión o interacción del solicitante. El modelo de nube requiere cinco características esenciales. auto servicio de la demanda, amplio acceso a la red, puesta en común de recursos, capacidad de almacenamiento y elasticidad del sistema y dimensión del servicio" (Mell & Grance, 2011).
2. Kallberg, 2020.
3. Veazey, 2019 y Freedberg Jr., 2020.

Para ello, tomando en cuenta el nuevo escenario donde se plantean los conflictos del futuro, el Departamento de Defensa de Estados Unidos ha encargado la misión a sus Fuerzas Armadas para organizar, instruir, adiestrar y alistar a su personal y medios, asignando a cada Fuerza una tarea específica. El Ejército de Estados Unidos anunció que el Comando Ciber de la Fuerza tenía la intención de cambiar su nombre por Comando de Guerra de Información del Ejército, planteando la nueva organización desde un concepto más abarcativo en relación a las tareas que deberán cumplir sus Unidades dependientes en este nuevo ambiente operacional que impondrán las Operaciones Multidominio en los conflictos armados futuros[4].

El objetivo final del Comando Ciber es lograr, en un plan de diez años, superar a sus adversarios en el espacio de la información, en combinación con otras operaciones de los distintos dominios. Así, el Ejército de Estados Unidos se ha planteado que resulta imprescindible "superar a los países en clara competencia con sus intereses, influyendo sobre sus comportamientos. Las Operaciones Multidominio se han convertido en una preocupación cada vez más urgente para el Pentágono en los últimos años"[5].

En relación con el párrafo anterior, vale la pena mencionar la sostenida relación de competencia que existe entre Rusia y Estados Unidos de América, incluso Rusia había sido acusada de intervenir de manera cibernética en los comicios presidenciales de 2016 manipulando la campaña en favor de un candidato[6]. Así también, pesa sobre Rusia la acusación de algunos funcionarios de la Casa Blanca por difundir por difundir información tergiversada sobre la actual pandemia de coronavirus, que utiliza una serie de sitios web en inglés, habiendo sido identificados al menos tres de ellos a través de la plataforma *InfoRos.ru, Infobrics.org y OneWorld.press*[7].

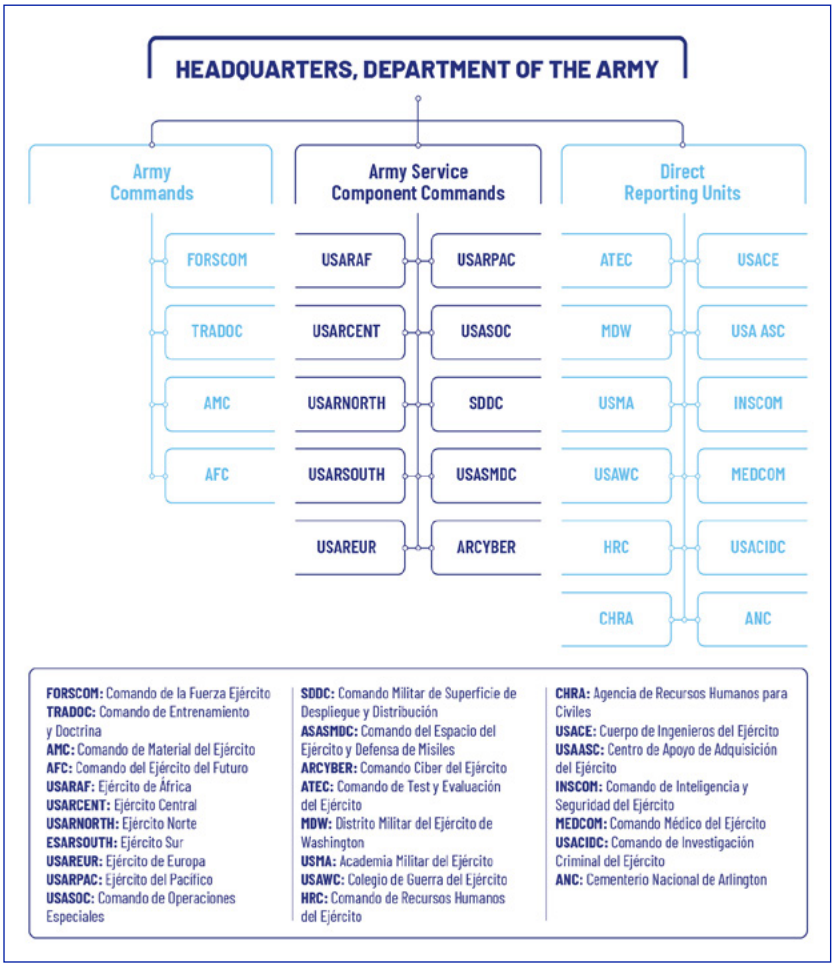
Organización de la Fuerza Ejército de los Estados Unidos de América

En este marco de cambios permanentes en su orgánica, institucionalmente, el Ejército de Estados Unidos proyecta una visión para el año 2028 en la cual dicha Fuerza será capaz de:

> desplegar, combatir y obtener éxito contra cualquier adversario, en cualquier momento y en cualquier lugar, en un conflicto armado conjunto, multidominio y de alta intensidad, al tiempo que deberá guardar capacidad de disuasión a otros actores y mantener su capacidad para conducir un conflicto no convencional. El Ejército logrará esto mediante el empleo de vehículos de combate terrestres modernos tripulados y no tripulados, aviones, sistemas de apoyo logístico y armas, junto con formaciones de armas combinadas robustas y tácticas basadas en una doctrina moderna de combate centrada en líderes y soldados excepcionales con letalidad sin igual[8].

Consecuentemente, la estructura del Comando del Ejército se encuentra organizado en cuatro Comandos Principales, diez Comandos Componentes y doce organismos que le dependen directamente. Particularmente, el Comando Ciber se encuentra integrando al grupo de los Comandos Componentes.

ESTRUCTURA DEL COMANDO DEL EJÉRCITO DE ESTADOS UNIDOS DE AMÉRICA



Fuente: https://www.army.mil/organization

El dominio ciber resulta una de las más críticas áreas de la Defensa Nacional. Este campo requerirá del más alto entrenamiento profesional y conocimiento disponible por parte de los interesados en ingresar a la Fuerza.

A su vez y para asegurar su eficiencia, el Ejército cuenta con distintos Centros de Excelencia dedicados a capacitar al personal de las distintas jerarquías y diferentes especialidades. Entre ellos, pueden mencionarse el "Centro de Excelencia de Aviación (ACoE), Fuegos (FCoE), Médico (HRCoE), Inteligencia (ICoE), Maniobra (MCoE), Apoyo a la maniobra (MSCoE), Comando de Misión (MCCoE), Liderazgo para Suboficiales (NCOLCoE), Operaciones Especiales (SOCoE) y Comando de Apoyo de Armas Combinadas (CASCOM)"[9].

Antecedentes del Comando Ciber del Ejército (ARCYBER) de Estados Unidos

El 1º de octubre de 2010, el Ejército designó a un General de tres estrellas como Comandante del ARCYBER, una organización del Ejército de nivel operacional que reporta directamente al Cuartel General del Departamento del Ejército y que además recibiera el honor de ser designado como el Segundo Ejército, organización que fue disuelta luego de la Primer Guerra Mundial. Dicho Comando operaba con un efectivo de aproximadamente 561 personas asignadas en Fort Belvoir y Fort Meade, a la espera de una decisión sobre su emplazamiento final. El efectivo total del Comando incluía aproximadamente unos 21.000 soldados, civiles y contratistas del Departamento del Ejército distribuidos en todo el mundo. Este Comando contribuyó a sincronizar y unificar el esfuerzo de todas las otras organizaciones del Ejército que cumplían sus funciones dentro del dominio cibernético.

Los principales cambios que trajo aparejado el Comando Ciber estuvo dado principalmente en las nuevas funciones esenciales dentro de su estructura y en el establecimiento del Centro de Operaciones e Integración Ciberespacial del Ejército (ACOIC). Por ejemplo, el ARCYBER hizo posible la integración del Comando de Inteligencia y Señales (INSCOM) con el Comando de Tecnología en Redes (NETCOM), colocándolas bajo su control operacional.

En la actualidad, el Comando Ciber del Ejército resulta una organización específica de nivel operacional dependiente del Cuartel General del Departamento del Ejército. Su Comandante ejerce el control operativo de todas las operaciones relacionadas con el dominio ciber, tanto de las operaciones ofensivas y defensivas en el ciberespacio como de la protección de la red de información que recae sobre el resto de las organizaciones de la Fuerza Ejército. Asimismo, dicho Comando organiza, administra, educa, adiestra, despliega y sostiene a las organizaciones relacionadas con el dominio ciber

CV

OSCAR SANTIAGO ZARICH

Es Coronel y Oficial del Arma de Infantería. Participó en la Misión de Naciones Unidas UNPROFOR en 1992 y Campaña Antártica 1999 – 2000. Es Oficial de Estado Mayor y Oficial de Estado Mayor Conjunto de las FFAA de la República de Francia. Es Licenciado en Administración de Empresas, en Estrategia y Organización, Master en Defensa y Geoestrategia por la Universidad de Paris II – Assas y Profesor Universitario para la Enseñanza Media y Superior Militar. Realizó el curso de maestría en estrategia militar en la ESGC. Actualmente se desempeña como Oficial de Enlace en el Ejército Sur de los Estados Unidos de América.

4. Pomerleau, 2020.
5. Vavra, 2020.
6. Agencia Reuters, 2020.
7. Tucker, 2020.
8. Milley, 2020.
9. U.S. Army Cyber Center of Excellence, 2020.

con dependencia en el Ejército para llevar a cabo sus operaciones.

Por otra parte, el Comando cuenta con las siguientes organizaciones; *U.S Army Network Enterprise Technology Command, 1st Information Operations Command, 780th Military Intelligence Brigade y la Cyber Protection Brigade*. A su vez, mantiene vínculos con el Departamento de Defensa de Estados Unidos, con el Comando Ciber de la Fuerza Aérea, la Armada, el Cuerpo de Marines y la Guardia Costera; como así también se relaciona estrechamente con la Reserva, la Guardia Nacional y el Centro de Excelencia del Ejército. Finalmente, mantiene vínculos con las siguientes academias; *Army Cyber School, Army Civil Institute, National Defense University College of Information and Cyberspace, Air Force Institute of Technologie, Defense Cyber Investigations Training Academy and Hacking for Defense.*

Plan de carrera y capacitación del personal de Ciberdefensa

El Ejército ofrece la posibilidad tanto a personal en servicio como a civiles técnicos que quieran incorporarse a la Fuerza, determinada capacitación profesional en el área de conocimiento relacionada con la ingeniería en *software*, ingeniería en sistemas operativos y desarrollo de *software*, ingeniería en *data scientist - machine learning* o sobre un campo de interés relacionado con la seguridad o protección ciber. Quienes ingresen al Cuerpo Ciber del Ejército accederán con el grado de Subteniente para poder alcanzar la jerarquía de Coronel.

"El dominio ciber resulta una de las más críticas áreas de la Defensa Nacional. Este campo requerirá del más alto entrenamiento profesional y conocimiento disponible por parte de los interesados en ingresar a la Fuerza"[10]. Para lograr ello, el Ejército de EE.UU. convoca a candidatos para cubrir vacantes en alguna de sus áreas de conocimiento de interés, tanto en **Oficiales y Suboficiales** como en aquellos candidatos que deseen ingresar a sus filas como **Oficiales Especialistas**.

Mientras que para los primeros básicamente las áreas a desarrollarse están dadas en Especialidades de Operaciones Ciber y de Guerra Electrónica, para los segundos lo serán como Técnicos en Guerra Ciber y en Guerra Electrónica.

En consecuencia, a través de distintos institutos y cursos se educa e instruye al personal que integrará el Comando Ciber. El Colegio Técnico Ciber recibe tanto al personal de Oficiales recientemente egresados, Oficiales Especialistas y Suboficiales. Los Oficiales recientemente egresados podrán realizar el Curso Básico para Oficiales en Conducción Ciber. Los Oficiales Especialistas podrán acceder al Curso de Técnico en Adiestramiento de Guerra Ciber. Por su parte, los Suboficiales tienen la posibilidad de capacitarse en el Curso de Técnicas Centrales Comunes Ciber y el Curso de Especialista en Adiestramiento Avanzado en Operaciones Ciber.

A su vez, existen cursos comunes destinados solo para Oficiales y Oficiales Especialistas, como el Curso Ciber para Capitanes y el Curso de Técnico Avanzado en Guerra Ciber (Avanzado para Oficiales Especialistas).

Por otra parte, en el Colegio de Guerra Electrónica, tanto los Oficiales Especialistas como los Suboficiales tendrán la posibilidad de capacitarse asistiendo a los siguientes cursos; Avanzado de Guerra Electrónica para Oficiales, Equipo Especialista de Compañía, Técnico Básico en Guerra Electrónica (Básico para Oficiales Especialistas), Técnico Avanzado en Guerra Electrónica (Avanzado para Oficiales Especialistas) y Conducción Avanzada en Guerra Electrónica[11].

Luego, el Centro de Excelencia Ciber exhibe un importante listado de cursos de capacitación donde el recurso humano del Comando Ciber podrá adquirir distintas competencias profesionales militares para el mejor desempeño en los distintos puestos.

Conclusiones

Algunas organizaciones militares en determinados países se han vuelto obsoletas, en relación con el directo condicionamiento que impone la incorporación de la tecnología en sus distintas estructuras, particularmente en aquellas que garantizan la supervivencia del comando y control de la Fuerza. Sin embargo, no solo la tecnología genera el motor en la revolución de los asuntos militares, sino que también influyen las nuevas formas para concebir las operaciones militares en el futuro inmediato. En este sentido, cinco serían los factores de éxito para garantizar una Fuerza Armada con capacidad de disuasión; 1) poseer dominio sobre el espacio exterior para controlar el posicionamiento global de los propios Elementos y guiado de proyectiles de largo alcance e identificar a los del oponente contrarres-

CURSOS DE CAPACITACIÓN A CARGO DEL CENTRO DE EXCELENCIA CIBER

COURSES	COURSES	COURSES	COURSES
• 17A - Cyber Operations Officer	• JC4PC - Joint C4 Planners Course	• International Military Students Office	• SWOILE - Signal Warrant Officer ILE
• 17B - Electronic Warfare Officer	• 26B - Information Technology Specialist	• SDMG - Signal Digital Master Gunner	• Management Client Course (MGC)
• 17C - Cyber Operations Specialist	• 25C - Radio Operator/Maintainer	• PCC - Cyber Center Pre-Command Course	• Security +
• 17E - Electronic Warfare Specialist	• 25D - Cyber Network Defender	• SBOLC - Signal Basic Officer Leader	• IP Addressing
• 170A - Cyber Operations Technician	• 25E - Electromagnetic Spectrum Manager	• SCCC - Signal Captains Career Course	• CISSP
• 170B - Electronic Warfare Technician	• 25L - Cable Systems Installer/Maintainer	• Signal Captains Career - Reserve Component	• WAN
• Warrant Officer Basic Course 255A	• 25M - Multimedia Illustrator	• Battalion S6	• Network Devices
• Warrant Officer Advance Course 255A	• 25N - Nodal Network System	• Brigade S6	• Network Security and Monitoring
• Warrant Officer Basic Course 255N	• 25P - Microwave Systems	• COMSEC Account Manager	• Network Troubleshooting
• Warrant Officer Advance Course 255N	• 25Q - Multi-Channel Transmission Systems	• Network Manager Security	• Networking Concepts
• Warrant Officer Basic Course 255S	• 25R - Visual Information Equipment	• 46Q - Public Affairs Specialist	• PC Troubleshooting
• Warrant Officer Advance Course 255S	• 25S - Satellite Communication Systems	• 46R - Public Affairs Broadcast Specialist	• Routing Operations
• FA26A - Network Systems	• 25U - Signal Support Systems Specialist	• Advanced Leaders Course	• Switching Operations
• FA26B - Information Systems Engineer	• 25V - Combat Documentation / Production	• Senior Leaders Course	• Joint Spectrum Manager

Fuente: U.S. Army Cyber Center of Excellence (www.cybercoe.army.mil)

tando sus ataques, 2) contar con inteligencia artificial en apoyo al sistema C4I2VR (Comando, Control, Comunicaciones, Computación, Inteligencia, Información, Vigilancia y Reconocimiento) para acelerar el proceso de toma de decisión garantizando la preservación de la Fuerza en el campo de combate, 3) lograr rapidez estratégica y velocidad táctica para desplazar elementos de magnitud desde la zona de retaguardia hacia la profundidad del dispositivo del oponente, 4) influir sobre la información que se desprende de los medios de comunicación y en los distintos portales de noticias y en las redes sociales para engañar al adversario, 5) contar con un sistema de sostenimiento logístico ininterrumpido acortando los tiempos entre el requerimiento y la distribución de los efectos en primera línea. Es allí, en este último punto, donde la impresión 3D está teniendo un desarrollo experimental y exponencial en la impresión de piezas de reemplazos de aeronaves no tripuladas, vehículos, raciones de combate y en otro tipo de efectos. Al respecto, ya existen desarrollos de este tipo en las Fuerzas Armadas de Estados Unidos y en la República de Francia. "Los soldados son los primeros usuarios de su equipo en el campo y sus comentarios son ricos en lecciones. Ahora pueden transformar sus necesidades en una realidad inmediata gracias a la impresión 3D"[12].

Por otra parte, la evolución y desarrollo de la tecnología, junto con la complejidad e incertidumbre que plantean los escenarios de los conflictos futuros, han generado la necesidad de mayor especificidad y especialización en todas las áreas de conocimiento en pos de intentar descomponer la realidad para comprenderla e interpretarla de una forma más acabada. Esto ha dado motivo al desarrollo de diferentes cursos de capacitación, particularmente en aquellas áreas relacionadas con el dominio ciber, un espacio de conocimiento en constante evolución y desarrollo. Tanta es la necesidad de especificidad, que el personal que integra el Comando Ciber integra un Cuerpo o Escalafón separado del resto de las Armas, que posee un plan de carrera y capacitación propio.

Por parte del Ejército Argentino, desde hace no más de dos años, se encuentra en evolución el área de Ciberdefensa formando parte de la Dirección de Comunicaciones e Informática del Ejército, siendo parte del proceso de la evolución que ha experimentado la Fuerza. En este sentido y ante la experticia desarrollada por otros países, como es el caso del Ejército de Estados Unidos de América, cabe hacernos la pregunta si la evolución de la Ciberdefensa del Ejército Argentino debería encontrarse separada de la Dirección de la cual depende y si nos encontramos ante la ocasión y necesidad de sumar una nueva Arma a las ya tradicionalmente conocidas.

10. U.S. Army Cyber, 2020.
11. U.S. Army, 2020.
12. Lagneau, 2020.

BIBLIOGRAFÍA

Cyber, U. A. (s.f.). www.goarmy.com. Recuperado el 30 de julio de 2020, de https://www.goarmy.com/army-cyber/careers-in-army-cyber.html

Excellence, U. A. (s.f.). www.cybercoe.army.mil. Recuperado el 30 de julio de 2020, de https://cybercoe.army.mil/

Grance, P. M. (septiembre de 2011). The NIST definiction of cloud computing. Gaithersburg, Maryland, Estados Unidos de América: National Institute of Standards and Technology.

Jr., S. J. (25 de febreo de 2020). breakingdefense.com. Obtenido de https://breakingdefense.com/2020/02/future-vertical-lift-armys-aerial-vanguard

Kallberg, J. (28 de julio de 2020). www.c4isrnet.com. Obtenido de https://www.c4isrnet.com/opinion/2020/07/28/in-an-evaporating-ooda-loop-times-is-of-the-essence

Lagneau, L. (1 de julio de 2020). www.opex360.com. Obtenido de http://www.opex360.com/2020/07/01/larmee-de-terre-dispose-de-lune-des-plus-importantes-fermes-militaires-dimprimantes-3d/

Milley, G. M. (s.f.). www.army.mil. Recuperado el 29 de julio de 2020, de https://www.army.mil/about/

Pomerleau, M. (26 de julio de 2020). www.c4isrnet.com. Obtenido de https://www.c4isrnet.com/smr/informacion-warfare/2020/07/26how-the-defense-department-is-reorganizing-for-information-warfare

Reuters. (s.f.). www.dw.com. Recuperado el 29 de julio de 2020, de https://www.dw.com/es/senado-de-eeuu-concluye-que-rusos-perjudicaron-a-clinton-en-comicios-de-2016/a-50743428

Tucker, E. (28 de julio de 2020). www.infobae.com. Obtenido de http://www.infobae.com/america/eeuu/2020/07/29/la-campaña-de-desinformacion-sobre-el-coronavirus-que-disemina-rusia-a-traves-de-tres-sitios-web-en-ingles

Vavra, S. (29 de julio de 2020). Here's how Army Cyber command plans to take on information warfare. Obtenido de www.cyberscoop.com: https://www.cyberscoop.com/army-cyber-command-plan-transition-information-war/

Veazey, S. (06 de noviembre de 2019). es-mb.theepochtimes.com. Obtenido de https://es-mb.theepochtimes.com/ejercito-de-ee-uu-publica-plan-de-16-años-para-superar-a-china-con-un-nuevo-concepto-de-batalla

www.goarmy.com. (s.f.). Recuperado el 30 de julio de 2020, de https://www.goarmy.com/army-cyber/army-cyber-training.html