Facultad del Ejército
Escuela Superior de Guerra
"Tte Grl Luis María Campos"

TESIS MAESTRÍA EN ESTRATEGIA Y GEOPOLÍTICA

Título:

"EL USO DE LAS OPERACIONES DE INFORMACIÓN EN LA DIRECCIÓN E IMPLEMENTACIÓN DE LAS OPERACIONES MILITARES."

Que para acceder al título de Magíster en Estrategia y Geopolítica presenta el Maestrando Tomás de Vergara

Director de Tesis: CR (R) Mg Dr Justino Bertotto

Ciudad Autónoma de Buenos Aires, 30 de junio 2021.

RESUMEN

Uno de los términos que aparece cada vez más frecuentemente en la literatura militar y civil especializada en conflictos es Operaciones de Información (OI). Esa frase no se encuentra definida en el léxico militar argentino, y normalmente se la pasa por alto, porque se piensa que es una parte de la especialidad de Inteligencia, desde que se ordena reunir información sobre el enemigo y el ambiente geográfico hasta que se la difunde en una organización jerárquica vertical. Sin embargo, y como se verá más adelante, se refiere a la información como una actividad de modificación de percepciones y de influencia en públicos tanto militares como civiles. Este aspecto merece la atención especial en los países del mundo oriental y occidental, debido al desmesurado progreso de las tecnologías de Información y Comunicaciones (TICs) en el comienzo del Siglo XXI. Todo es informaciyn: tal como enuncia Mark Vertuli, "la tecnología ha permitido que medios significativos interrumpan, manipulen, distorsionen y nieguen información, tecnología que los adversarios han ya demostrado que tienen la voluntad de usar con gran efecto … […] quien controle la informaciyn puede dominar la competencia y el conflicto".

Las OI son efectos que favorecen el logro de los propios objetivos, usando herramientas denominadas Capacidades Relacionadas con la Información. Estas OI causan efectos simultáneos a toda la profundidad del territorio propio, aliado, adversario y enemigo, en todos los medios de comunicación y en el ambiente de la información. En Estados Unidos, en el año 2018, la información pasó a ser considerada un nuevo ambiente que incluye el ciberespacio y el espacio electromagnético agregado a los dominios físicos de aire, mar, tierra y espacio.

No es propósito de esta investigación cuestionar el marco legal argentino, las implicancias en la división de seguridad interna y defensa externa, ni modificar ni sugerir cambios a lo que está legalmente establecido. Solo se pretende que se incluya la consideración sobre OI en la doctrina argentina, para poder entender el mundo que nos rodea, donde la construcciyn narrativa del conflicto se convierten en un "arma bondadosa"(Qiao y Wang, 2002) que podría significar una Revolución en Asuntos Militares, es decir una forma diferente de hacer la guerra.

PALABRAS CLAVE: Operaciones de Información (OI) - Capacidades Relacionadas con la Información (CRI) - Revolución en Asuntos Militares -Operaciones Militares.

TABLA DE CONTENIDO

INTRODUCCION

La frase Operaciones de Información (OI) aparece ahora con frecuencia en la literatura militar, y normalmente se la pasa por alto. Algunos lectores ponen énfasis en la palabra operación, entendiendo como tal toda actividad que implica el empleo de medios militares para el cumplimiento de una misión determinada (PC-00-02, Glosario de Términos de empleo militar para la Accion Militar Conjunta, 2015, pág. 155)

Otros lectores ponen énfasis en la palabra información, que por el uso y la costumbre llevaba al área de Inteligencia, donde en el ciclo de la inteligencia incluía la dirección del esfuerzo de reunión de información, la reunión de información, el proceso de la información y su difusión y uso. Estos lectores sostienen que con la frase OI, lo que se refiere es a lo que denominan gestión de la información, en el sentido de la acción y efecto de administrar información, ordenar, disponer y organizar. Subyacen en estos lectores la especialidad del área Inteligencia, en las actividades de reunión y discriminación de la información, de lo más urgente e importante a lo menos urgente e importante. A lo sumo, en los actuales escenarios de gran volumen y velocidad de la información, derivan en sistemas de inteligencia artificial que seleccionen de cantidad de información sin categorizar, suponiendo que solo las principales la que debe llegar al Comandante para que decida.

La principal dificultad es que en la doctrina argentina, no está definido en qué consistirían las OI. Esa frase no figura en el Glosario de Términos Conjuntos. Lo que está definido es el concepto de la Guerra Fría sobre Guerras de la Información.

Guerra de la información: Uso y manejo de la información con el objetivo de conseguir una ventaja competitiva sobre un oponente, pudiendo consistir en la recolección de información táctica, en la confirmación de la veracidad de la información propia, en la distribución de propaganda o desinformación a efectos de desmoralizar al enemigo, socavar la calidad de la información de la fuerza enemiga y negarle las oportunidades de recolección de información, pudiendo adquirir diversas formas. (PC-00-02, Glosario de Terminos de uso militar para la Acción Militar Conjunta, 2015, pág. 111/112)

Otras fuentes extranjeras consultadas definen lo que son las OI. Así, actualmente el Diccionario del Departamento de Defensa de Estados Unidos Ed 2012 las define como

Operaciones de Información — El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Información, en conjunto con otras líneas de operación para influenciar, interrumpir, corromper o usurpar el proceso de toma de decisiones de adversarios o potenciales adversarios mientras se protege a los propios (DoD Dictionary, 2020, pág. 104)[1]

Sin embargo, en las fuentes de Occidente, todavía no hay una definición unívoca de esta frase, como lo expresa el libro "Perceptions are reality" en su Capítulo8, (Perceptions are reality, 2018, pág. P. 134) cuando dice

Parte de la inconsistencia en la aplicación de las OI surge de una multitud de cambios doctrinales que llevan a una ausencia general de un entendimiento común de las Operaciones de Información en el Ejército [de Estados Unidos]. Desde el 2002 al presente, el Ejército [de Estados Unidos] cambió su definición de Operaciones de Información varias veces, incluyendo el período cuando el Ejército [de Estados Unidos] definió las Operaciones de Información como una actividad conjunta mientras el Ejército [de Estados Unidos] conducía "actividades e informaciyn e influencia".

En 1992, el experto estadounidense Martin Libicki las definía de otra manera, y la OTAN lo hacía en forma parecida. La diferencia sustancial parecería ser que en la definición de Guerra de la Información, se restringe a las acciones tácticas resultantes de una competencia en la obtención, difusión y uso de la información, y por lo tanto una responsabilidad del campo de inteligencia dentro del conocido ciclo de la inteligencia.

Como en la Argentina la definición imperante en la Guerra Fría era que Guerra de la Información consiste en el Uso y manejo de la información con el objetivo de conseguir una ventaja competitiva sobre un oponente, pudiendo consistir en la recolección de información táctica, en la confirmación de la veracidad de la información propia, en la distribución de propaganda o desinformación a efectos de desmoralizar al enemigo, socavar la calidad de la información de la fuerza enemiga y negarle las oportunidades de recolección de información, pudiendo adquirir diversas formas.(PC-00-02, Glosario de Términos de empleo militar para la Accion Militar Conjunta, 2015, pág. P. 111) se lo consideraba una acción propia del campo de inteligencia, y exclusiva de las operaciones convencionales. Sin embargo, el concepto

[1]En toda la investigación, si el texto original se encuentran en idioma inglés, ha sido traducidos por el autor de este trabajo. Original en inglés, traducción propia.

comenzó a modificarse porque si nos ajustamos a la categorización de Martin Libicki en 1992 de las acciones de las OI, las acciones de la guerra basada en inteligencia son solamente una parte de las OI. Así expresaba que las OI consistían en

> 1. Guerra de comando y control [C2W]; 2. Guerra basada en inteligencia [IBW]; 3. Guerra electrónica [EW]; 4. Operaciones psicológicas [PSYOPS]; 5. Ataques de hackers basados en software sobre los sistemas de información; 6. Guerra económica de información [IEW] guerra a través del control de la información de comercio; y 7. Ciberguerra [combate en el reino virtual]. (Libicki, 1995, pág. 18)[2]

En las averiguaciones realizadas surgió otro aspecto: si bien el nombre es el mismo, para Occidente (EEUU y la OTAN) en la teoría las OI son Operaciones Complementarias de las Operaciones Militares convencionales con medios cinéticos, en Rusia y conforme a la doctrina del General Gerasimov en los inicios del S XXI, las OI constituyen los medios principales no militares de preparación para obtener objetivos políticos, que se inician mucho antes en todos los campos del poder nacional sin que se esbozara el uso de medios militares convencionales cinéticos. O sea que para Occidente, las OI serían parte de la Estrategia Militar, y para Oriente, las OI son parte de las Estrategia General. Esto da lugar a las denominadas guerras híbridas, que aunque no son motivo de esta investigación, es necesario aclarar brevemente.

Las guerras híbridas son un nuevo modelo de guerra que tiene su particular interpretación según se trate de fuentes estadounidenses o rusas. Mientras que para Occidente las guerras hibridas son la mezcla de operaciones convencionales, operaciones no convencionales y operaciones de guerra no militares para obtener los objetivos políticos, para Rusia las guerras híbridas son una aproximación indirecta avanzada de los Estados Unidos para cambiar los regímenes de gobierno adeptos a Rusia, que reemplazan los antiguos golpes militares de la década del 70.(Korybko, Guerras Híbridas Revolución de Colores y Guerra No Convencional, 2015) En ese concepto, las guerras híbridas son las que llevarían a cabo Estados Unidos y la OTAN en contra de los intereses rusos, para avanzar su dominio a Occidente.

Para Occidente, decidido el uso de los medios militares cinéticos en operaciones de guerra, se deben emplear OI. Para Rusia, Estados Unidos ya está usando OI en todos

[2] Original en inglés, traducción propia.

los campos del poder, político, económico, psicosocial, tecnológico, mientras se reserva en el uso de los medios militares convencionales cinéticos (Korybko, Guerras Híbridas - Revolución de Colores y guerra no convencional, 2019). Sin embargo, a juzgar por los casos testigo donde se usaron Operaciones de Información (Estonia, Georgia, Crimea y Ucrania), los rusos usan las OI y las Fuerzas Especiales para preparar un ambiente favorable para emplear las fuerzas militares cinéticas. Nótese que aún en el caso de escenarios híbridos, las fuerzas militares cinéticas siguen siendo principales para someter la voluntad de un adversario.

Tampoco la frase guerra híbrida tiene aceptación universal. Mientras que en Oriente la mencionan, pero se refieren con mayor frecuencia a "conflictos en la zona gris", puesto que están entre la guerra y la paz, o "no lineales" porque es difícil identificar frentes, en Occidente y principalmente Estados Unidos, se sostiene que los conceptos en boga de "guerras asimétricas", "guerras híbridas" "conflictos no tradicionales" "guerra sin restricciones" son doctrinariamente pobres, y que lo único doctrinariamente definido para ellos es la insurgencia, dentro de la guerra no convencional y la guerra irregular. En la doctrina militar argentina la frase guerra hibrida está incluida en la PC 00-01 Doctrina Básica para la Acción Militar Conjunta (Proyecto) del 2018 (PC 00-01, Doctrina Basica para la Acción Militar Conjunta, 2018, pág. 27), pero no está desarrollada doctrinariamente. Es solo una transcripción de la definición expresada por el Teniente Coronel USMC Frank Hoffman en su artículo Hybrid Warfare and challenges, publicado en JFQ, Edición 52, primer cuatrimestre del 2009, P. 34. (Hoffman, 2009, pág. 34). Como ya se expresó, esta investigación no avanza en el tema de guerra híbrida en sus diferentes conceptos, ya que el tema por su naturaleza e importancia ameritaría una investigación adicional.

En cualquiera de los casos, estas operaciones en el ambiente de la información contribuyen directamente al éxito estratégico, operacional y táctico según sea la dirección estratégica, y respalda la obtención de los objetivos en todos los niveles. También deben proteger su propia toma de decisiones y la información que la alimenta. Si bien los términos diferenciados informar e influir en las actividades se ha dejado de lado, muchos de los principios continúan, especialmente la sincronización de las CRI. Estas son aquellas capacidades que generan efectos en y a través del ambiente de la información, pero estos efectos casi siempre se logran en combinación e integración con otras CRI. Solo a través de su sincronización eficaz y efectiva con las líneas de

operaciones físicas los comandantes podrían obtener una ventaja decisiva sobre los adversarios, las amenazas y los enemigos.

Como ya se expresó, la aparición de este nuevo ambiente o entorno de actuación que es el de la información divulgada por el espectro electromagnético y el espacio cibernético, se agrega a los dominios tradicionales físicos de aire, mar, tierra y espacio. Este dominio de la información tuvo un inusitado empuje por la asombrosa evolución de las Tecnologías de Información y Comunicaciones (TICs), y al parecer, esto hace a la diferencia de concepto entre Occidente y Oriente. El tema por resolver reside que la literatura militar y civil mundial se refiere a OI, y todavía se las confunde o se las considera sinónimo de Guerra de la Información que era el concepto que predominaba durante la Guerra Fría.

En esta investigación la línea de investigación principal es la postura de Occidente, por lo que la hipótesis a corroborar sería "El progreso de las TICs en la última década ha priorizado el uso de Operaciones de Información en todos los umbrales de la conducción por lo que ahora se ha hecho imprescindible integrarlas completamente con las operaciones militares convencionales cinéticas. "El título de esta investigación conduce a la concepción occidental, porque cuando se comenzó la investigación, se pensaba que era la única postura posible y la investigación efectuó otros hallazgos que abren camino a otras investigaciones.

Conforme a lo anticipado más arriba el objetivo general de esta investigación fue el determinar un concepto globalizador moderno de Operaciones de Información para que sea incluida en el Glosario de Términos Conjunto y así sean tenidas en cuenta en la doctrina militar argentina.

La demostración de esta hipótesis se implementó con objetivos de mayor especificidad, como i) un análisis de la evolución del concepto sobre Operaciones de Información: ii) una categorización tentativa de las Operaciones de Información teniendo en cuenta sus formas y propósitos particulares; iii) el uso del espacio cibernético para la aplicación de las Operaciones de Información en los actuales escenarios donde se priorizan las percepciones sociales, y iv) un estudio de casos de aplicación de estas OI en escenarios reales (Lituania, Georgia, Crimea, Ucrania).En consecuencia se van a desarrollar los siguientes capítulos 1 Antecedentes de las OI, 2 Los conceptos de OI en el mundo Occidental y Oriental, 3 La redes sociales y las TICs, y 4 Estudio de Casos donde se emplearon OI según fuentes occidentales.

En el primer capítulo tiene por finalidad determinar los antecedentes que precedieron al origen de la frase OI, expresión que tomó auge a fines del siglo XX. En el segundo capítulo, se determinará si la definición de la frase OI es de aceptación universal o si difieren según lo interpreten los contendientes. Este capítulo no estaba concebido inicialmente, pero al avanzar la investigación se encontró que las definiciones no eran únicas. En el tercer capítulo se verá la creación de realidades diferentes mediante las percepciones sociales, y el rol que en ello le cabe a lo que se denominan redes sociales. Luego, se tratarán los estudios de casos donde recientemente se emplearon Operaciones de Información, según las fuentes militares Occidentales.

Durante la investigación se siguió una línea exploratoria y descriptiva. Debe aclararse que no se pretende sentar bases doctrinarias sobre guerras híbridas, guerras irregulares y OI. Esta investigación no discute aspectos legales nacionales que acepten o rechacen esas nominaciones. Solamente se pretende que se entienda el significado de OI, que se ha tornado un punto de referencia en los conflictos luego de finalizada la Guerra Fría y en función del progreso geométrico desmesurado de las TICs.

Las OI es uno de los aspectos más consustanciados con el conflicto moderno y más integradores porque abarca diferentes dominios del quehacer humano de las fuerzas en operación con acciones tácticas concretas. Como se expresa en el último párrafo del libro "La Guerra sin Restricciones"[3], la clave de la guerra del futuro debe ser adecuada para todos los niveles y dimensiones, desde la política de guerra, la estrategia y las técnicas operacionales a las tácticas; y también debe ajustarse a las manos de los individuos, de los políticos y los generales, hasta a los soldados comunes.(Qiao y Wang, Unrestricted Warfare, 1999, pág. 191)

La globalización ha hecho al mundo más chico, aunque no más unido. Al parecer, en el Siglo XXI, todos los principios de la guerra se resumirán en uno solo: ustedes peleen con sus métodos, que nosotros pelearemos con los nuestros. En cuanto a las OI, tendría validez la séptima estratagema china que dice "Crea algo de la nada", es decir que cambie algo que no es sustancial o verdadero, en una realidad indiferente o amenazante. (McFate, The New Rules for War - Victory in the Age of Durable Disorder , 2019, pág. 190)

[3] Para los autores chinos QiaoLiang y Wang Xiangsui, la traducción correcta del chino al inglés es "La Guerra más allá de los Límites".

CAPITULO I: ANTECEDENTES DE LAS OPERACIONES DE INFORMACIÓN (OI)

El presente capítulo tiene por finalidad determinar los antecedentes que precedieron al origen de la frase Operaciones de Información, expresión que tomó auge a fines del siglo XX. El orden en que se expresarán los antecedentes es en nuestro país, en Latinoamérica, en Europa y en Estados Unidos.

Hay veces que los diccionarios incluyen el significado de frases, que sin ser expresiones idiomáticas, tienen un significado reconocido. La frase operaciones de información con un significado particular no figura en el Diccionario de la Real Academia Española, ni en el Oxford Concise Dictionary. Allí pueden encontrarse el significado aislado de cada una de las palabras, pero no unidas. Es por eso que se hizo necesario buscar las definiciones en las Fuerzas Armadas de otros países.

EN LA ARGENTINA

Para nuestro país, el primer punto de referencia fue la consulta a la PC 00-01 Doctrina Básica para la Acción Militar Conjunta Ed 2018, y la Publicación Conjunta PC 00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta. Ed 2015.

En la PC 00-01 Doctrina Básica para la Acción Militar Conjunta, la palabra información se encuentra mencionada en el Capítulo 5 La Conducción, Sección 2. La Inteligencia Militar. (PC 00-01, Doctrina Básica para la Acción Militar Conjunta, 2018, págs. 63, puntos 9 y 11) No obstante, la frase operaciones de información, no aparece mencionada. En la PC 00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta Ed 2015, se lee que espionaje es una operación de inteligencia militar ofensiva (PC-00-02, Glosario de Terminos para la Acción Militar Conjunta, 2015, pág. 90), cuatro conceptos sobre información, en el cual el primero aclara entre paréntesis que se trata de Inteligencia (PC-00-02, Glosario de Terminos para la Acción Militar Conjunta, 2015, pág. 119) y 26 conceptos de la palabra operaciones con adjetivos que le dan especificidad, (PC-00-02, Glosario de Terminos para la Acción Militar Conjunta, 2015, pág. 155 a 159) , donde referido al tema que nos ocupa podrían asociarse Operaciones de Inteligencia Militar (PC-00-02, Glosario de Terminos para la Acción Militar Conjunta, 2015, pág. 158) que son las que se llevan a cabo para obtener

información, Guerra de Información que es el uso y manejo de la información con el objetivo de conseguir una ventaja competitiva sobre un oponente (PC-00-02, Glosario de Terminos para la Acción Militar Conjunta, 2015, pág. 111) y Operaciones Psicológicas que es el empleo planificado de la propaganda y la acción psicológica orientadas a direccionar conductas del adversario (PC-00-02, Glosario de Terminos para la Acción Militar Conjunta, 2015, pág. 159), donde se aclara que se realizan en tiempo de conflicto bélico. También pueden encontrarse definiciones sobre Guerra Electrónica que es la que se lleva a cabo dentro de los espectros de radiaciones electromagnéticas y acústicas, (Ibídem: P. 112), Guerra Electrónica de Comunicaciones que trata de la guerra electrónica sobre las trasmisiones de comunicaciones (Ibídem: P 112) y Guerra Electrónica de No Comunicaciones que trata de guerra electrónica aplicada a la porción del espectro electromagnético normalmente utilizado por las emisiones de sensores, sistemas de guiado, armas y cualquier otro tipo de emisión distinta a las de comunicaciones. (Ibídem: P 112)

El primer inconveniente por salvar fue el de las definiciones. En la PC 00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta, no se define Operaciones de Información. Además, se conceptualiza ámbito como sinónimo de ambiente, pero dominio trata únicamente del control de los espacios. Aunque debiera aparecer en la PC 00-01 Doctrina Básica para la Acción Militar Conjunta Ed 2018, no se expresa el concepto básico que la acción militar conjunta tiene lugar en el ambiente militar, es decir los dominios de aire, mar, tierra, y espacio (en la Argentina se agrega aeroespacio, al que el Glosario define como Ámbito que refiere al conjunto del espacio aéreo y el espacio exterior. (PC-00-02, Glosario de Términos de empleo militar para la Accion Militar Conjunta, 2015, pág. 10). El ambiente de la información fue agregado por EEUU y la OTAN en el año 2018 e incluye el espacio cibernético, las operaciones convencionales especiales, los misiles balísticos, la guerra electrónica y las capacidades espaciales. (JP 3-0 Joint Operations, 2018, pág. I 3). En la doctrina argentina, se hace una referencia lateral a esta distinción cuando en la PC 00-01 Doctrina Básica para la Acción Militar Conjunta, en el párrafo 2.11.1 Conflicto armado en ambiente convencional/regular, se expresa que las operaciones militares de fuerzas militares contra fuerzas militares se lleva a cabo "…en los diferentes ámbitos/dominios: aéreo, marítimo, terrestre, espacial y ciberespacial." (PC 00-01, Doctrina Basica para la Acción Militar Conjunta, 2018, pág. 26).

Mientras en la Argentina se toma como sinónimo ámbito y ambiente, y dominio con acepción de control, la opinión general distingue el aire, mar tierra y espacio como dominios físicos, y la información se considera un ambiente que influye en esos dominios físicos. Si no se entiende así, es difícil averiguar sobre la muy mencionada frase operaciones de multidominio, que no es motivo de esta investigación.

La frase de Operaciones de Información (OI) que hoy se lee en tantas publicaciones y manuales extranjeros, no aparece en la PC 00-02 Glosario de Términos de empleo militar para la AMC Ed 2015, ni en la PC 00-01 Doctrina Básica para la Acción Militar Conjunta Ed 2018. Tampoco se menciona nada en la PC 00-01 acerca de las funciones conjuntas que definen como

> Las funciones conjuntas son actividades y capacidades relacionadas agrupadas para ayudar al Comandante de Fuerzas Conjuntas a integrar, sincronizar y dirigir operaciones conjuntas. Las funciones comunes a las operaciones conjuntas en todos los niveles de guerra están en siete grupos básicos - C2, información, fuego, maniobra y movimientos, protección y sostenimiento. (JP 3 - 0 Change 1 Joint Operations, 2018, págs. Cap III P. III-1)[4]

Al no estar definidas en la doctrina básica para la acción militar conjunta argentina las funciones conjuntas, se hace difícil diferenciar la función conjunta inteligencia de la función conjunta información. Desde el punto de vista sistémico, una función es la tarea que lleva a cabo una parte de un sistema, para permitir el funcionamiento sincronizado de las otras partes de ese sistema. No es la forma en que es definido en la PC 00-02 Glosario de Términos de Empleo militar para la AMC, que dice que función es la responsabilidad asignada a un individuo, cargo u organización. Con esta definición, función podría tomarse como sinónimo de misión, y la opinión generalizada es que debe tomarse como misión secundaria.

Es así que en la lectura superficial, instintivamente, debido al vocablo información, todo lector argentino presupone que se trata de actividades de inteligencia, de manera tal que lo considera un asunto conocido y lo pasa por alto. Esta asociación instintiva entre Operaciones de Información y el área de Inteligencia es la más difícil de

[4] Original en inglés, traducción propia.

argumentar, porque hay resistencia natural en aceptar el carácter ecléctico de las Operaciones de Información.

En los conceptos con los que se estudiaba historia militar en el siglo XX, por guerra de la información se pensaba en operaciones convencionales, en las actividades de inteligencia de espionaje, en desciframiento de claves, en obtención de secretos del enemigo mediante espías, la radio interceptación y escucha de comunicaciones a la que se denominaba guerra electrónica, la propaganda y en la acción psicológica para influir en los comportamientos tanto propios como del enemigo. También se asociaba inteligencia con el engaño militar de operaciones de velo y engaño, aunque no eran actividades del campo de inteligencia sino, como su nombre lo indica, del campo de operaciones. Debido al surgimiento y avance en las comunicaciones radioeléctricas, otras acciones como la guerra electrónica recién se hicieron importantes en la II GM.

En conclusión, la frase Operaciones de Información (OI) no se encuentra definida en la doctrina argentina. Este hecho fue notado en la Contribución Académica de la ESGC titulada Operaciones Militares Cibernéticas Planeamiento y Ejecución en el Nivel Operacional, donde dice

> Las OI no están catalogadas en la República Argentina. Como el modelo de la administración gubernamental durante el periodo 2003/2013 implementó la absoluta veda de los militares en el marco interno, y se restringió el accionar militar al "enemigo militar estatal externo", en conformidad con ello se prohibieron las OI dado que el supuesto básico era que ningún país iba a atacar a la Argentina.(Trama y otros, Las operaciones Cibernéticas, Planeamiento y ejecución en el nivel operacional, 2018, pág. 215)

La causa de esta omisión en la Argentina no está bien definida, pero se supone y coincide con lo que dice esta investigación, que es una consecuencia de la división seguridad interna/defensa externa establecida por la reglamentación de la Ley de Defensa por Decreto 727/2006 Reglamentación de la Ley de Defensa Nacional.

Por la Resolución Ministerial 381/06, del 19 de Abril del 2006, en su Artículo 17 se estableció que

> ARTÍCULO 17°: En función de lo estipulado en las Leyes N° 23.554 de "Defensa Nacional", N° 24.059 de "Seguridad Interior" y N° 25.520 de

> "Inteligencia Nacional", los organismos de inteligencia pertenecientes al ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS y a los ESTADOS MAYORES GENERALES del EJÉRCITO, la ARMADA y la FUERZA AÉREA, no podrán realizar ningún tipo de actividad o de apoyo a la actividad conocida según la doctrina vigente como "Acciyn Psicolygica" o cualquiera otra de tales características, cualquiera fuera la denominación que reciban.

Según la Ley de Inteligencia que se ajustaba al pensamiento estratégico militar del poder político a cargo en esos momentos, las Fuerzas Armadas tenían una concepción estratégica defensiva, y para defenderse de la agresión militar externa de otros Estados, por lo que las conocidas como Actividades Especiales de Inteligencia (Espionaje, Sabotaje y Subversión) les estaban vedadas. Asimismo, como las Fuerzas Armadas no tenían jurisdicción fronteras adentro, las actividades de Contrainteligencia (contra espionaje, contra sabotaje y contra subversión) también les estaban legalmente prohibidas.

En el contexto de OI, la palabra información, no se refiere al antiguo Ciclo de la Inteligencia, ni al campo de la conducción 2 Inteligencia, sino que se trata de la gestión de la información en las restantes funciones conjuntas (C2, Maniobra y movimiento, fuegos, protección, sostenimiento, inteligencia e información), operaciones que se conducen como una función conjunta. Las OI son capacidades integradas que afectan disciplinas que Occidente tradicionalmente ha considerado como desconectadas (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 80).Las OI son operaciones que buscan efectos, se conducen y se gestionan: no consisten únicamente en recopilar información sobre un enemigo, o un terreno, sino que además, afecta a todos los componentes del poder civil y militar del adversario influyendo con desinformación y propaganda para buscar una ventaja en la obtención de objetivos políticos y militares. Las OI no son exactamente operaciones cibernéticas, no son exactamente guerra electrónica, no son solamente inteligencia, sino una integración efectiva de todas esas capacidades con medidas cinéticas para crear el efecto que quieren lograr sus comandantes. Las OI son eclécticas por naturaleza (Cyberpower and National Security, 2013, pág. Chapter 12)

A lo sumo los especialistas de inteligencia argentinos más avanzados conceden que con los adelantos en tecnología que permitieron la información en tiempo real

permite tomar decisiones más rápidas, y eso ha hecho que la tradicional pirámide jerárquica militar se achate ya que todos los niveles (estratégicos y tácticos) tienen conocimiento de la información al mismo tiempo. Así nacieron las organizaciones en red. Además, el volumen de la información se ha multiplicado, y es más difícil discriminar lo urgente de lo importante, y la veracidad y confiabilidad de la fuente. Por eso, se recurre a la inteligencia artificial para que discrimine la información. En suma, esta transformación de las TICs ha dado origen a las organizaciones en red, que requieren la aplicación de la iniciativa de quienes la integran, puesto que las grandes debilidades humanas de las organizaciones piramidales jerárquicas quedaron al descubierto: órdenes que llegaban tarde, propuestas que llegaban deformadas, demora en las decisiones y aversión al riesgo. En suma, la frase OI en el concepto que consiste en el tratamiento de los sistemas de información para influir y desinformar creando un ambiente propicio en la opinión para llevar a cabo las restantes funciones conjuntas, en la doctrina argentina no está definida todavía.

EN OTROS PAÍSES IBEROAMERICANOS

En Brasil, el Ejército de Brasil editó el reglamento referente a las Operaciones de Información (EB 20 - MC - 10.213) del año 2014, que define la actividad como:

> La actuación metodológicamente integrada de Capacidades Relacionadas con la Información, en conjunto con otros vectores, para informar e influenciar grupos y personas, así como también para afectar el proceso de toma de decisiones del adversario, protegiendo al mismo tiempo el propio. Sumado a esto, tienen que evitar, impedir o neutralizar los efectos de las acciones adversas en la dimensión informacional.(Ministerio da Defensa Brasil, 2014, págs. 3-1)[5]

En la encuesta al Coronel EB Moacyr Couto Junior, el encuestado respondió que las OI en Brasil son doctrinarias, aclarando que[6]

> En la doctrina brasileña, las operaciones de información (OpInfo) consisten en coordinar el empleo de capacidades integradas relacionadas con la información, en contribución a otras operaciones o incluso constituir el esfuerzo

[5] Original en portugués, traducción propia.

[6] Las citas son textuales.

principal, para informar e influir en las personas o grupos hostiles, neutrales o favorables, capaces de impactar positiva o negativamente con la finalidad de alcanzar objetivos políticos y militares, así como comprometer el proceso de toma de decisiones de los oponentes o potenciales oponentes, garantizando al mismo tiempo la integridad de nuestro proceso.

La OpInfo contribuye en gran medida a obtener la superioridad de la Información, que se caracteriza por el alcance de la ventaja, persistente o transitoria, resultante de la capacidad de brindar información útil a los usuarios interesados e interesados, en el momento adecuado y en el formato adecuado, negando la oponente las oportunidades para lograrlo.

Además, las operaciones de información se planifican y realizan a nivel estratégico, operativo (sic) y táctico en situaciones de guerra y no guerra. En el Nivel Estratégico, las OpInfo se diseñan en el marco de acciones estratégicas, las cuales se guían por condiciones y lineamientos políticos. Estas acciones pueden resultar de demandas u oportunidades relacionadas con el entorno interno y externo del país.

Agregó el CR EB Moacyr que los aspectos doctrinarios de las OI se encuentran volcados en las siguientes publicaciones

En el ámbito del Ministerio de Defensa, las operaciones de informaciones están reglamentadas en la reciente publicación MD30-M-01 - "DOUTRINA DE OPERAÇ®ES CONJUNTAS" - (2ª Edição/2020), de 15 de Septiembre de 2020, en los volúmenes 1 y 2.

En el ámbito de las fuerzas armadas por separado, el Ejército Brasileiro publicó el EB70-MC-10.213 "OPERAÇ®ES DE INFORMAÇÃO" (2ª Edição/2019), que trata sobre la temática

Respecto a la relación entre el espacio cibernético y las OI, el encuestado expresó que:

Las Capacidades Relacionadas a las Operaciones de Información, según la visión brasileña, son: Operaciones Psicológicas, Acciones de Guerra Electrónica, Ciberdefensa, Comunicación Social y Asuntos Civiles.

Con respecto específico a la cibernética, ninguno de los principales documentos de defensa del país, como el Libro Blanco de la Defensa, la Política

Nacional de Defensa y la Estratégica Nacional de Defensa, que están en vigor desde 2012, no citan la relación de la cibernética con las Operaciones de Información. Tampoco, la reciente revisión de los citados documentos encaminada, en junio de este año, para el Congreso Nacional para aprobación también no incluyó la presente temática.

Sin embargo, el documento doctrinario MD31-M-07, "DOUTRINA MILITAR DE DEFESA CIBERNÉTICA - (1ª Edição/2014), en el capítulo IV, aborda la participación de la Cibernética en el contexto de las Operaciones de Información en el ámbito del Estado Mayor Conjunto.

El 23 de Junio de 2021 se escuchó mediante el recursos Google Meet la charla que pronunció el Coronel EB Marcio Saldanha Walker para el Curso de Estrategia Militar y Conducción Superior de la Escuela Superior de Guerra Conjunta de la República Argentina, sobre las Operaciones de Información en el Brasil. El Coronel Walker es maestrando de esta Maestría en Estrategia Militar en la República Argentina, es Bachiller en ciencias militares por la Academia Militar de las Agujas Negras, es oficial de Mando y Estado Mayor llevado a cabo en la Escuela del mismo nombre, tiene un postgrado en Psicopedagogía, en Universidad Federal del Rio de Janeiro; tiene también una maestría en Operaciones Militares, posee un doctorado en Ciencias Militares, por la Escuela de Mando y Estado Mayor, en el tema operaciones de información conjuntas; y ha realizado el Curso de Derecho Internacional Humanitario en la Escuela Superior de Guerra del Brasil

El Coronel EB Walker se desempeñó como analista en operaciones de información en el Comando Militar del Sur, (2011.2013), como analista en operaciones de información en el Comando de Operaciones terrestres (2017-2018); y Especialista de Operaciones de Información en el planeamiento del ejercicio multinacional PANAMAX 2018. En la parte de Encuestas y Entrevistas, de adjunta un resumen de su ponencia en el tema Operaciones de Información.

En la República de Ecuador, en julio de 2014, mediante la Resolución Nro. 14 de la DIEDMIL D-003, el Jefe del Comando Conjunto de las Fuerzas Armadas promulgy el "Manual de Operaciones de Informaciyn", que las define como

> …el empleo integrado de las capacidades principales y de apoyo que se desarrollan en los procesos de Operaciones de Información aplicables a las

> amenazas propias con lo que es coherente con los procesos de restructuración de las Fuerzas Armadas, y que se detallan a continuación: 1. Capacidades Principales: - Operaciones Psicológicas - Operaciones de Decepción y Engaño - Telecomunicaciones y Guerra Electrónica - Seguridad en las Operaciones (Ciberseguridad) 2. Capacidades de Apoyo: - Inteligencia para Operaciones de Información 3. Capacidades Relacionadas: - Comunicación social.(Comando Conjunto FFAA del Ecuador, 2014)

Conforme a la información obtenida por correo electrónico con el General del Ejército del Ecuador Edwin Bolívar Mena Villamarín, profesor de la Academia de Guerra del Ejército Ecuatoriano, de fecha 18 de Enero de 2021, ese manual no está actualizado y en el Comando Conjunto de las Fuerzas Armadas de Ecuador hay un grupo de oficiales trabajando en esa tarea. Hasta el momento hay un artículo todavía inédito de autoría del Teniente Coronel Christian Regalado Davila, que sería publicado en la revista del Comando Conjunto (COMACO) en el mes de Febrero del corriente año 2021.

Aparte de Brasil y Ecuador, el restante país latinoamericano que podría tener referencias al concepto moderno de OI es Colombia. Los restantes países iberoamericanos no lo tienen considerado en su doctrina.

Se han diligenciado cuestionarios a oficiales superiores de otros países que revistan en el año 2020 en el Curso de Estrategia Militar y Conducción Superior de la Escuela Superior de Guerra Conjunta, para determinar el grado de conocimiento en la temática. Las encuestas de opinión y la entrevista se adjuntan al final de la presente tesis.

EN EUROPA

La OTAN define Operaciones de Información (AJP 3-10, 2009, págs. punto 1007 P. 1-3) diciendo

> a. Las operaciones de información es una función militar para proporcionar asesoramiento y coordinación de actividades de información militar con el fin de crear los efectos deseados en la voluntad, la comprensión y la capacidad de los adversarios, adversarios potenciales y otras partes aprobadas por el National Atlantic Council (NAC) en apoyo de los objetivos de la misión de la Alianza.

b. Las actividades de información son acciones diseñadas para afectar la información o los sistemas de información. Pueden ser realizados por cualquier actor e incluyen medidas de protección.[7]

Sin embargo, como se verá más adelante, al estudiar la postura de Europa respecto a la definición de Operaciones de Información, surgió que Rusia y China tienen un concepto que no es igual al imperante en Occidente.

EN LOS ESTADOS UNIDOS DE NORTEAMÉRICA

Es en este país donde se encuentra la mayor cantidad de tratamiento de la problemática. El antecedente más lejano encontrado es un libro de un experto de Estados Unidos llamado Martin Libicki, de la Universidad de Defensa de EEUU, que en su obra "What is Information Warfare", de 1995, dice que en 1992 la definición era

> …MOP [Memorandum of Politics]-30 (Kuehl, 2000), que se está revisando actualmente, corta en rebanadas la guerra de información a las unidades operacionales. Limitado a las operaciones militares, cubre "el uso integrado de las operaciones de seguridad, engaño militar, operaciones psicológicas, guerra electrónica y destrucción física, con el apoyo mutuo de la inteligencia, para negar información, influir, degradar o destruir las capacidades adversarias de C2 mientras protege a las propias capacidades C2 contra tales acciones "(Libicki, 1995, pág. 30)[8]

En la obra de Libicki, editada en 1995, se describe lo que llama OI en ese momento. En esta obra, el autor se pregunta si las OI son simplemente una característica actualizada de una forma de hacer la guerra. También se pregunta si se trata de una nueva forma de conflicto en la infraestructura global de la informaciyn, "cuyo origen descansa en el cerebro humano pero que la era de la información le ha dado una vida nueva". (Libicki, 1995, pág. passim).

En las Fuerzas Armadas de Estados Unidos, en 1993 el Presidente de la Junta de Jefes de Estado Mayor emitió un Memorándum de Política (MOP) 30, que estableció un conjunto de definiciones y relaciones que guiaban a la Comunidad Conjunta para pensar en los conceptos relacionados de guerra de información y guerras de comando y control.

[7] Original en inglés, traducción propia.

[8] Original en inglés, traducción propia.

No obstante, como a la fecha de la publicación de su obra Libicki no encontró definiciones formadas, propuso las siguientes categorías para lo que denominó operaciones de información:

> Guerra de comando y control [C2W]; 2. Guerra basada en inteligencia [IBW]; 3. Guerra electrónica [EW]; 4. Operaciones psicológicas [PSYOPS]; 5. Ataques de hackers basados en software sobre los sistemas de información; 6. Guerra económica de información [IEW] guerra a través del control de la información de comercio; y 7. Ciberguerra [combate en el reino virtual].(Libicki, 1995, pág. 18)[9]

Martin Libicki sostenía que en las guerras por el comando y control (C2W), durante la Guerra Fría se las definía como la estrategia militar que implementaba la Guerra por la Información, que era de responsabilidad exclusiva de la comunidad de Inteligencia. . Frecuentemente - dice - las operaciones exitosas contra el Comando y Control son calificadas como la causa principal de la derrota de las fuerzas convencionales. Es una práctica antigua la de eliminar al comandante o jefe, como ocurrió en los tiempos bíblicos con Holofernes y Judith, el asesinato de Cesar, la emboscada y muerte del almirante Yamamoto, Saddam Hussein, y más recientemente la muerte de Osama Bin Laden en Pakistán y de Qasem Solimani en Irak. Actualmente, es más fácil y sencillo ubicar puestos de comando que ubicar líderes, cuyas ubicaciones geográficas permanecen cambiando. Hoy, no solamente el ataque con armas cinéticas satisface la necesidad de eliminación de los puestos de comando. También rinden buenos resultados el corte de energía eléctrica, la interferencia electromagnética o los virus de las computadoras. También es útil destruir los nodos de comunicaciones entre Puestos de Comando. Sin embargo - agrega - la experiencia muestra que casi siempre los Puestos de Comando encuentran vías alternativas de ejercer el comando, aun empleando estructura de comunicaciones de empresas privadas en la zona.

En las guerras basadas en la inteligencia ofensiva y defensiva, Libicki distingue el aporte de los sensores. A medida que la tecnología haga que los sensores se vuelven más agudos y confiables, a medida que proliferan en tipo y número, y se vuelven

[9]Original en inglés, traducción propia.

capaces de alimentar sistemas de control en tiempo real o casi en tiempo real, la tarea de desarrollar, mantener y explotar sistemas que detectan, evalúa e informan los resultados a los medios empeñados asumen una creciente importancia. Los sistemas de información con arquitectura mixta de sensores son difíciles de interceptar, porque se aplica el dicho que la mejor manera de ocultar un árbol es dentro de un bosque y no detrás de un muro. Dejando de lado los entornos abiertos, Libicki sostiene no queda claro todavía si los buscadores de alta tecnología saldrán triunfantes sobre los escondites de baja tecnología.

En las operaciones de información en la forma que son categorizadas por Libicki, la tercera es la guerra electrónica, en sus dos formas; radioeléctricas o criptográficas y por lo tanto, se trata del reino de las comunicaciones. La tendencia tecnológica va hacia los bits y los bytes. Una gran parte de la guerra electrónica va hacia los radares, ya sea de búsqueda y de seguimiento de blancos. Los radares generan frecuencias, graban firmas acústicas, que pueden ser interferidas y sus emisiones pueden ser usadas para destruir el radar con misiles antirradar. Las medidas electrónicas contra las comunicaciones son más fáciles de llevar a cabo que contra las no- comunicaciones, como los radares. También una de las tareas de la guerra electrónica es ubicar geográficamente a los emisores de señales.

En cuanto a la criptografía, se ha vuelto más dificultosa con la digitalización. No es que no se puedan descifrar claves, ocurre que puede llegar a demandar mucho tiempo y se debe enfrentar la suplantación de identidad - en inglés spoofing - aunque a cada momento surgen nuevas formas de atacar mediante spoofing, y otras contra- técnicas para evitarlo mediante certificados de identidad. No es propósito de este ensayo profundizar en esos aspectos técnicos.

La cuarta forma de las OI en operaciones convencionales, según la opinión de Libicki en 1995, es la guerra psicológica y aquí el esfuerzo es dirigido contra la mente humana, antes que contra el apoyo de computadoras. La acción psicológica para modificar comportamientos basándose en el miedo o en la confusión, es muy antigua en la historia de la humanidad. Esta acción psicológica adopta la forma de amenaza creíble, o de consecuencias desagradables de persistir en la oposición, y puede ser dirigida contra Estados, contra organizaciones o contra individuos. Desde el mismo momento en que los videos y las comunicaciones telefónicas pudieron ser editados, cortando parte de la información e introduciendo otra, la acción psicológica ha tomado renovados

impulsos. Lo más peligroso de la acción psicológica es ignorar su existencia: un desfile militar poderoso no sería otra cosa que una acción psicológica disuasoria ejercida sobre un Estado con intereses contrapuestos. Una sociedad que rechaza las bajas de combate de sus soldados, puede ser un blanco de interés en una acción psicológica apuntada a debilitar el deseo nacional de lucha.

Según Libicki, ya en 1995 categorizaba una quinta forma de OI a la que llamaba guerra de hackers. Una descripción pormenorizada de las acciones de los hackers se encuentra en la contribución académica de la ESGC Las Operaciones Militares Cibernéticas - Planeamiento y Ejecución en el Nivel Operacional, (Trama y otros, Las operaciones Cibernéticas, Planeamiento y ejecución en el nivel operacional, 2018) en su Capítulo VI. El empleo de las capacidades cibernéticas en apoyo de las operaciones de información.(Trama y otros, Las operaciones Cibernéticas, Planeamiento y ejecución en el nivel operacional, 2018). Los ataques de los hackers pueden ser hechos sobre el comando y control militares, o sobre objetivos civiles. Los ataques sobre objetivos civiles también podrían ser catalogados en apoyo de operaciones no convencionales. Los intentos de un ataque pueden ir de parálisis de sistemas por saturación de dominios, robo de información, fraude con pagos de servicios, fuente de recolección de inteligencia y cualquier otro propósito delictivo. Es de notar que también existen hackers patrióticos, cuya acción está dirigida por propósitos idealistas. Entre las herramientas más conocidas están los virus, las bombas lógicas, los troyanos, los sniffers y los encriptadores de archivos oransomeware. Las dificultades de estos ataques de hackers como operaciones de información residen en que no hay clara separación entre lo que es ataque y lo que es defensa, y que los escenarios son muy volátiles, ya que aparecen y desaparecen con rapidez. Habiéndose dicho todo, la guerra de hackers parece ser un problema que no lo es hasta que se manifieste, pero que será de corto plazo porque pronto deja de serlo.

Finalmente, Libicki sostenía que las ciberguerras pueden servir a las operaciones convencionales porque los sistemas necesarios para la vida diaria están tan informatizados que su anulación o interrupción pueden causar daños de mucha importancia a una fuerza militar, mayores a los que se podrían causar usando el armamento cinético convencional.

Para Libicki en 1995, donde aún las computadoras se comunicaban por modem de tono telefónico, y recién se expandía al uso común la World Wide Web, ciertos

aspectos de las operaciones de información eran antiguos, como ataques al comando y control, los engaños de todo tipo y las operaciones psicológicas. Otros, como la guerra electrónica, se hicieron importantes en la Segunda Guerra Mundial. Sin embargo, lo que Libicki describe como iniciación es las automatizaciones de los Centros de Comando por invasión de la tecnología, donde de la vulnerabilidad a las armas convencionales se pasó a la vulnerabilidad de un software malicioso; también se da cuenta de la importancia y frecuencia creciente de los piratas informáticos contra los sistemas civiles; las guerras de información económica y la guerra cibernética aprecia que se verían aumentadas y transformadas, y concluye que "con la guerra de información que abarca tantas actividades dispares, pocas generalizaciones cubren todo el campo". Como se verá más adelante en esta investigación, estas predicciones de 1995 quedaron superadas por la realidad del 2019.

Sin embargo, no había consenso en la definición de esta frase OI. Según Mark Vetulli, esta frase es uno de los términos más mal entendidos y mal usados en el Ejército de Estados Unidos (Perceptions are Reality, 2018, pág. P. xi) y eso se debe a múltiples cambios que emergieron del concepto C2 (Comando y Control) de hace más de 25 años. El autor Mark Vertuli escribe en el año 2018, y dice que en los últimos 11 años, esa definición de OI cambió tres veces,

> desde un enfoque en cinco capacidades centrales hasta la participación en la información (2007), para informar e influir en las actividades (2011), hasta su encarnación actual centrada en las Capacidades Relacionadas con la Información (2016).(Perceptions are Reality, 2018, pág. P. xi)

En el FM 3-0 Operations, del Ejército de Estados Unidos Año 2008 con cambios del 2011, en el Capítulo 6 acerca de la aplicación de la ciencia del control, se habla de la conducción de la administración del conocimiento y administración de la información. En el punto 6-88 se trata de la conducción de las actividades ciber /electro magnéticas de información e influencia y se diferencia claramente lo que es información de lo que es influencia. Mientras las actividades de información proporcionan información a audiencias internas y externas para describir con exactitud las operaciones, las actividades de influencia buscan efectivamente cambiar actitudes, creencias y comportamientos de audiencias propias, neutrales, adversarias y enemigas, para apoyar las operaciones.(FM 3-0 Operations, 2011 Change 1, 2011, pág. Cap 6)

Esta definición parece ser la más comprensible. Sin embargo y como ya se ha expresado, la definición que se sostiene hoy en las Fuerzas Armadas de Estados Unidos conforme al Diccionario del Departamento de Defensa de Estados Unidos del año 2020, que se expresara más arriba y que dice

> Operaciones de información (OI) — El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Información, en conjunto con otras líneas de operación para influenciar, interrumpir, corromper o usurpar el proceso de toma de decisiones de adversarios o potenciales adversarios mientras se protege a los propios. También denominados OI. Vea también Guerra electrónica; engaño militar; operaciones de seguridad; apoyo de información militar a las operaciones(DoD, 2020, pág. 104)[10]

Esta definición es la adoptada por la mayoría de los países occidentales que se han dado cuenta de este nuevo ambiente de actuación, que se suma a los tradicionales dominios de aire, mar, tierra, espacio y ciberespacial (el ambiente de la información dividido en el espacio electromagnético y el espacio cibernético) (PC 00-01, Doctrina Basica para la Acción Militar Conjunta, 2018, pág. P.26).

El término original anterior a 1995 de "Guerra de la Informaciyn" se desarrolly más en el sentido de lucha entre sistemas de toma de decisiones, y se extendió a la guerra electrónica, la guerra cibernética, la seguridad en la información y las operaciones de sistemas de computadoras en red.(Qiao y Wang, 2002, pág. 21) El concepto de OI, en cambio, incluye no solamente el uso de tecnología, sino también los aspectos humanos relacionados con el uso de la información, como las redes sociales, los proceso de toma de decisiones y aspectos del Comando y Control propios y del adversario. Como se expresa arriba en el año 2018, la información fue incluida en las Fuerzas Armadas de Estado Unidos como la quinta dimensión de las operaciones, que al describir el ambiente estratégico se agregó a los dominios de aire-mar-tierra y espacio.

> ….los dominios físicos de la tierra, el mar, el aire y el espacio; y el ambiente de información (que incluye el ciberespacio), así como el espectro electromagnético (EMS), e involucran operaciones convencionales, especiales, misiles balísticos,

[10] Original en inglés, traducción propia.

> guerra electrónica (EW), información, ataque, ciberespacio y capacidades espaciales.(JP 3 - 0 Change 1 Joint Operations, 2018, pág. I 3)[11]

Por una cuestión de terminología que no avanza tan rápido como los hechos, se denominan OI tanto a las del nivel táctico como las del nivel operacional, y aunque la diferencia es clara, causa confusión: mientras que en el nivel táctico se trata de hechos que por sus efectos influencian los enfrentamientos, en el nivel operacional, serían las líneas de operaciones lógicas que apoyan la conquista de los puntos decisivos de las líneas de operaciones físicas. Estas líneas de OI al ser una función conjunta, deben estar integradas, sincronizadas y concebidas por los comandantes conjuntos desde el inicio de las líneas de operaciones físicas. El concepto base es que las OI son, en esencia, operaciones centradas en el adversario / enemigo que se llevan a cabo para obtener una ventaja relativa para los tomadores de decisiones propios.(Perceptions are reality, 2018, pág. xii)

Nótese que hasta 1995 las OI eran operaciones complementarias a las operaciones militares básicas. Sin embargo, un hito importante ocurrió durante la Guerra del Golfo I, donde quedó claro que una de las CRI, los medios de presa, habían pasado de ser una forma de informar o desinformar, a constituirse en un elemento de comando más. Durante la Guerra del Golfo de 1991 ya se comentaba en Unrestricted Warfare la necesidad del General Schwarptkoft de engañar al líder iraquí Saddam Hussein, sobre la hora de iniciación del ataque, y para ello contó con la complicidad de la prensa, que como señalan los coroneles Qiao y Wang, no solo difundían hechos no verídicos, sino que le cerraban los micrófonos a Saddam, y le negaban la posibilidad de difundir las razones de su resistencia.

> El día anterior al inicio de "Tormenta del Desierto", los medios de comunicación occidentales volvieron a pregonar la noticia de una flota de portaaviones pasaba por el Canal de Suez, que sirvió para confundir a Saddam y hacerle creer que, ante la inminencia del desastre, las fuerzas estadounidenses todavía no habían completado su despliegue.(Qiao y Wang, 2002, pág. 60)[12]

También, se usó la difusión sobre lo inexorable de las acciones militares, y la dispersión de volantes a las tropas iraquíes incitándolos a la rendición. Este concepto de

[11] Original en inglés, traducción propia.

[12] Original en inglés, traducción propia.

OI también implicaba censura a la prensa, y de allí la necesidad de controlar a los periodistas que podían difundir inadvertidamente datos útiles para el enemigo, o cuidar los textos de las entrevistas periodísticos que podían revelar los propios planes e intenciones, como el plan de maniobra, o la ubicación de la División 101 que llevaría el rodeo al flanco iraquí. Tal cual figuran en el libro Autobiografía, del General Schwarptkoft, pueden leerse varios ejemplos de la influencia de los medios en las operaciones. (Schwarptfoft, 1994, pág. 370/409/423/452/459/460/ 468/500)

Lo innovador en la Guerra del Golfo I fue que los medios de información excedieron el viejo rol secundario de propaganda, para ser parte de los medios de conducción de las operaciones, un campo más donde debía ejercerse el comando. No obstante, hasta ese momento - 1991 - las OI continuaban siendo complementarias de las operaciones militares convencionales.

Para concluir, sería acertado reproducir un párrafo de la Introducción del Coronel Mark Venturi al libro Perceptions are reality, cuando dice:

> Todo es acerca de la información. Los líderes visualizan y entienden el ambiente operacional mediante la información. Como un elemento del poder de combate, la información permite la toma de decisiones, y su trasmisión ayuda decisivamente a las operaciones. Hoy la tecnología moderna ha incrementado significativamente la velocidad, el volumen y el acceso a la información. (Perceptions are reality, 2018, pág. xii)

Lo que parece surgir con énfasis de los antecedentes de las OI son varias cuestiones que se detallan a continuación:

La definición de OI como una función conjunta diferenciada, data del S XXI. La información ha surgido como un ambiente nuevo derivado de la evolución de las Tecnologías de Información y Comunicaciones (TICs). Por ello en el año 2017, en Estados Unidos se ha agregado en su doctrina militar a la información como séptima función conjunta, es decir agregada al comando y control, inteligencia, fuegos, movimiento y maniobra, protección, sostenimiento e información.(JP 1 CJCS, 2017, pág. I 18). Como ya se expresó, se consideran funciones conjuntas a las capacidades y actividades relacionadas agrupadas para ayudar a los comandantes de la fuerza conjunta a integrar, sincronizar y dirigir las operaciones conjuntas. No obstante, este concepto no se encuentra todavía incluido en la doctrina argentina.

Aunque ya fue considerado en un estudio de la RAND Corporation, lo que confunde es el uso de la misma frase Operaciones de información, para los operadores tácticos como para los planificadores de efectos operacionales y estratégicos. Si bien el uso coloquial de la palabra información derive por el uso naturalmente al campo de inteligencia, el concepto nuevo hace que las OI no pertenezcan con exclusividad al campo de inteligencia. Las OI se caracterizan por su eclecticismo y pertenecen al campo 3 Operaciones.(Perceptions are reality, 2018, pág. xiii). Son operaciones que generan efectos que se conducen, sincronizan y dirigen, integradas con los restantes elementos de las funciones conjuntas y con todas las audiencias militares y civiles. En cambio, la gestión de la información es propia del campo de inteligencia, y trata de la ciencia de usar procedimientos y sistemas de información para reunir, procesar, almacenar, diseminar y proteger los productos del conocimiento, los datos y la información sobre el enemigo, sus capacidades y vulnerabilidades, sus cursos de acción probables, tentativos y sus intenciones.

Uno de los objetivos que se establecieron al iniciar esta investigación es establecer una categorización tentativa de las Operaciones de Información teniendo en cuenta sus formas y propósitos particulares. Esta tarea no es sencilla, porque las OI son efectos que se obtienen empleando lo que se denomina Capacidades Relacionadas con la Informaciyn (CRI), definidas como "una herramienta, técnica o actividad empleadas dentro de la dimensión del ambiente de la información que pueda ser usada para crear efectos y condiciones operacionalmente deseables"[13] (DOD Dictionary, 2020, pág. 113). En Estados Unidos, inicialmente Libicki (1995) las catalogaba como se expresa más arriba. Posteriormente, en el 2011 la definición doctrinaria del Ejército de Estados Unidos limitaba las OI a cinco capacidades núcleo: Operaciones de Seguridad (ser refiere a la seguridad informática y física de instalaciones cibernéticas), Engaño Militar, Operaciones Psicológicas, Guerra Electrónica y Operaciones de Red de Computadoras, (Perceptions are Reality, 2018, pág. P. xiii), y actualmente desde el 2016 ha evolucionado a una definiciyn más amplia centrada en efectos, definiendo OI como "El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Informaciyn…"(DoD, 2020, pág. 104)

[13] Original en inglés, traducción propia.

La discusión acerca en qué consisten las OI está en proceso, pero la explicación se entiende un poco más cuando distintos protagonistas en un contexto doctrinario todavía difuso difieran sobre quién las lleva a cabo, en qué momento se usan, y si son propias de las operaciones convencionales, de las operaciones no convencionales o lo que se ha dado en llamar escenarios híbridos o "zonas grises", o "zonas no lineares" que es el tema que se tratará en el próximo capítulo.

CAPITULO II: LOS CONCEPTOS SOBRE OPERACIONES DE INFORMACIÓN EN EL MUNDO OCCIDENTAL Y ORIENTAL

La finalidad de este capítulo es determinar si la definición de la frase OI es de aceptación universal o si difieren en su concepto según lo interpreten los contendientes. Este capítulo no estaba concebido inicialmente, sino que surgió del proceso de la investigación al descubrir diferentes conceptos entre Oriente y Occidente. Al avanzar en este proceso, se encontró que las definiciones no eran unívocas.

LAS DIFERENTES DEFINICIONES

Es muy difícil establecer con exactitud cuando ocurrió el cambio conceptual de la frase OI, aunque casi con certeza puede decirse que tuvo auge a comienzos del S XXI. No debe alarmar que en la doctrina argentina este cambio haya pasado inadvertido, porque como se verá más adelante, hasta en la primera potencia militar del mundo occidental no se ha alcanzado consenso en la temática. El pensamiento difundido más avanzado es que hay un adelanto tecnológico que afecta la información porque ahora se consigue información en tiempo real y se ha multiplicado la obtención, pero eso requiere que se gestione la información, si es necesario con medios de inteligencia artificial, para que al Comandante llegue la información correcta, oportuna y precisa. No obstante, el salto tecnológico ha sido mucho más abrupto que esta concepción, y el problema de la información no es la forma en que se gestione, ni el problema pasa por la mejor administración, sino aceptar que la información se conduce, no se administra únicamente, sino que debe conducirse, debe ser integrada y coordinada entre todas las fuerzas armadas, (es decir en todos los dominios) y de allí que sea considerada una función conjunta para sincronizar y dirigir operaciones conjuntas.

Como se expresó en el capítulo anterior, las OI se usan en un contexto doctrinario todavía difuso, en las operaciones convencionales y en otros escenarios que se han dado en llamar indistintamente guerras híbridas, operaciones híbridas, ambiente hibrido, contexto híbrido, escenarios híbridos o conflictos de la zona gris. En algunos lugares los rusos también las denominan como nuevas guerras, o guerras no lineales, para diferenciarlos de la linealidad de los frentes de fuerzas cinéticas convencionales.

Al avanzar la investigación, surgió que el concepto de OI es diferente en el mundo Occidental (EEUU y OTAN), y en el Oriental (Rusia y China). También existe un concepto no gubernamental de amplia difusión en la red social Facebook.

EL CONCEPTO DE OPERACIONES DE INFORMACION (OI) EN EL MUNDO OCCIDENTAL.

Como se expresó antes, para Occidente (Estados Unidos de Norteamérica y la OTAN) las Operaciones de Información se definen en forma similar. Para EEUU, consisten en

> El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Información, en conjunto con otras líneas de operación para influenciar, interrumpir, corromper o usurpar el proceso de toma de decisiones de adversarios o potenciales adversarios mientras se protege a los propios. (DOD Dictionary, 2020)

En esta definiciyn, debe notarse la frase "durante operaciones militares", y de suyo se refiere a enfrentamiento de fuerzas militares convencionales. Luego, para Occidente las OI tratan de operaciones complementarias de las operaciones militares convencionales cinéticas. Luego, se trata de operaciones pertinentes a la estrategia militar, de las que se hace uso cuando el poder político decide el empleo de los medios militares convencionales. También debe notarse el empleo integrado de las Capacidades Relacionadas con la Información.

Las OI requieren de varias Capacidades Relacionadas con la Información (CRI). Las OI son operaciones que no consisten únicamente en recopilar información sobre un enemigo, o un terreno, o en sus cursos de acción probables, sino que además, afecta a todos los componentes del poder del adversario influyendo con desinformación y propaganda para buscar una ventaja. (Perceptions are Reality, 2018, pág. 34).

Como ya se expresó, las Operaciones de Información se caracterizan por su eclecticismo: son una combinación de elementos de diversos estilos, ideas o posibilidades. Es una mezcla de operaciones cibernéticas (de la red informática), operaciones psicológicas, de engaño y de manipulación, comunicaciones estratégicas de la Estrategia General, operaciones de influencia, inteligencia y contrainteligencia, disuasión, desinformación, guerra electrónica, debilitamiento de las comunicaciones, degradación del apoyo de información, presión psicológica, y de destrucción de las capacidades informáticas enemigas. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 15)

Las Capacidades Relacionadas con la Información (CRI) de los niveles operacional y táctico son una extensa lista de capacidades que tengan el potencial de influir en el ambiente de información de esos niveles, tales como Actividades Ciber-Electromagnéticas (CEMA), Operaciones de Apoyo a la Información Militar (MISO) u Operaciones Sicológicas (PSYOP), Asuntos Civiles (CA), Cámara de Combate (COMCAM), Equipos Humanos en el Terreno (HTTs), operaciones espaciales, operaciones de técnicas especiales y engaño, Compromisos de Soldados y Líderes (SLEs) y otros. Es importante tener en cuenta que estas son capacidades sobre las cuales el personal dedicado a las OI no tiene control directo. (Perceptions are Reality, 2018, pág. 18). Estas Capacidades Relacionadas con la Información evolucionarán para incluir todos los elementos que tengan la capacidad de penetrar en el dominio de la información, dar forma a la actividad de combate físico y maximizar el potencial para las operaciones cinéticas.(Perceptions are Reality, 2018, pág. 18). Esto permite concluir inicialmente que las OI son efectos originados por el uso de herramientas, las CRI.

Sin embargo, hay que reconocer que el concepto de Operaciones de Información en las Fuerzas Armadas de Occidente no está difundido como para captar su naturaleza. Uno de los inconvenientes es que equivocadamente se consideran un sinónimo de Operaciones de Apoyo a la Información Militar, y así insensiblemente se lo enlaza con actividades de Inteligencia, y específica y únicamente, con Acción Psicológica.

Existe una diferencia clave. Los funcionarios de OI integran una amplia gama de Capacidades Relacionadas con la Información arriba mencionadas, mientras que los funcionarios de Acción Psicológica se especializan en el desarrollo de mensajes diseñados para resonar en audiencias como cámaras de eco. Las Operaciones de Apoyo de Información Militar se concentran en el mensaje y en la manera más efectiva de difundirlo para crear una percepción; las OI se enfocan en la integración del mensaje con otras actividades en todos los dominios.(Perceptions are reality, 2018, pág. 91)

En Europa, conforme a las encuestas a oficiales superiores llevadas a cabo, el Coronel de Alemania (Lufftwaffe) BerndPfaffenbach expresó que

> “El tema de la información ya se trata de manera amplia en el Libro Blanco de 2016 en la sección Conducción […]Parte de las operaciones en el espacio cibernético y de información son precisamente las operaciones de información indicadas anteriormente, que se supone que son capaces de reaccionar ante la

> propaganda y desinformación de un oponente.[…] El entorno de la información es el espacio en el que se desarrollan los procesos cognitivos, sensoriales, interpretativos, intelectuales y comunicativos y sobre la base del cual las personas ajustan sus actitudes, voluntades y comportamientos. La comunicación dirigida, coordinada y coherente de la Bundeswehr (Fuerzas Armadas Federales Unificada) a través de palabras explicativas y acción militar se lleva a cabo de acuerdo con la narrativa política en el entorno de la información. El oponente utiliza el entorno de la información para la agitación, la demagogia, la desinformación y la propaganda. La Bundeswehr protege a su propio personal fomentando la resiliencia cognitiva".

Esta respuesta indica que las Operaciones de Información son tenidas en cuenta en las Fuerzas Armadas de Alemania, con un concepto similar al vigente en Estados Unidos, pero con cierta ambigüedad acerca de su influencia en el mundo no militar.

En España, el 1ro de enero de 2019 fue creado el Regimiento de Tropas de Informaciyn, que "se constituirá una agrupaciyn ad hoc con todas las capacidades necesarias teniendo en cuenta que la mayor parte de ellas tendrá lugar en el reach back fuera del Teatro de Operaciones" (Portal Infodefensa, 2019) Su finalidad era influir, en beneficio de las operaciones, sobre las percepciones, las conductas y las actitudes de la población y de otros actores que intervengan en el conflicto. Como puede distinguirse, los efectos de las OI exceden a las fuerzas militares de un Teatro de Operaciones.

EL CONCEPTO DE OPERACIONES DE INFORMACIÓN EN ORIENTE (RUSIA Y CHINA)

Existe más bibliografía sobre Rusia que sobre China, aunque con los dos hay diferencias idiomáticas profundas, y con China está el problema adicional que ese idioma es ideográfico, no tiene cambios entre género y número, y otras particularidades, por lo que puede contener inconsistencias en estilo y deletreo.

Según surge de la lectura del artículo "Los ciegos y el elefante; la guerra en ambiente operacional híbrido", los rusos no pensarían de la misma manera que los Estados Unidos. (Trama y otros , Los ciegos y el elefante: la guerra en ambiente operacional híbrido, Diciembre 2019).

RUSIA

Rusia habla de una “guerra no lineal” (non lineal warfare) o de “nuevas guerras” en la cual las fronteras entre la paz y la guerra, entre lo militar y lo no militar se diluyen, es decir, son las “guerras de nuevo tipo”, en las cuales, sin una declaraciyn formal de guerra y sin enfrentamiento de fuerzas convencionales, se emplean medidas convencionales, irregulares, terroristas, criminales, de desinformación, cibernéticas (ataques, espionaje, engaño), económicas y políticas (influencia, intimidación). (Trama y otros , Los ciegos y el elefante: la guerra en ambiente operacional híbrido, Diciembre 2019, pág. 7)

Es aquí donde según los rusos, entra el nuevo rol de las OI: en el umbral inmediatamente inferior al uso de la fuerza militar cinética convencional. No se necesita declaración de guerra previa, ni enfrentamiento convencional previo, sino que es una actividad que se desarrolla en todos los campos del poder y desde época de paz. Este punto de vista fue sostenido por el General ruso Valery Gerasimov, cuya teoría conocida como la “doctrina Gerasimov” fue tratada por el Coronel Makotchensko en el artículo “Una nueva visiyn de la Estrategia Militar en la concepciyn del General de la Federaciyn Rusa Valery Gerasimov”. (Makochensko , 2019, pág. 20) . La doctrina Gerasimov dispone una nueva forma de instrumentar la Estrategia Militar, que usa todos los métodos que posee el Estado para el logro del objetivo impuesto por la Estrategia Nacional.

> Las mismas "reglas de guerra" han cambiado. El papel de los medios no militares para lograr objetivos políticos y estratégicos ha crecido y, en muchos casos, han excedido el poder de la fuerza de las armas en su efectividad.(Gerasimov, Getting Gerasimov Right, 2016, pág. 24)

Esta es una nueva definición de OI diferente a la que sostiene Occidente, tanto en oportunidad de aplicación como en contenidos que se aplican. Es otra concepción de OI como

> "un conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y comunidad internacional en todos los niveles”. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 15).

Nótese que a diferencia de la concepción de Estados Unidos, la influencia de las OI no solo es sobre el público militar, sino también “sobre la poblaciyn y comunidad internacional en todos los niveles”.

La idea original es que se sostiene que ha surgido un nuevo tipo de guerra, en la que la guerra armada convencional ha cedido su lugar decisivo en el logro de los objetivos militares y políticos de la guerra a otro tipo de guerra: la guerra de medios de información. En el pensamiento ruso, la guerra de la información no es una actividad que se limite al tiempo de guerra, como dice pensar Occidente. Ni siquiera se limita a la fase inicial de un conflicto, lo que en la doctrina occidental se denomina “preparaciyn de inteligencia del espacio de batalla”.

En la concepción rusa, las OI son una actividad continua independientemente del estado de relaciones con el oponente o el competidor; y sostienen que "en contraste con otras formas y métodos de oposición, la confrontación de información se libra constantemente en tiempos de paz”. Es decir que para los rusos, las operaciones de información no necesariamente estarían subordinadas a operaciones complementarias de las operaciones militares con medios convencionales cinéticos.

Se hace una clara distinción entre la definición rusa amplia y no limitada a tiempo de guerra - y la definición de la OTAN y de Estados Unidos que las describe como operaciones limitadas de información táctica realizadas durante hostilidades.

En este entendimiento, para Rusia, Occidente ya está compitiendo en el dominio de la información y esta confrontaciyn “pacífica” porque se desarrolla en el umbral inmediatamente inferior al uso de las Fuerzas Armadas del estado, ya ha comenzado. La guerra de medios no militares está en curso y es "una característica habitual de la cobertura de noticias y actualidad del país”. (Keir Giles, Handbook of Russian Information Warfare, 2016, págs. 4, notas 6 y 7)

Los rusos consideran que Occidente está usando las OI en época de paz, aunque declaradamente en la teoría sostengan que son parte de operaciones complementarias a operaciones militares convencionales. Citan como ejemplo la expansión de la OTAN hacia el Este desde el colapso del Imperio Soviético, la rebelión en Libia en el año 2011, y la Primavera Árabe (2010/2012).(Korybko, Guerras Híbridas Revolución de Colores y Guerra No Convencional, 2015)

> …la mayoría de estas fuentes rusas presentan sus investigaciones y hallazgos como una descripción no de los enfoques propios de Rusia, sino de los enfoques

> que dicen que son adoptados por potencias extranjeras que buscan dañar a Rusia. En algunos casos, los principios descritos no reflejan la teoría local, sino la adopción rusa de lo que considera una práctica occidental.(Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 1 y 2)

En la concepción rusa y a diferencia de la concepción occidental, las OI son operaciones principales, complementadas o respaldadas por operaciones militares convencionales que si la tarea de las Operaciones de Información ha sido eficaz, hasta podrían no ser necesarias. Por lo tanto, son operaciones propias de la estrategia política.

> En el concepto ruso puede abarcar una amplia gama de diferentes actividades y procesos que buscan robar, plantar, prohibir, manipular, distorsionar o destruir información. Los canales y métodos disponibles para hacer esto cubre una gama igualmente amplia, que incluye computadoras, teléfonos inteligentes, medios de comunicación reales o inventados, declaraciones de líderes o celebridades, campañas en línea de trolls, mensajes de texto, mensajes publicitarios, la opinión callejera de ciudadanos involucrados, videos YouTube o aproximaciones directas a objetivos humanos individuales. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 4)

Se trata de influenciar a las masas para que en los individuos se imponga la opinión mediática sobre la opinión pública. Por supuestos que se eligen blancos principales para estas acciones, en especial a la clase dirigente política que en el mundo occidental está regida por las encuestas (por ejemplo, el presidente, los ministros de Relaciones Exteriores y de Economía, los comandantes militares, los periodistas y en especial los denominados "formadores de opinión"). Esta influencia involucra hechos distorsionados, inculcar opiniones emocionales antes que racionales, e influenciar sentimientos y no estados finales. Todo apunta a crear un ambiente tolerante a hechos que presentados de otra forma, serían intolerables. Modifica la realidad creando una percepción tal que permite sacar provecho a la confusión generada por la falsedad de noticias.

> Rusia busca influir en la toma de decisiones extranjeras suministrando productos contaminados de información, explotando el hecho de que los representantes elegidos occidentales reciben y son sensibles a los mismos flujos de información que sus votantes. Cuando la desinformación entregada de esta manera es parte

del marco para las decisiones, esto constituye un éxito para Moscú. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 22)

El blanco principal es ganar la opinión pública, cambiándola por la opinión mediática. De esa manera, se instala un ambiente tolerante a la actuación rusa y por lo tanto, se atenúa la resistencia social y también eso reduce la posibilidad de reacciones adversas de la comunidad internacional.

La percepción rusa es que Occidente busca comprometer la soberanía rusa, y se apoyan en la evidencia histórica que la postura de Gorbachov sobre la glasnot[14] una libertad de expresión que inició el proceso que llevó al colapso de la Unión Soviética. Hoy hay una evidente contradicción entre la postura Occidental oficial de una internet libre de restricciones y un flujo de información sin restricciones, con la postura de Rusia que pone restricciones importantes en el flujo de la información e insiste en el principio de soberanía nacional en el espacio cibernético. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 38)

Es importante destacar que mientras Occidente ve estas OI como herramientas rusas para llevar a cabo operaciones de guerra no militares, para los rusos se presentan como campañas planificadas por el Occidente hostil contra Rusia, en su intento de desplazar sus dominios hacia el Este. Sostienen que, si Rusia acepta llevar a cabo este tipo de OI, lo hace adoptando y adaptando las lecciones aprendidas de Occidente en guerras de la información (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 26). El mismo General Gerasimov sostiene que no es dueño de ninguna doctrina, sino que solamente ha observado la realidad y sacadas conclusiones.

Es conveniente aclarar que existe una publicación argentina de Andrew Korybko, periodista y analista de origen estadounidense que reside en Moscú, cuyo título es Guerras Híbridas, Revolución de Colores y Guerra No convencional, que acusa a Estados Unidos de usar las "revoluciones de colores" [15](nombre que los rusos

[14]Glasnot: (en ruso Гласность, 'apertura', 'transparencia' o 'franqueza') política que se llevó a cabo a la par que la perestroika en la Unión Soviética por Mijaíl Gorbachov, desde 1985 hasta 1991. Finalizó con el colapso del Imperio Soviético.

[15]Así se conoce con el nombre de "Revolución de las Rosas" la salida del poder del presidente Shevardnadze de Georgia (2003) la "Revolución Naranja" la elección de Yúshchenko en Ucrania (2004); la "Revolución de los Tulipanes" que expulsó al gobierno de kayev en Kirguistan (2005) la "Revolución del Cedro", consistente en la salida de Siria del Líbano (2005) la "Revolución de los Jazmines" salida del gobierno de Zine el Abidine en Tunez (2010). Hay otras como las que ocurrieron con suerte diversa en

dan a las sublevaciones civiles en países de la ex Unión Soviética) y la insurgencia, para ejercer un "liderazgo" velado sobre ellos y así avanzar su poder geográfico hacia el Este, zona que denomina "Balcanes Euroasiáticos". En las "revoluciones de colores", se hace uso intenso de las Operaciones de Información. Según Korybko, existiría un "puente" entre las "Revoluciones de Colores" y la Guerra no convencional. Esta Guerra no convencional incluye guerrillas, insurrección urbana, sabotaje y terrorismo. Esta edición es difícil de conseguir en las librerías argentinas, pero se puede bajar de internet puesto que no tiene derechos de copyright. En la edición argentina, llama la atención un párrafo de su prologuista Juan Grabois, que expresa

> Se consolidó la capacidad de las redes sociales de influir en las percepciones, ideas, emociones y acciones de grandes masas humanas. Así, el ciberespacio pasó a ser otro teatro de guerra (Korybko, Guerras Híbridas Revolución de Colores y Guerra No Convencional, 2015, pág. 21)

El concepto de guerra híbrida de Korybko es el mismo que sostiene el General Gerasimov, cuando sostiene que Occidente desde el final de la Guerra Fría ya está llevando campañas planificadas contra Rusia. Como ya se expresó, este tema no es motivo de esta investigación.

En 2017, las autoridades rusas crearon las llamadas "tropas de operaciones de informaciyn", cuyo cometido, según el Ministro de Defensa de Rusia, Sergei Shoygu, era difundir "Propaganda inteligente y eficiente".[16]. El objetivo de estas tropas abarca una mezcla de comunicaciones estratégicas, operaciones psicológicas y actividades de influencia. Ellas no deberían ser tratadas como un comando separado basado en el ciberespacio, ya que sus medios van más allá de simplemente llevar a cabo la guerra cibernética para afectar redes, sino que también incluyen manipular los medios e infiltrar contrapropaganda con el fin de controlar y distorsionar la comprensión cognitiva del enemigo, de lo que es real y lo que es falso. Esto también involucra infiltrar historias de noticias falsas para avivar la violencia anarquista. (Perceptions are reality, 2018, pág. 41)

Bielorusia (Revolución Blanca); en Irán en protesta de un fraude electoral (Revolución Verde); y las protestas antigubernamentales en Moldavia de 2009.

[16]DamienSharkov, "Rusia nuncia Tropas de Operaciones de Información con la Misión de Contrapropaganda. *Newsweek*, 22 Febrero 2017.

CHINA

En cuanto a China, los datos son mucho más difíciles de lograr. No existen datos que puedan ser comprobados, aunque se dice en fuentes de Internet que la intranet china se denomina QQ, que los usuarios de correo electrónico se les asignan un número y si no usan ese correo electrónico en cierto lapso pierden vigencia. Lo único verificable es lo que publica el China‘s National Defense in the new era Año 2019, que puede encontrarse en referencia en Internet, pero no es posible obtener una copia completa.

Se diligenció una encuesta para el cursante de la República Popular China Coronel EPL Yin Zhiyong, que expresó que “Las redes de información son una nueva tendencia que ha cambiado profundamente el entorno ideológico y de la opinión pública.[…] Se debe mantener el ritmo de la tecnología de la información, servir a la guerra de información, aumentar el nivel de la tecnología de la información, para poner las alas al trabajo política tradicional, para lograr la integración orgánica de los portadores de la red y el trabajo político propiamente dicha, así como la gran integración de las ventajas tradicionales con la tecnología de la información.[….] Debemos estudiar y comprender activamente las características y leyes del trabajo político en la era de las redes de información, llevar a cabo las luchas de la opinión pública en línea como si estuviéramos librando una guerra, seguir de cerca las características cognitivas de los jóvenes oficiales y soldados al llevar a cabo la educación ideológica y política en línea.[….] promover la integración del trabajo político en el sistema de información de la red y el sistema de operación conjunta, y hacer de la red de información un "multiplicador" que dé pleno juego a las ventajas tradicionales del trabajo político.”

Lo más llamativo es lo que se menciona sobre OI en el libro Unrestricted Warfare, publicado en China en 1999 y escrito por dos en ese momento coroneles de la Fuerza Aérea del Ejército Popular de Liberación Qiao Liang y Wang Xiangsui. Allí, al hablar de un nuevo concepto de armas, adelantan que

> La guerra computarizada en sentido amplio y la guerra de información en sentido estricto son dos cosas completamente diferentes. El primero se refiere a las diversas formas de guerra que se mejoran y van acompañadas de tecnología de la información, mientras que el segundo se refiere principalmente a la guerra

en la que la tecnología de la información se utiliza para obtener o suprimir información. (Qiao y Wang, Unrestricted Warfare, 1999, pág. 9)

En una nota llamativa si se tiene en cuenta el año en que este libro fue escrito - 1999 - se refiere a las armas de informaciyn como ejemplo destacado de "armas bondadosas", al decir que

> Las armas bondadosas representan un derivado del nuevo concepto de armas, mientras que las armas de información son un ejemplo prominente de armas más amables. Ya sea que se trate de armas de energía electromagnética para la destrucción dura o golpes suaves con bombas lógicas de computadora, virus de red o armas de medios, todo se enfoca en paralizar y socavar, no en bajas de personal.(Qiao y Wang, Unrestricted Warfare, 1999, pág. 16)

Asimismo, citan que el general Gordon R. Sullivan, ex Jefe de Estado Mayor del Ejército de EE. UU., sostuvo que la guerra de información será la forma básica de la guerra en la guerra futura. (Qiao y Wang, Unrestricted Warfare, 1999, pág. 31)

Las notas aclaratorias 4, 6 y 7 al Capítulo 1 denominado Lo que invariablemente viene primero es la Revolución de las Armas, son llamativas porque indican que las OI ya estaban siendo esbozadas hace 20 años.(Qiao y Wang, Unrestricted Warfare, 1999, pág. 18 a 21)

EL CONCEPTO DE OPERACIONES DE INFORMACIÓN (OI) EN ORGANIZACIONES NO GUBERNAMENTALES

Facebook es una red social no gubernamental que conecta personas con personas, y que dio origen a las denominadas Redes Sociales. En esta organización no gubernamental, existe también un concepto no militar sobre Operaciones de Información, que dice

> Definimos las operaciones de informaciyn, […..] como acciones tomadas por actores organizados (gobiernos o actores no estatales) para distorsionar el sentimiento político nacional o extranjero, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una

combinación de métodos, como noticias falsas, desinformación o redes de cuentas falsas destinadas a manipular la opinión pública (nos referimos a estos como "amplificadores falsos").(Facebook Inc , 2017, pág. 4)

Puede verse que la definición de OI no es unívoca, y hasta para el caso de Estados Unidos, en los últimos diez años han cambiado de significado. No ha ocurrido lo mismo con el concepto oriental, donde parece resaltar que lo sustancial es el predominio de la narrativa del conflicto. En los conflictos de inicio del siglo XXI, en Estonia, Georgia y Ucrania, Rusia hizo uso intenso de este tipo de OI. Aunque Occidente lo niega, es acusación rusa y china que Occidente usó OI desde la finalización de la Guerra Fría en la expansión de la OTAN hacia el Este luego de 1990, y que usa las OI durante la paz con objetivos políticos. Esta investigación no profundiza sobre la veracidad de estos hechos, porque se incursionaría en las denominadas guerras híbridas, que no son motivo de esta investigación.

LA RELACION ENTRE LOS NIVELES DE GUERRA Y LAS OI

Los denominados niveles de guerra son una herramienta metodológica para distinguir la asignación de medios y fines, y facilitar así la asignación de responsabilidades a cada nivel de conducción.

NIVELES DE LA GUERRA	FINES	MEDIOS
Estratégico	El Estado Final Estratégico / Político.	Todos los medios del poder nacional
	El Estado Final Estratégico/ Militar [17]	Todos los medios militares del poder nacional y eventualmente aquellos otros provenientes del poder nacional.
Operacional	El Estado Final Operacional en un Teatro de Operaciones	Los asignados al Teatro de Operaciones. (los

[17] Significa obtener los objetivos de incumbencia militar, luego de lo cual continúan otros elementos del poder nacional en la consecución de los Objetivos Nacionales.

	[18]	correspondientes a cada Comando Subordinado)
Táctico	Los resultados convenientes para obtener el Estado Final Operacional	Los medios enfrentados en cada operación militar

Fuente: PC 20-01Planeamiento Para La Acción Militar Conjunta Nivel Operacional Año 2017, Relaciones entre niveles de la guerra, niveles de conducción, fines y medios, Página 2.

El planeamiento de los diferentes niveles se relaciona estrechamente y se hace interdependiente. En la práctica, existe un solapamiento entre los niveles y la distinción entre los mismos suele hacerse confusa. No obstante, es necesario reconocer que cada uno de ellos tiene elementos diferenciales que no son únicamente un problema de tamaño o de naturaleza de una operación.

Además de todas las consideraciones que figuran en la Publicación Conjunta PC 00-02, en las páginas 148 y 149, surge claramente que el nivel estratégico es de dirección ya que establece los estados finales a lograr con el empleo de los medios, y que los niveles operacional y táctico son los responsables de implementar[19] esa dirección.

Si fuéramos más en detalle a las responsabilidades, es sencillo ver que el nivel operacional [20] trata de las maniobras y la logística para colocar a las fuerzas que se van a enfrentar en cada punto decisivo en las mejores condiciones, en tanto que el nivel táctico trata de los enfrentamientos.

Es en el nivel operacional donde se llevan a cabo campañas y se expresan las Líneas de Operaciones (LDO) que permiten alcanzar el estado final deseado de ese nivel. Cada campaña refleja el arte operacional del Comandante del Teatro de Operaciones, volcado en un diseño operacional. Las LDO unen Puntos Decisivos (PD) que pueden ser tanto materiales, como es el caso de un objetivo físico, como inmateriales, como sería el caso de la moral propia o de la del oponente, e incluso puede

[18] Pueden existir simultáneamente más de un Teatro de Operaciones.

[19] Se acostumbra a decir “operacionalizar”, pero esta es una palabra inexistente en el idioma español. La palabra del idioma que significa “llevar la teoría a la práctica” es *implementar.*

[20] Erróneamente denominado “nivel operativo” en algunas fuerzas armadas, debido a un error de traducción del francés.

tratarse de una situación, como podría ser la efectividad de un embargo económico de un bloqueo naval. (PC 20-01, 2017, pág. 23) . Es fácil darse cuenta que las OI facilitan que se obtengan los estados finales de cada PD, para así poder emplear el mínimo de esfuerzo necesario.

Las líneas de operaciones (LDO) pueden ser físicas o lógicas. Las primeras son las que conectan a la propia fuerza desde su base de operaciones hasta los objetivos físicos. Es decir, las LDO físicas conectan una serie de PD, que llevan a obtener el objetivo operacional. Las LDO lógicas por su parte, conectan acontecimientos o situaciones a lograr, que pueden coincidir o no con una referencia en el terreno. (PC 20-01, 2017, pág. 23)

Las OI que se lleven a cabo deben facilitar la obtención de los estados finales de cada Punto Decisivo, e influenciarán en decidir si la aproximación operacional será directa o indirecta.

El problema de este razonamiento es que según un Informe de la RAND Corporation del año 2019, la causa por la cual la frase OI lleva mucho tiempo acosado por la ambigüedad es la siguiente:

> "El sentido común y la comprensión coloquial de las operaciones de información toman el término al pie de la letra, suponiendo que las operaciones de información son aquellas que tienen algo que ver con la información. Esta comprensión del sentido común sugiere además que el personal de OI son, por lo tanto, operadores que participan en estas operaciones empleando información de alguna manera. Esto tiene mucho sentido y es una manera fácil de usar el término". (Paul Christopher, 2019)

Esto es una razón más que hace que se confundan las OI con actividades del campo de la Inteligencia. Este estudio de la RAND Corporación sentencia que

> Un paso para mejorar la forma en que la fuerza conjunta habla y piensa acerca de la información es simple: cambiar el léxico. El Departamento de Defensa podría eliminar las OI como un término formal y permitirle caer a su significado coloquial. Los operadores no son del campo de inteligencia, son oficiales del Estado Mayor que planifican e integran, no son operadores.

> Sin embargo, las actividades planificadas y coordinadas como parte de las OI también se denominan errónea e incorrectamente "operaciones de información". Esto combina la planificación y el EM con actividades y acciones, y puede generar confusión sobre los roles y las expectativas. Alguien que no entienda las OI bien podría esperar que un funcionario del EM cuya responsabilidad sea planificar e integrar diseñe un guion gráfico para folletos, se conecte a una computadora y realice algún reconocimiento cibernético, o ejecute actividades de información.(Paul Christopher, 2019)[21]

Es decir, con el mismo nombre de OI se mencionan las LDO lógicas de OI en apoyo de los estados finales de cada PD, y las actividades de los operadores de OI en el nivel táctico.

Lo que se debe ser cuidadoso es encasillar el razonamiento estrictamente dentro de la clasificación metodológica de los niveles de guerra. Por el carácter global de los medios de comunicación, las OI son un problema de comunicación estratégica, que se origina en el nivel de dirección, y que derrama sus efectos en los niveles de implementación, buscando un objetivo político estratégico, por lo que no es sencillo separar los límites entre niveles de guerra, que naturalmente se tornan borrosos. Por lo expresado, sería un error conceptual grave pretender que la conexión entre los estados finales de cada punto decisivo y las OI en sus efectos de propaganda o de influencia, fuesen delegados en una célula de “Operaciones de Informaciyn” dependiente del J 3 de un Comando de Teatro. Antes bien, la comunicación entre estados finales de OI requiere de una fluida comunicación entre niveles, y esa es la razón por la cual en OI los niveles se hacen borrosos.

En el nivel táctico, se concentra en el mensaje y en la manera más efectiva de difundirlo para crear una percepción; en el nivel operacional y estratégico, se enfoca en la integración del mensaje con otras actividades para obtener un efecto deseado. El foco de la OI no es tanto el tipo de operación sino el tipo de efectos que deben ser generados en y a través del entorno de información para apoyar la operación a gran escala que esté siendo emprendida.(Perceptions are reality, 2018, pág. 113).En los elementos cinéticos del poder de combate, se actúa según la misión establecida en la oportunidad determinada. En OI, no se descansa ni se duerme, ya que están siempre

[21] Original en inglés, traducción propia.

activas.(Perceptions are reality, 2018, pág. 108), y esto hace suponer que queda abierto el camino para la lucha política internacional e interna, por lo que las acciones en los tres niveles deben estar entrelazadas.

Aunque no esté concretamente expresado en ninguna bibliografía en estos términos, se deduce como características o principios de las OI en su relación con las LDO del nivel operacional a la preparación (deben pensarse con antelación en búsqueda de un estado final político deseado), sincronización (con las líneas de operaciones físicas), integración o convergencia o combinación con otras capacidades relacionadas (por el eclecticismo de las Operaciones de Información) (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 68), profundidad y efectos simultáneos(no solo se dirigen al frente de combate sino a la retaguardia de la población y del adversario)(Gerasimov, The Value of Science in the Foresight, 2016), no distinción (entre tiempos de paz y de guerra) y selección de blancos (también pueden apuntarse a los líderes que conducen) (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 71). Según Keir Giles, en las guerras híbridas las Operaciones de Información deben ser oportunas, inesperadas y clandestinas.(Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 65)

Existen ejemplos históricos del uso de OI para influenciar con propaganda, desinformación, y acción psicológica el curso de las operaciones militares. Uno de ellos fue la influencia de la opinión pública en la derrota de las fuerzas de Vietnam del Sur y Estados Unidos de Norteamérica en Vietnam. La ofensiva de Tet fue una operación llevada a cabo por el Vietcong y el ejército de Vietnam del Norte en Febrero de 1968, que resultó en un fracaso militar de las fuerzas comunistas, pero tuvo efecto contrario en la opinión pública estadounidense. Las pérdidas comunistas fueron muchas, pero conmovieron a los estadounidenses que pensaban que estaban cerca de la victoria. El reconocido comentarista Walter Cronkite de CBS Evening News, produjo un informe pesimista por televisión. Unos pocos meses después, el Presidente Johnson dijo que no se presentaría en las próximas elecciones. Según dice Sean McFate, “ese fue el momento en que los Vietnamitas del Norte ganaron la guerra, no por su poder de fuego sino por las noticias vespertinas” (McFate, The New Rules of War Victory in the Age of Durable Disroder, 2019, pág. 174). Los norvietnamitas habían entendido la forma de llevar a cabo una guerra en la era de la televisión depende mucho más de la propaganda

que de los hechos en el terreno. Saigón usó agentes secretos como PhamXuanAn, y norteamericanos influyentes como la actriz Jane Fonda, para manipular la opinión pública.

> PhamXuanAn era un periodista de la agencia Reuters y la revista Time, y también una fuente anónima para periódicos mayores como el New York Times. Después de la Guerra, se descubrió que había sido un Coronel en el Ejército de Vietnam del Norte, todo el tiempo.(McFate, The New Rules for War - Victory in the Age of Durable Disorder , 2019, pág. 175)

Para los Estados Unidos, la guerra no había sido perdida en Vietnam, había sido perdida en casa. En el caso de Vietnam, la información se había convertido en un arma más decisiva que el poder de fuego. "Transformar la información en un arma es eficaz porque controla la narrativa del conflicto, haciendo la pregunta por qué la gente debería luchar y morir (o no)." (McFate, The New Rules of War Victory in the Age of Durable Disroder, 2019, pág. 176)

Otro ejemplo fue el inicio de la guerra del Yom Kippur en 1973, día de la expiación, del perdón y del arrepentimiento de corazón o de un arrepentimiento sincero para la religión judía, fecha elegida por los árabes para iniciar la guerra, ya que Israel debió pedir permiso al Gran Rabino de Israel para empeñarse en combate y eso llevó una demora en la reacción israelí.

Para planificar los efectos de una OI se requiere el conocimiento profundo de la cultura que se enfrenta. Los rusos definen este requisito como *control reflexivo* (de un espejo, el *reflejo*) se entiende "un proceso por el que un enemigo transmite las razones o bases para la toma de decisiones a otro". Cuando un sistema alcanza el control reflexivo sobre otro adversario, puede influir en la forma que éste último percibe la situación, en sus planes y en la forma que actuará".(Martínez Pointijas, 2020), ya que será reflejo de la forma cultural en que su adversario ve su propia realidad y actúa en consecuencia.

Lo que se está viviendo es lo que en 1989 William Lind y otros, en su artículo "El rostro cambiante de la guerra; hacia las guerras de Cuarta Generaciyn" adelantaba diciendo que sería el cuarto cambio que ocurriría respecto a las Guerras de Tercera Generación:

> La cuarta es la meta de colapsar al enemigo internamente, en vez de destruirlo físicamente. Los objetivos incluirán cosas como el apoyo de la población a la guerra y la cultura del enemigo. […] En términos generales, la guerra de cuarta generación parece probable que sea muy dispersa y en gran medida indefinida; la distinción entre la guerra y la paz se desdibujará hasta el punto de desaparecer. Será no lineal, posiblemente hasta el punto de no tener campos de batalla o frentes definibles. La distinción entre "civil" y "militar" puede desaparecer. Las acciones ocurrirán simultáneamente en toda la profundidad de los participantes, incluyendo su sociedad como una entidad cultural, no sólo física.(Lind, 1989, pág. 24)[22]

En la construcción de la narrativa del conflicto, la influencia en la población, la propaganda y la acción psicológica, la opinión pública tiene gran importancia y en este rol juega un papel importante las denominadas redes sociales. En el próximo capítulo se verá la relevancia y la importancia de reforzar los efectos de las OI, especialmente en el ambiente del ciberespacio, mediante el uso de las redes sociales, al estudiar el análisis de ellas y su efecto en el predominio de la opinión pública.

[22] Original en inglés, traducción propia.

CAPITULO III: LA IMPORTANCIA DE LAS TECNOLOGÍAS DE INFORMACION Y COMUNICACIONES (TICS) EN LAS PERCEPCIONES SOCIALES Y EN LOS ESCENARIOS MILITARES

> Esta nueva Guerra Fría se diferencia de la anterior en que vivimos en un mundo globalizado. Así pues, los medios de comunicación e Internet, es decir, la construcción narrativa del conflicto, se convierten en un elemento fundamental.
>
> Jesús M. Pérez Triana, Las Guerras Posmodernas

La finalidad de este capítulo es investigar sobre la influencia de las denominadas redes sociales en las percepciones de una sociedad, y en la formación de la opinión pública usada como arma política en OI. Las redes sociales son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. A través de ellas, se crean relaciones entre individuos o empresas de forma rápida, sin jerarquía o límites físicos. Esto no significa que la única Capacidad Relacionada con la Información sean las operaciones en el ciberespacio, ya que existen otras capacidades relacionadas que también generan efectos en el dominio de la información.

En este trabajo no se referirá al uso de la cibernética con propósitos delictivos, a lo que se define como delito informático o delito cibernético. Estos delitos se hacen usando las nuevas tecnologías de información y comunicaciones, y en la Argentina se incorporaron al Código Penal, por la ley 26.388 de junio del 2008. Existen con varios nombres, tales como phreaking (robo para hacer llamadas telefónicas a larga distancia usando una cuenta ajena); pishing o robo de identidad; el sexting y el stalking con contenidos sexuales; el ransomware o secuestro de datos; y demás malware, como los troyanos (que permite una administración remota de un equipo a un usuario no autorizado) y gusanos (malware que se replica para atacar otras computadoras). No se tratarán esos aspectos. Se concentrará en lo que afecta las redes sociales a la influencia de la opinión pública.

LA INFORMACIÓN ANTES DE LA PROLIFERACIÓN DE LAS TECNOLOGIAS DE INFORMACION Y COMUNICACIONES

A medida que se fueron acortando las distancias por la velocidad de propagación de las comunicaciones, simultáneamente comenzó a elevarse la importancia de la opinión pública. El primer indicio de la importancia de las comunicaciones como

difusora de ideologías fue la aparición de la censura, cuyos orígenes podrían verse en el fraile Torquemada. Según relata la historia, para evitar la propagación de las herejías, a fines del S XV y luego de expulsados judíos y moros de la península, el sacerdote Torquemada, al igual que se hacía en toda Europa, promovió la quema de literatura no católica, en particular bibliotecas judías y árabes.

La uniformidad del pensamiento fue una característica de todos los imperios para mantenerse unidos. En el Imperio Español, por ejemplo, entre los siglos XVI y XIX, la uniformidad de pensamiento se lograba con el sistema de enseñanza basado en la cultura de la religión católica, (Maltby, 2008, pág. 127) y la prohibición de otras religiones, "junto con una notable cualidad del pensamiento político". Es de esta época en que se instrumentó el sistema de enseñanza hasta hoy predominante en países latinos, que consiste en el profesor que da clase a los alumnos, los alumnos son los que rotan, y su deber es repetir lo que dice el maestro. Cuanto más exacto sea lo que sostiene el alumno de los que dice el profesor, más alta será la nota que se obtendrá.

También pasaba en la China de Mao TseTung, donde lo que había que saber estaba escrito en el Libro Rojo de Mao, que consistía en una recopilación de los discursos de Mao TseTung (en otras citas se lo llama Mao Zedong) escrito en 1947 y publicado en 1964. Por su parte, los soviéticos echan la culpa de la caída de su Imperio a la glasnot (palabra rusa que significa trasparencia o franqueza) y la perestroika, que fue un proceso de transformación de la economía llevada a cabo por el presidente de la Unión Soviética Mijaíl Gorbachov, entre 1985 y 1991. Según esta visión, eso causó la disolución del Pacto de Varsovia y la Unión Soviética en 1990.

El engaño de la opinión pública con medios de prensa puede reconocerse en la frase prensa amarilla, que aún perdura en la frase "Usted suministre las fotos, y yo facilitaré la guerra", que se atribuye al periodista William R.Hearst, al fotógrafo Frederick Remington en 1898, con motivo de la guerra entre Estados Unidos y España, por la isla de Cuba. Esta fue una de las competencias más reñidas, con los diarios Hearst y Pulitzer como competidores líderes. La única preocupación era la de vender más diarios, y esta parcialidad, vulgaridad y sensacionalismo dejó lo que hoy llamamos "prensa amarilla". El término actual vino de la sensacional cobertura del diario Hearst "Yellow Fellow Transcontinental Bicycle Relay of August - September 1896. La Prensa Amarilla fue directamente responsable de alinear la opinión pública a favor de una guerra para liberar Cuba. La fama de ciertos escritores y corresponsales elevó al periodismo amarillo. Estos individuos incluían a Richard Harding Davis, quien también

había cubierto las Guerras Boers y Ruso-Japonesa; Stephan Crane, que escribiy "El emblema rojo del coraje"; y el pintor e ilustrador Frederick Remington."(Strategy and Tactics, 1954)

Estos medios de prensa de ese entonces idearon el recurso de inventar historias sobre "las brutalidades españolas". Lo cierto es que esos eran los temas más candentes en su país, en especial cuando se los condimentaba con "relatos de testigos" cubanos o la "evidencia indiscutible" relatada por los rebeldes. La pérdida de Cuba significó el colapso del Imperio Español.

Hasta mediados del S XX, los medios de difusión de información escritos o visuales se usaban para medidas de engaño militares, o como acción psicológica. En esa época comenzaron a cambiar dos cosas: una de ellas es que de los medios radiofónicos se pasó a los medios televisivos. Ahora no solamente se escuchaba, sino que se veía y se daba por cierto lo que se veía, porque no estaba difundida la técnica de "ediciyn" (composición de varias imágenes) de los archivos. La otra, la democracia electiva tomó fuerza y es la que legitima los gobiernos, de forma tal que la opinión pública comenzó a tomar fuerza en el ámbito político, al punto de comenzar a influir en las Relaciones Internacionales de los Estados, como ocurrió en Estados Unidos en la guerra de Vietnam.

Con estos antecedentes, la importancia de los medios de comunicación tradicionales recibió especial atención luego de Vietnam, y se pusieron en acto en la guerra del Golfo I, ya que el Comandante H. Norman Schwarptkoft con el grado de Mayor había participado de la Guerra de Vietnam, mientras su hermana manifestaba en contra de la guerra en Washington. Ese aspecto no fue descuidado por el General Schwarptkoft, como surge en la lectura de su obra "It doesn´t take a heroe". En este libro, hace notar la importancia que se le dio a la difusión de noticias, no solo como medida de engaño militar sino también para que Saddam Hussein se confundiese al tomar decisiones. (Schwarptzkoft, 1993, pág. 370 a 500). Sin embargo, en la opinión de los autores chinos Qiao y Wang, la prensa es un arma de doble filo ya que indujo al presidente George Bush para dar por finalizada la guerra antes que se lo aconsejasen los comandantes militares, para poder denominarla políticamente "la guerra de las 100 horas", cuando el Presidente Bush ordenó un alto el fuego, pese a la oposición militar. (Qiao y Wang, Unrestricted Warfare, 1992, pág. 61)

Este rol sustantivo de los medios también es resaltado por estos autores chinos en el párrafo Otro jugador escondido detrás de la victoria, donde aclaran:

> El impacto de los medios de comunicación en la guerra se está volviendo cada vez más extendido y cada vez más directo, hasta el punto donde incluso grandes decisiones por el presidente de una superpotencia como la que tomó, implican el cese de las hostilidades hechas en muy gran medida sus raíces en la reacción a un programa de televisión único. De esto, uno puede percibir un poco la importancia que los medios de comunicación llevan hoy en día en la vida social. Se puede decir sin exageración que un rey sin corona se ha convertido en la principal fuerza para ganar cualquier batalla. (Qiao y Wang, Unrestricted Warfare, 1992, pág. 61)

Estos autores sostienen que los estadounidenses se esforzaron por sugerir que "la fuerza de los informes de los medios de comunicación pudo tener un efecto inmenso en la dirección estratégica y el alcance de las operaciones militares", mientras que los nuevos manuales del Ejército de Estados Unidos sobre Operaciones de Información van aún más lejos en el uso del ejemplo de la guerra de medios durante la Guerra del Golfo. Parecería que, en todas las guerras futuras, además del método básico de los ataques militares, la fuerza de los medios de comunicación será un jugador más en la guerra y jugará un papel comparable al de los ataques militares para promover el curso de la guerra.

A diferencia de la propaganda en el campo de batalla, que tiene un tinte excesivamente subjetivo y es fácilmente rechazada por un oponente o individuos neutrales, la información supuestamente objetiva de los medios tiene un impacto silencioso que es difícil de calibrar. En el Golfo, de la misma manera que las fuerzas aliadas lideradas por Estados Unidos privaron a Irak de su derecho a hablar militarmente, los poderosos medios occidentales lo privaron políticamente de su derecho a hablar de sus razones, a defenderse, e incluso a su derecho a la simpatía y al apoyo , y comparada con la voz débil de la propaganda iraquí, que retrató a Bush como el "gran Satanás" que era un malvado más allá de la redención, la imagen de Saddam como un agresor enloquecido por la guerra fue representada de una manera mucho más convincente. “Fueron precisamente los medios desequilibrados con las fuerzas militares desequilibradas con un preciso uno-dos a Irak en el campo de batalla y moralmente, y esto selló la derrota de Saddam” y agregan que “Después de que "Tormenta del

desierto" barriera el Golfo, ya no sería posible confiar solo en la fuerza militar sin la participación de los medios de comunicación para lograr la victoria en una guerra" ((Qiao y Wang, Unrestricted Warfare, 1992, pág. 61 y 62)

La opinión pública tomó cada vez más importancia, hasta que alguien se dio cuenta que si se la manipulaba, era una formidable arma política. El dominio y control de los pueblos se lleva a cabo mediante técnicas de manipulación. Sandalio y Arauz enumeran algunas de esas estrategias de manipulación, a saber: crear problemas, después ofrecer soluciones; la estrategia del "poco a poco" o la degradaciyn progresiva; la estrategia del acontecimiento inevitable y la resignación; dirigirse a un público infantilizándolo; utilizar el aspecto emocional y no la reflexión; mantener al público en la ignorancia y la mediocridad; reemplazar la acción revolucionaria por la culpabilidad y el individualismo; conocer a los individuos mejor de lo que se conocen a sí mismos; controlar la democracia; y manipular el lenguaje.(Sandalio y Arauz, 2004)

Fue a partir de 1995 cuando el progreso inaudito de las Tecnologías de Información y Comunicaciones hizo posible llegar a todo el mundo instantáneamente.

LA INFORMACIÓN DESPUÉS DE LA PROLIFERACIÓN DE LAS TICS

Esta proliferación ocurrió en el último cuarto del siglo XX, y se dio casi al mismo tiempo que con la importancia que adquirió la opinión pública. Como se ha visto hasta ahora, la vida del ser humano transcurre absorbiendo información. Creemos en lo que creemos porque nos han informado. No hemos estado en Nueva Zelanda, pero sabemos que existe. No hemos estado, pero hemos visto videos, fotos y mapas. No hemos estado en Vietnam, pero sabemos que existe y que allí hubo una guerra sangrienta.

Todo es información. Nos comportamos, resolvemos y decidimos conforme a la información que recibimos, que suponemos es cierta. Si la información es errónea, o falsa, se decidirá mal. Se tomará por beneficioso lo que en realidad es malo para nosotros. Es el reino de los lobos vestidos con piel de oveja. Una persona inteligente puede transformar casi todo en un arma: información sobre refugiados, información sobre tendencias en elecciones, ciclos de elecciones, dinero, la ley o cualquier aspecto de una relación social.

El primer indicio que cosas que veíamos podían no ser ciertas es cuando pudo filmarse en celuloide hechos de la vida real, y luego verlos en pantalla. Luego

aparecieron los videos, y una posibilidad: editarlos, y luego reproducirlos mostrando una realidad falsa. Hay que ser muy experto para darse cuenta cuando un video ha sido editado. Poca gente sabe que un actor filma diferentes escenas de una película, y luego el contenido es editado según la secuencia que quiere mostrar el Director, no se filma en la secuencia que aparece en la película porque el cambio de vestuario y de escenarios sería muy costoso.

> No obstante, cualquier movimiento que hacemos en la red, cualquier exploración en los buscadores de Internet, cualquier página que visitamos o cualquier comentario que hacemos en las redes sociales virtuales proporciona una información muy valiosa para perfilar nuestra personalidad mediante la identificación de preferencias, gustos, intereses, ideología, estado civil, nivel educativo y cualquier otra información que pueda ser de interés para empresas, gobiernos, servicios de seguridad o delincuentes. Además, la agregación de estas informaciones procedentes de múltiples fuentes junto con los datos personales, bancarios, administrativos, económicos o académicos sienta las bases del Big Data [23], que en los próximos años se convertirá -si no lo ha hecho ya- en el "Gran Hermano" de la Era de la Informaciyn y donde nadie que tenga una identidad digital y presencia en la red podrá escapar a su control casi absoluto.(Chamorro y Colom Piella, 2015, pág. 592)

En esta parte de la investigación no se hará referencia las dos concepciones de OI, una que sostiene que son un complemento de las operaciones militares convencionales, y otra que sostiene que se desarrollan en época de paz en todos los niveles inferiores a la confrontación violenta. Se van a analizar los medios artificiales para influir en la opinión pública, transformándola en lo que se denomina "opiniyn mediática".

Uno de los aspectos más destacados de las campañas de información son los medios de prensa y electrónicos, desde la radio y TV hasta Internet. Otro de los aspectos más destacados de la campaña de información en la conciencia pública occidental son las actividades de los trolls (personajes en línea dirigidos por humanos) y bots

[23]Por Big Data se entiende al proceso de gran cantidad de datos y volúmenes de información, estructurados y no estructurados. Por su forma de hacer negocios, Uber y Netflix usan en su gestión comercial gran volumen de información relacionada.

(ejecutados por procesos automatizados), que interactúan directamente con los lectores en una variedad de medios.(Keir Giles, Russian Handbook of Information Operations, 2015, pág. 54)Ambos persiguen la misma finalidad: dar idea de consensos y opiniones públicas generalizadas, para esgrimir clamores populares y poder hacer lo que se desee para llegar, ejercer y mantenerse en el poder.

Los medios de prensa visual, oral y escrita son un negocio, que debe producir dinero para satisfacer las necesidades de empresa. Sin embargo, a partir de su uso en OI, también son una ideología. De manera tal que hay que coordinar ambas premisas, y ya se puede ver empresas de medios que son vendidas supuestamente con presiones, y cambian el sentido de la información. No es lo mismo difundir como noticia urgente por TV una "feroz represiyn policial en la estaciyn de trenes XX", a decir "vándalos destruyen las instalaciones de la estaciyn de trenes XX". El lenguaje se manipula con facilidad y pasa inadvertido. Una cosa es decir que "el delincuente fue abatido por las fuerzas del orden" a decir "el delincuente fue asesinado por las fuerzas del orden". Hay palabras que por el uso malintencionado frecuente, pierden su significado original. Esa es una técnica de manipulación a través del lenguaje.

Los engaños son múltiples. Cierta vez un periodista de la estación pro gubernamental denunció haber sido agredido por partidarios del gobierno anterior, pero otro periodista demostry que el mismo "agresor" tenía nombre y apellido y era un partidario del gobierno que simulaba ser de la oposición. De esa forma, a propósito se buscaba manipular a la opinión pública.

La principal finalidad de los medios de prensa oral, escrita y televisiva no solo es informar sobre los hechos, sino formar opinión. Esto se nota en los numerosos comentarios de los reporteros, con los que adornan la difusión de un hecho. Estos comentarios tienen toda una tendencia ideológica. Algunos se revisten del ropaje de la neutralidad, como la BBC de Londres, o la CNN en Atlanta, o el Canal de Televisión Rusia TV, que son órganos de comunicación estratégica.

Además, con la aparición de internet, los medios dejaron de ser verbales y televisivos, para usar el espacio cibernético a través de la Internet, en las denominadas redes sociales, y en su aprovechamiento.

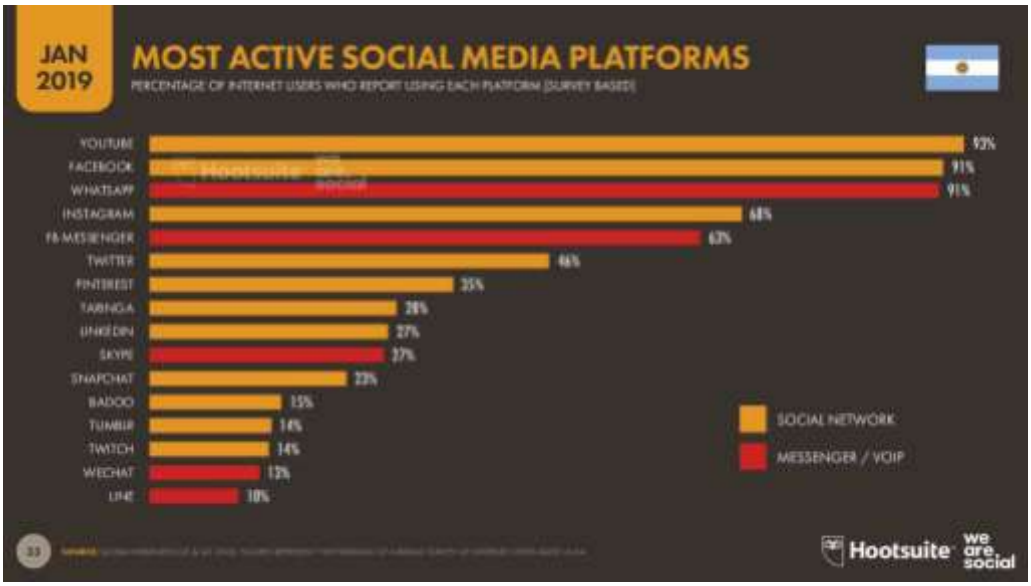
LAS REDES SOCIALES Y LA OPINIÓN PÚBLICA

Las redes sociales son estructuras formadas en Internet por personas u organizaciones que se conectan a partir de intereses o valores comunes. A través de ellas, se crean relaciones entre individuos o empresas de forma rápida, sin jerarquía o límites físicos.

El proceso de construir capacidades en los medios sociales es visible en las cuentas de medios sociales con un gran número de seguidores, como Facebook o Twitter. Se ha argumentado que, además de la desinformación patrocinada por los gobiernos, el uso de trolls y bots de esta manera también puede explicarse por ejercicios de marketing. Las formas de las tácticas, técnicas y procedimientos para el delito cibernético son iguales a los que son utilizados para el espionaje cibernético, por lo que el marketing, por un lado, y la desinformación, por el otro, también usan las mismas técnicas. Ya hay ejemplos disponibles de cómo la transferencia entre un dominio y otro es perfecto. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 70)

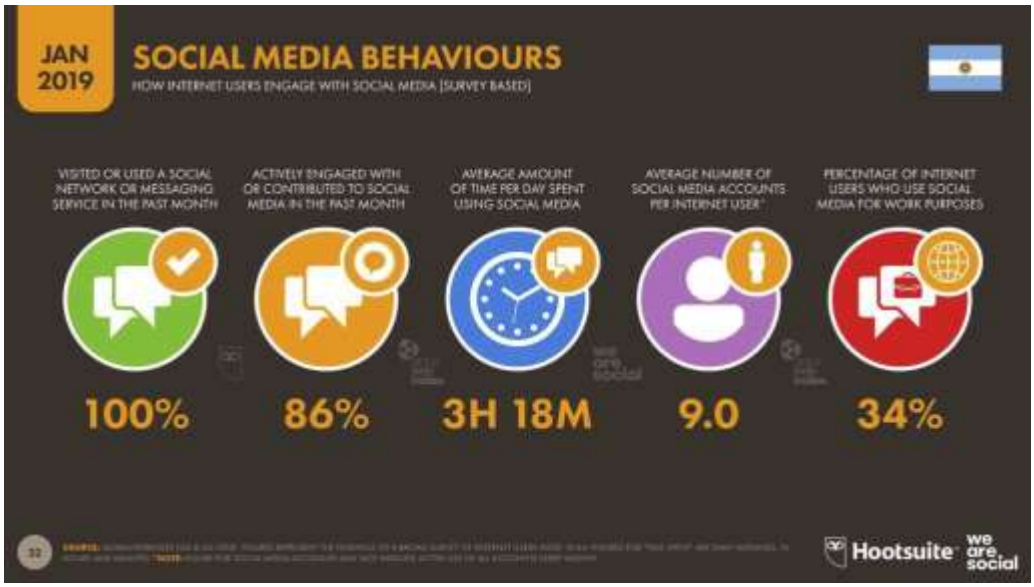
Hay que estar preparado a que se difundan mensajes falsos a gran escala, dirigidos a individuos seleccionados. Hoy es fácil seleccionar personal como blanco, porque identidades y credenciales pueden ser fácilmente falsificadas por cualquier Proveedor de Servicios de Internet (Internet Service Provider - ISP). Estas son vulnerabilidades que incluyen recoger datos de elementos electrónicos personales, porque nadie lee las condiciones de las aplicaciones que baja, y las acepta sin mayores trámites.

Muchas personas creen que las redes sociales y la denominada social media son lo mismo y que los términos se pueden utilizar como sinónimos, pero no es cierto. Social media es el uso de tecnologías para hacer interactivo el diálogo entre personas, mientras que red social es una estructura formada por personas que comparten intereses similares, como ya detallamos en el ítem anterior. Lo llamativo de estas redes sociales y social media, es que es un conducto de dos vías, entre el que habla y el que recibe la comunicación. Se permite el intercambio de opiniones, se promocionan actitudes y muestran tendencias de opinión.



Fuente: https://yiminshum.com/digital-social-media-argentina-2019/

Específicamente en el ámbito militar, las redes sociales son empleadas en apoyo a la preparación del espacio de batalla, promoviendo relatos, alterando las percepciones o popularizando puntos de vista que faciliten la obtención de los estados finales políticos.



Fuente: https://yiminshum.com/digital-social-media-argentina-2019/

Según el científico político Ronald J. Deibert, el uso de las redes sociales para controlar, confundir, engañar y dividir a un público es tan efectivo en manos de quienes buscan el poder en una democracia, como lo es para los regímenes autoritarios. Hoy en día, todas las autocracias en el mundo exigen que las compañías extranjeras ubiquen sus dispositivos de almacenamiento de datos en su territorio nacional, donde el gobierno puede entrometerse y controlar lo que sale o entra. No obstante, las autocracias no son las únicas que hacen esa demanda. La manipulación autoritaria de las redes sociales trasciende las fronteras, y las formas de gobierno. (Deibert, 2019)

Debido a los cambios recientes en los medios, la tecnología y la cultura, la población juega un papel aún más vital en los conflictos no convencionales del siglo XXI. Es una era de cobertura de noticias las 24 horas del día, donde la población, ayudada por teléfonos inteligentes, televisión por cable y redes sociales, puede rastrear lo que pretenda con una frecuencia sorprendente. Las personas están más conectadas, pero también pueden ser más volubles en su opinión. Se ven inundadas por distracción tras distracción: desde el último rumor sobre una controversia política creciente, pasando por el conflicto emocional de bailarinas, hasta una próxima tormenta eléctrica que puede cancelar los deportes que se pasan por TV, los períodos de atención de los espectadores son cortos y de allí deviene la costumbre del "zapping"[24]. Aún más preocupante, la población es susceptible a la desinformación. En la búsqueda interminable "zapeando" diferentes programas de televisión, las redes de horario estelar promueven "historias de última hora" sin validar adecuadamente su precisión, con analistas "expertos" en la pantalla cuyas observaciones pueden ser influidas por la emoción o el impulso que se transmiten a los espectadores en casa. Todos estos factores plantean un desafío particular para el liderazgo militar y político que participa en una guerra híbrida.

Las redes sociales son un arma bondadosa nueva, anticipada por Qiao y Wang. A mediados del siglo XX, en Occidente se comenzó una concepción cultural en forma de gobierno, llamada democracia. En realidad, bajo este nombre ya no se refería a una forma de gobierno, sino a una forma de vida de la sociedad. Este cambio cultural está descripto muy pormenorizadamente por Alberto Schiuma, cuando dice:

[24]Cambio rápido y continuo del canal del televisor por medio del mando a distancia o control remoto.

> [La democracia] Ya no es más una forma de gobierno, sino una forma de estado, un modo de ser, un estilo de vida caracterizado por el respeto a la persona humana, a su libertad, su igualdad de especie ante la justicia y ante la ley. Sería aquella forma de estado que realiza la convivencia política en la libertad, dentro del ordenamiento divino y humano.(Schiuma, 1976, pág. 19)

Se identificó el sistema republicano de división del poder, de controles y equilibrios, de las garantías individuales ante los avances del poder, de la libertad de reunión, de la libertad de expresión, del derecho a no ser juzgado con ley posterior al hecho que se imputa, del derecho al libre tránsito, con la forma de gobierno democrático y la expresión de la voluntad popular. Esta democracia es electiva, y luego deviene del voto de las mayorías. Por lo tanto, si se influye en el deseo de las mayorías, se accederá al poder en forma democrática, así que todo consiste en influir esa opinión. Esta figura de la democracia hizo surgir una importancia descomunal a una técnica de evaluación de opinión denominada "encuesta".

Encuesta significa según el diccionario RAE, "un conjunto de preguntas tipificadas dirigidas a una muestra representativa de grupos sociales, para averiguar estados de opinión o conocer otras cuestiones que les afectan." Si la democracia era el reino de las mayorías, todo consistía en modificar la opinión de esas mayorías y de esa manera, mediante lo denominado "ingeniería social", construir poder consensuado por las mayorías.

A la opinión pública se la puede manejar con ingeniería social. No es intención de este trabajo describir las formas de ingeniería social, pero el concepto básico es que

> La Ingeniería Social se sustenta en un sencillo principio: "el usuario [de la informaciyn] es el eslabyn más débil". Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla.(Sandoval Castellanos, 2004)

Con la proliferación de las TICs, se logró algo impensado: crear realidades inexistentes mediante percepciones erróneas. Repitiendo una información, se crea una

cámara de eco de las noticias, donde a una afirmación surgen varias desmentidas y se desconoce la verdad real. Este disfraz de la información real se difunde mediante información falsa, (fakenews) y desinformación.[25] La aceptación de lo que se difunde se logra mediante las redes sociales, los influencers, los trolls y a los bots.

LA DIVULGACIÓN DE INFORMACIÓN FALSA.

La información falsa se crea para generar visitas a sitios web, desprestigiar, desinformar y manipular la opinión pública. Existen sitios que permiten crear noticias falsas y compartirlas por las redes sociales como si fuesen reales. Se pueden agregar imágenes, un título, se elige una URL falsa o se la disfraza en su ortografía falsa por una verdadera muy parecida. Las personas a las que se quiere engañar difunden (viralizan es el término nuevo creado) las noticias falsas creyendo que son verdaderas a través de las redes sociales, servicios instantáneos como Whatsapp o Telegram, blogs u otros medios de comunicación masiva.

Las noticias falsas pueden ser elaboradas con la intención de mentir (disinformation) o ser lisa y llanamente errónea (misinformtion). Aunque en el idioma español no se hace la diferencia, se la hace en el idioma inglés.

Las noticias falsas las pueden escribir personas que quieren dañar reputación de otras, generar sensacionalismo, generar reacciones sociales, o personas que quieren ganar dinero. Para poder detectar si una noticia es verdadera o real, hay que tomar algunas precauciones, como investigar la fuente de la noticia, ver quién es el autor, leer toda la noticia completa y no quedarse con el título, ver la fecha de publicación, controlar bien la ortografía del sitio web o buscar la misma noticia por otros medios.(Argentina gob ar, 2020). El común de las gentes no se toma este trabajo, y cree la primera noticia que lee.

Los influencers son agentes de marketing en el campo de los negocios, y difusores de popularidad falsa en el ámbito político. No se tratará aquí el rol de los influencers en el marketing del campo de los negocios, pero si en el rol que les cabe en crear opiniones falsas predominantes en una sociedad, que luego darán lugar a encuestas que los políticos seguirán

[25] Como existe mucha literatura en idioma inglés, se debe estar alerta que en ese idioma y en el ámbito militar, *disinformation* es información con intención de engañar, y misinformation es información errónea sin malicia

ciegamente. Entonces ha ocurrido que el resultado práctico de una elección no es el que indicaban las encuestas, como ya ha ocurrido en dos o tres lugares del mundo.

Esta acción premeditada de influencers se ha transformado ya en una forma primitiva. Consistía en abrir varias cuentas falsas de lectores de medios de prensa, y opinar tendenciosamente sobre un hecho en particular, para dar idea de consenso sobre un tema. Era fácil de identificar porque los autores, aunque de diferentes nombres, los invadía la pereza y se limitaban a cortar y pegar el mismo comentario en varios diarios digitales.

Los trolls

Según el diccionario de la Real Academia Española, un troll es un personaje de la mitología escandinava, un monstruo maligno que habita en bosques o grutas. En la jerga de Internet se usa para referirse a una persona que se dedica a realizar comentarios provocadores, que busca crear controversia o desviar la atención de una temática con el fin de captar miradas o porque, simplemente, quiere causar cierta molestia. Es una persona con identidad desconocida que publica mensajes provocadores, irrelevantes o fuera de tema en una comunidad en línea, como pueden ser un foro de discusión, sala de chat, comentarios de blog, o similar, con la principal intención de causar molestia o generar animadversión hacia la noticia que se publica, y de esa manera generar respuestas En realidad, lo que hace es difundirla noticia.

Una cuenta falsa de troll puede servir para distribuir desinformación, y sembrar argumentos y confusión, creando a propósito una imagen para mostrar discordia. Estos trolls también sirven para atemorizar a periodistas, investigadores o autores de opiniones contrarias al pensamiento único que debe imperar. Sin embargo, no existe una línea divisoria que pueda ser fácilmente identificable entre una campaña de trolls orquestada, y una genuina opinión contraria, aún equivocada.

> La gran mayoría de la población del país víctima ni siquiera sospecha que está siendo sometido a influencia psicológica de la información. Esto lleva a su vez a una paradoja: el agresor logra sus objetivos políticos y militares con el apoyo activo de la población del país que está siendo sometido a influencia. El control sobre recursos estatales estratégicamente importantes se entrega voluntariamente, ya que esto se ve no como resultado de la agresión, sino como

> un movimiento progresivo hacia democracia y libertad.(Keir Giles, Russian Handbook of Information Operations, 2015, pág. 56)

Las granjas de trolls

Las granjas de trolls son agrupamientos de trabajadores a sueldo, cuyo cometido es generar información en Internet, foros y redes sociales. Al respecto, citan a la agencia rusa Internet Reasearch Agency (IRA), con asiento en San Petersburgo.

> Esta agencia emplea identidades y perfiles falsos en redes sociales, registrados y con contenido y apariencia real. Se vale de foros de debate, sitios web, periódicos digitales y páginas de vídeos y contenido multimedia para impulsar los intereses de Moscú en relación a la política interior y exterior como pueda ser Ucrania, Latinoamérica, EE. UU u Oriente Medio. De hecho, ya ha sido acusada de haber actuado en Estados Unidos durante la elección de Donald Trump, en Reino Unido en el referéndum del Brexit, en Francia durante la elección de Emmanuel Macron y en España con el referéndum sobre la independencia de Cataluña. […]Los empleados de la Agencia,[…] tienen presencia en cualquier rincón de Internet incluso en sitios vagamente visitados, allí producen todo tipo de contenido tal como comentarios, fotos o vídeos. Los trolls poseen un listado, a modo de itinerario o instrucciones, sobre los temas en los que tienen que centrase cada día. En su caso, su principal cometido durante el tiempo que estuvo activa en la IRA, fue difundir noticias negativas y manipuladas sobre Ucrania.(Romero Sanchez, 2020)

Es difícil verificar la exactitud de esta información. Según otras fuentes de Internet, durante la elección de Trump esta IRA fue hackeada por Estados Unidos.(Padinger, 2019) También se cita como otra “granja de Trolls” a Cambridge Analytica, a la que se acusa de manipular las últimas elecciones de EEUU.

¿Qué es un Bot?

Un bot(aféresis de robot) es un programa informático coordinado que intenta imitar el comportamiento humano a través de interacciones. Por ejemplo, un bot puede manipular los resultados de búsqueda devueltos por varios motores de búsqueda como Google. Estos métodos se pueden usar para elevar un tema a "tendencias principales",

que a menudo se destacan en la parte superior de los resultados de búsqueda o en las plataformas de redes sociales.

Muchos usuarios simplemente confían en estos "resultados principales" para formular sus percepciones o posiciones iníciales de un evento en particular, sin un examen riguroso de todas las fuentes de información. En resumen, existe una forma técnica de filtrar la información en las redes sociales, respecto un tema de interés. Por si alguien no se da cuenta, cuando se "googlea" sobre un tema, los artículos encontrados superan los miles, pero siempre hay algunos que aparecen al principio de la pantalla. Esos son los consultados, y se descarta al resto sin leerlos. La investigación informática muestra que la mayor parte del tráfico de Internet, especialmente en las redes sociales, es generado por "botnets".

Las búsquedas de datos se lleva a cabo por motores de búsqueda de internet y hay varios: google, yahoo, baidu, safari, bing, ask, AOL y otros. Cada motor de búsqueda tiene algoritmos de selección diferentes, y es por eso que al buscar el mismo tema en diferentes buscadores con diferentes algoritmos, la precedencia de los sitios es diferente. Esa es la razón por la cual cuando se visita un video de youtube, el autor pide que se le coloque un "like", para subir en la precedencia.

Numerosos bots simplemente repiten el mismo artículo después de copiarlo en varios sitios web y blogs, haciéndolos parecer como si los artículos se hubiesen publicado de forma independiente en diferentes URL de sitios web. En otras palabras, los robots clonan la información [errónea], creando un eco de noticias falsas. (Perceptions are Reality, 2018, pág. 166)

En la obra "Perceptions are reality" se pone como ejemplo el uso de botnets en la crisis de Ucrania. Para identificar estos botnets, se usan programas informáticos descriptos abajo. Dice que

> "A menudo, el contenido (por ejemplo, informes, imágenes, videos y artículos) se originó en un sitio de redes sociales y se difundió a muchos otros sitios sin indicar la fuente en forma fehaciente. Para ilustrar este punto, los investigadores rastrearon múltiples sitios populares de redes sociales en un intento de identificar las fuentes y sus interconexiones implícitas. Las palabras clave "Ucrania", "Crisis de Ucrania", "Euromaidan", "Automaidan" y "Protestantes de Automaidan de Ucrania" se utilizaron para recopilar datos sobre la crisis. Primero, se identificaron publicaciones de blog populares para el

> conflicto entre Ucrania y Rusia, y luego se hicieron referencias cruzadas de estas publicaciones con datos de Twitter para encontrar las publicaciones que más se difundieron en Twitter. Luego, se utilizaron herramientas como Tweet Tracker y NodeXL para recopilar datos de Twitter para el período de investigación entre el 29 de abril de 2014 20:40:32 y el 21 de julio de 2014 22:40:06 UTC, que coincidió con el [evento]. Esta serie de métodos las consultas dieron como resultado 1.361 tweets únicos, 588 usuarios únicos de Twitter y 118.601 relaciones (incluidos los siguientes, menciones, respuestas y tweets) entre estos usuarios." (Perceptions are Reality, 2018, pág. 166)

Técnicamente existen metodologías para identificar botnets cuyo contenido se distribuye por nodos. Esas metodologías son aspectos técnicos que están descriptas en el Capítulo 10 Evolución de los Botnets durante las Operaciones de Combate Modernas a Gran Escala, del libro Perceptions are reality, escritos por el Teniente Coronel Rick Galeano y otros.(Perceptions are Reality, 2018, pág. 167 a 169).

Se ha introducido un nuevo medio artificial, los bots sociales, en un ambiente de información en constante evolución para dar forma e influir en las percepciones y desencadenar un cambio de comportamiento en una escala exponencialmente masiva en todo el mundo. El objetivo es influir en el ambiente de la información amplificando las redes sociales

> Los bots sociales son códigos escritos que imitan a los usuarios humanos y sirven como súper difusores de información. Estos bots sociales se pueden usar para promover puntos de vista particulares, fabricar la percepción de popularidad o punto de vista popular, confundir el discurso y el espacio narrativo, y / o servir como un medio para reforzar estos puntos de vista mediante la promoción de blogs u otro contenido digital. Los efectos pueden variar en las dimensiones físicas, cognitivas (en otros lugares se le llama dimensión humana) e informativas para desencadenar en última instancia comportamientos específicos en individuos y grupos que impactan el entorno donde se opera de una manera que es beneficiosa para aquellos que operan los bots.(Perceptions are Reality, 2018, pág. Cap 10 pag 163)

Los bots son capaces de interrumpir la infraestructura al sobrecargar las redes o alojar plataformas con un diluvio de información; o podrían transportar fácilmente

malware o virus molestos para negar o degradar un sistema objetivo. Debe notarse los efectos que estos bots pueden causar en el Comando y Control de fuerzas militares donde las comunicaciones seguras pueden llegar a ser la diferencia entre el éxito y el fracaso.

También los bots pueden corromper y / o interrumpir la forma en que la información se recibe, procesa y / o difunde a través de sistemas de comando y filtros humanos, lo que limita efectivamente el empleo óptimo del poder de combate. Contrariamente a lo que se cree, los efectos populares dentro del ambiente de la información no se generan únicamente a través de efectos no cinéticos; más bien las funciones de combate particularmente los fuegos y las maniobras, ya sea con intención o sin ella, producen efectos en el ambiente de la información.

Debe notarse que los bots generan percepciones que el público recibe de cualquiera de los mensajes y el comportamiento resultante basado en esos estímulos. Los mensajes repetidos de lo que parece ser una variedad de fuentes independientes crean una repetición en la mente de individuos o en determinados grupos. Asimismo, las diferentes formas de difundir un mensaje y su frecuencia de difusión, la variedad empleada en la difusión de un mensaje y la frecuencia con la que se difunde ese mensaje en algunos casos son tan importantes como su contenido, para generar una multiplicación de influencias para cambiar los comportamientos. (Perceptions are Reality, 2018, pág. 163)

Lo que se busca es crear un falso ambiente de consenso y mayorías, para fomentar un ambiente permisivo o tolerante. Esto puede lograrse no solo por la repetición de mensajes por trolls y bots, sino por la ausencia de noticias cuando existen hechos que no se difunden naturalmente. Aquí el principio es que si un hecho no se difunde, es como si no hubiese ocurrido.

En el artículo “Redes Sociales y Fuerzas Armadas, ¿Oportunidad o riesgo? Sus autores sostienen que

> Los avances tecnológicos que se han producido desde la década de 1970 en los campos de la informática, las telecomunicaciones o la robótica han cambiado nuestras vidas. No sólo estamos rodeados de muchos productos tecnológicos que facilitan y simplifican nuestro día a día; sino que también estos mismos productos han creado un mundo más interconectado y globalizado que nunca, una sociedad en red cuya característica fundamental es que ingentes volúmenes

> de información pueden transmitirse de forma casi instantánea a cualquier punto del globo, con un coste irrisorio, con una facilidad asombrosa y sin precisar de grandes bibliotecas físicas para almacenar tantos volúmenes de información. Ésta ha sido la base sobre la cual se ha erigido la Era de la Información y está siendo reemplazada por la Era del Conocimiento.(Chamorro y Colom Piella, 2015, pág. 592)

El uso de los medios sociales ha cambiado del entretenimiento del público, a ser una herramienta para influenciar grupos de opinión o lograr objetivos políticos en el umbral inferior a la violencia, esparciendo propaganda o desinformación. Estos actos son parte de la denominada Guerra Híbrida, la que incluye medios violentos convencionales, no convencionales, no gubernamentales y delictivos.

El panorama podría ser bastante sencillo, si no se entremezclase con el uso de bots, que incluyen en el ámbito de la información medias verdades, hechos retorcidos, imágenes manipuladas y videos que son recogidos en diferentes páginas de internet y URLs para pasar una doble verificación artificial. Las otras plataformas sociales como Facebook y Twitter son solo un mecanismo para guiar a los lectores en la dirección que se desea. Así se generan historias creíbles.

La supuesta confidencialidad de datos

En la teoría, todos los datos volcados en internet tienen la advertencia que se resguarda la privacidad. Las redes de intranet invocan la preservación de los datos personales, y de las opiniones, y cada vez que se baja alguna aplicación el usuario debe estar conforme con el acuerdo de privacidad, que se da por leído y casi nadie lee. Las redes de intranet se acusan mutuamente de no respetar la privacidad de los usuarios, pero la experiencia ha demostrado que hasta en Internet, no hay nada asegurado ni reservado. Occidente acusa a Rusnet (la intranet rusa) y a QQ (la intranet china) de usar esos datos para controlar a su población, pero ya existen varios casos que prueban que en Internet de Occidente nada es confidencial. Los datos de todas las personas están en la web, y no necesariamente para que sean conocidos se debe recurrir a la piratería informática. Tal fue el caso de Cambridge Analytica (una empresa de Big Data), que según los datos disponibles era propietaria también de Facebook, Instagram y WhatsApp, y que aparentemente fue usada con fines electorales en Estados Unidos.

Ese no fue el único caso de vulneración de privacidad en las redes occidentales. . Ello se vio reflejado en los casos de Julián Assange y Edward Snowden, que se hicieron conocidos mundialmente por filtrar información clasificada del gobierno de Estados Unidos y revelar secretos sobre su accionar. Tanto Assange como Snowden hicieron público a la prensa de proyección internacional sobre esos asuntos, para propagar la información que hasta ese momento era desconocida. Ambos esgrimían como causa la acumulación desmesurada e incontrolada de información por parte del gobierno y en cierta manera conductas abusivas del servicio de inteligencia que consideraban que ponían en riesgo el sistema democrático y dejaban en evidencia abuso de poder, aunque el gobierno de Estados Unidos los acusaba de ser funcionales a los intereses rusos.

COMO REGULAR LA INFLUENCIA DE LOS MEDIOS SOCIALES

Tal cual se cita en el libro Perceptions are reality, como epígrafe del Capítulo 11, el Deputy Secretary of Defense 2017/2019 Patrick M. Shanahan expresó que

> El impacto de largo alcance de las redes sociales, la expansión de la tecnología de la información, la disponibilidad generalizada de comunicaciones inalámbricas y las campañas de influencia de la competencia han afectado en gran medida las operaciones militares y han cambiado el carácter de guerra moderna.

La velocidad instantánea y el alcance mundial de las redes sociales, junto con el rápido ritmo de las interacciones entre un conjunto grande de usuarios, muchos de los cuales no verifican la veracidad de la información que reciben y la retrasmiten sin pensarlo mucho, crean las condiciones adecuadas para la manipulación masiva de las sociedades y las personas dependientes de la tecnología. Lo más probable que ocurra es que la mayoría crea sinceramente que el contenido es verdadero.

En cuanto a la influencia de los bots en el medio militar, el libro Perceptions are Reality puntualiza que

> En los niveles estratégicos y operacionales de la guerra, las plataformas de redes sociales que son manipuladas por bots pueden cambiar las opiniones internacionales y regionales sobre el uso de la fuerza militar o la validez de las operaciones militares en una región. En el nivel táctico, la propaganda de redes

> sociales inducida por bots podría potencialmente usarse para persuadir a personas susceptibles para que interrumpan o retrasen las operaciones militares mediante protestas u otras resistencias pasivas.(Perceptions are Reality, 2018, pág. 169)

Los líderes militares deben comprender que la narrativa puede ser fácilmente manipulada e influenciada por bots y trolls. La mayoría de los usuarios de las redes sociales no pueden diferenciar entre cuentas reales y cuentas de bot falsas. Debido a que los bots sociales pueden emplearse clandestinamente en un contexto de bajo costo y bajo riesgo, lo más probable que ocurra es que se pueda encontrar una mayor cantidad de propaganda en las redes sociales generada por un adversario.

Como se ha dicho anteriormente, el uso de las redes sociales afecta tanto al ámbito militar como al ámbito civil. Usando las redes sociales, se puede influir y manipular los comportamientos militares y los comportamientos civiles. Entre los principales efectos de las redes sociales se encuentran las Operaciones Psicológicas. En la actualidad, y luego de la Guerra de Vietnam en el Ejército de Estados Unidos se suprimió la frase Operaciones Psicológicas como operación militar, y se la ha reemplazado por Operaciones de Apoyo de Información Militares (MISO por su sigla en inglés), pero los grupos que llevan a cabo las MISO se continúan llamando Grupos de Operaciones Psicológicas. Los operadores de operaciones psicológicas son definidos como pensadores adaptativos que se especializan en capacidades no convencionales, experiencia cultural, dominio del idioma, engaño militar, guerra cibernética y técnicas avanzadas de comunicación en todas las formas de medios.[26](Perceptions are Reality, 2018, págs. 92 y nota 6, pág 102)

Las MISO buscan influenciar las percepciones, los sentimientos y los comportamientos de las audiencias. Para ello, determinan los factores psicológicos clave en el ambiente operacional; identifican acciones con efectos psicológicos que sean capaces de causar, cambiar o reforzar comportamientos deseados en grupos o individuos objetivo identificados; moldean las percepciones de la población para apoyar los objetivos de la guerra no convencional; y contraatacan informaciones "falsas" o

[26]Ver https://goarmysof.com/PsyOp/PsyOprecruiting.html

"difamadoras" del enemigo que puedan debilitar las acciones de guerra no convencional.

En el ámbito civil

Hay varios documentos que tratan sobre las estrategias de manipulación, que ya han sido mencionadas al inicio del Capítulo III, entre ellos el artículo ya mencionado de Sandalio Francisco y Arauz Manuel, (2004) Técnicas de manipulación, artículo publicado en la Revista Autogestión, Octubre/ Noviembre de 2004.

Asimismo, la preocupación por la difusión de la manipulación y la desinformación se expresa en The Forumon Information and Democracy, organización formada por grupos de alrededor del mundo que incluye a Reporters Sans Frontiers and the Human Rights Center, del 12 de Noviembre del 2020, que han llegado a 250 recomendaciones para hacer frente al problema, porque "el caos de la información impone un riesgo vital para las democracias". (Hurst, 2020)

El tema es frondoso y ameritaría una investigación por separado en especial por las técnicas cibernéticas que se aplican. Sin embargo, como menciona Sean Mc Fate, el problema escala al nivel de la comunicación estratégica, ya que es un tipo de guerra diferente a la que estamos acostumbrados porque no se concentra en la soberanía geográfica de los Estados. Al respecto, refiriéndose a Estados Unidos, dice.

> Se deben cultivar otros instrumentos de poder nacional, tal como el dominio de la información, las sanciones puntuales que estrangulan financieramente a las élites enemigas, la mensajería estratégica para ganar la batalla de la narrativa, la diplomacia pública que habla directamente a las poblaciones, la fuerza que proporciona una negación plausible, y los sobornos para cambiar la mente de los adversarios para que no tengamos que dispararles. Este es el trabajo de la comunidad de inteligencia, los Departamentos del Tesoro y de Estado, y la Agencia de EEUU para el Desarrollo Internacional (USAID)(McFate, The New Rules of War in the Age of Durable Dirsorder, 2019, pág. 42)

En el ámbito militar

El uso de redes sociales afecta la ejecución y la seguridad de las propias operaciones militares. Según citan Chamorro y Colom Piella, en las Fuerzas de Defensa de Israel, "aproximadamente el 70% de sus oficiales y suboficiales y el 95% de su tropa disponen de perfil personal en Facebook. No obstante, su uso inadecuado provocó que en el año 2013 se prohibiera a los soldados pertenecientes a unidades de inteligencia y operaciones especiales compartir en las redes sociales virtuales fotografías que revelasen su condición de militar, máxime tras algunos episodios que pusieron en peligro la seguridad". (Chamorro y Colom Piella, 2015, pág. 594). Pero esto no es la única amenaza. Agregan que

> El servicio de mensajería instantánea WhatsApp también ha sido una importante fuente de problemas para las IDF y no debe descartarse que esta aplicación o sus equivalentes Telegram o Line puedan plantear graves problemas de seguridad para sus usuarios militares. De hecho, en 2013 doce oficiales de la Fuerza Aérea Israelí fueron condenados por compartir información clasificada como planos y coordenadas de vuelo, a través de esta plataforma. Y más recientemente, durante la Operación Margen Protector que se desarrolló en la franja de Gaza en verano de 2014, varios soldados fueron detenidos tras difundir a través de la misma red fotografías de varios soldados israelíes caídos en combate durante la incursión terrestre en Gaza(Chamorro y Colom Piella, 2015, pág. 594)

Además de la amplia influencia en la formación de la opinión pública, la mayoría de las aplicaciones modernas permiten la geolocalización de las emisiones, tanto de las fotos como de los mensajes. Esto es una vulnerabilidad de importancia. Es por eso que aún en los países más desarrollados del mundo, ya existen restricciones para que las tropas porten aparatos de alta tecnología en las operaciones militares.

Según Rick Galeano y otros, en el Ejército de Estados Unidos, contrarrestar de manera efectiva la propaganda de redes sociales es una tarea que se encomienda a la Oficina de Asuntos Públicos, a la oficina de Operaciones Psicológicas y al Departamento de Seguridad de Operaciones. Estas organizaciones deben coordinar sus esfuerzos para hacer frente a la amenaza de propaganda habilitada para bots. Una vez que se identifican los bots y los trolls, las unidades del Ejército pueden usar las cuentas oficiales de las redes sociales de Asuntos Públicos para contrarrestar la propaganda

informando a las audiencias interesadas de la verdad. Sin embargo, se debe ser consciente que la información errónea o desviada pudo haber sido leída por un número no determinado de personas, pero que el número que se enterará de la desmentida oficial será mucho menor. (Perceptions are Reality, 2018, pág. Cap 10 pag 171). En última instancia, la duda será sembrada de cualquier forma.

Los militares de Estados Unidos están autorizados a usar las redes sociales, pero deben seguir ciertas normas. Las regulaciones incluyen ciertas actividades que no se deben hacer, como usar medios con derechos de autor; publicar detalles sobre la misión de su unidad asignada o los procedimientos de seguridad; anunciar ubicaciones y horarios de despliegues de su unidad; divulgar información sobre la muerte de un miembro del Servicio antes de que se notifique a los familiares y el Departamento de Defensa divulgue la información; publicar imágenes de equipos y equipos dañados; compartir grandes transacciones de personal (por ejemplo, información de pago, poder notarial, testamentos o información de implementación) y publicar el estado de la moral o problemas de personal.(US Army Social Media, 2020) Existe una Regulación AR 600-20, Army Command Policy, del 6 de Noviembre del 2014 que trata de aspectos de la disciplina y conducta en estos aspectos.(US Army Command Policy, 2014) Por su parte, la División Medios Sociales del Pentágono, del Jefe de Asuntos Públicos del Ejército, publica un Manual con Instrucciones detalladas.(US Army Social Media Division, 2016) Al analizar su contenido, se deduce que está dirigido a gente con experiencia en medios sociales. No pueden violar el Código de Justicia Militar ni las reglas básicas de conducta de un soldado, así como difundir comentarios negativos acerca de sus superiores. No pueden subir fotos con armas, aunque se encuentren con ropas civiles, y tampoco revelar su grado, nombre de la unidad donde revistan ni nada relacionado con su trabajo militar. No deben aceptar solicitudes de amistad de gente que desconocen y deben advertir a su familia que no deben comentar su profesión ni los lugares donde se encuentren desplegados. Todo esto se concentra en la capacidad de OI Compromisos de Soldados y Líderes (SLEs).

Todas estas medidas son parte de las operaciones de seguridad (OPSEC por sus siglas en inglés) en el ámbito de la información. El uso indebido de los teléfonos móviles también sirvió para identificar a los autores del derribo del avión Vuelo 17 de Malasia Airlines sobre territorio ucraniano, ya que “Igor Girkin, líder separatista de la autoproclamada República Popular de Donetsk, felicitándose en la red social Vkontktede haber abatido un avión de transporte ucraniano Antonov AN-26 cerca de la

ciudad de Torez..... un avión que resultó ser el vuelo MH-17de Malaysia Airlines y en el que murieron trescientos pasajeros" El autor olvidy que la foto digital que subiy a Internet era georeferencial, y así fue identificado. (Chamorro y Colom Piella, 2015, pág. 595)

El uso de Facebook también presenta riesgos. Las vidas de los soldados estadounidenses corren riesgo, advirtió el ejército de EEUU, a causa de las fotos geoetiquetadas (aquellas que indican el lugar donde fueron tomadas) en redes sociales como Facebook. Las Noticias de BBC Mundo alertan que

> En 2007, cuatro helicópteros militares estadounidenses fueron destruidos en Irak, después de que fotografías geoetiquetadas de estos fueran publicadas en internet. Al colocar fotos en Facebook o ingresar en redes sociales como Foursquare o Gowalla, los soldados podrían revelar el lugar exacto en el que se encuentra su unidad o su familia, señaló el ejército en un comunicado. La información se conoce un año después de que el mismo ejército advirtiera que este tipo de fotos pueden servir para alertar a delincuentes o terroristas. "¿Realmente quiere que todo el mundo sepa la ubicación exacta de su casa o la escuela a la que van sus hijos?" cuestionó el sargento Dale Sweetnam, de la División de Internet y Redes Sociales. "Antes de agregar la ubicación a un foto, los soldados deben de verdad dar un paso atrás y preguntarse '¿Realmente quién necesita saber esta información?'" (BBC Mundo, 2012)

Las redes sociales también son parte de las OI, porque generan efectos. El uso de redes sociales ha estado cambiando de entretenimiento a formar opinión pública, y de ese modo haciéndolas una herramienta preferida para influenciar grupos de opinión, o alcanzar objetivos políticos al difundir propaganda o información errónea acerca de variados eventos. En los niveles de guerra estratégico y operacional, las plataformas de redes sociales que son manipulados por bots pueden cambiar opiniones internacionales y regionales, sobre el uso de la fuerza militar o validar operaciones militares en una región. En el nivel táctico, la propaganda en redes sociales inducida por bots, potencialmente podría ser usada para persuadir a blancos vulnerables, afectar o demorar operaciones militares mediante protestas u otras resistencias "no letales".(Perceptions are reality, 2018, pág. 169)

Tanta importancia tiene la desinformación y la manipulación de la opinión pública a través de las redes sociales, que ya existen estudios para tratar de atemperar esos

efectos. Sin embargo, la mejor barrera para evitar la filtración parece ser las intranets regionales, como la red rusnet en Rusia, y qq.net en China. Por supuesto, se deja pasar la información que favorece y no se deja pasar la información que perjudica a cada sistema político.

Finalmente, tal es la vulnerabilidad de los medios sociales en el ámbito militar que el 6 de enero de 2020, la División 82 de Paracaidistas que se desplegaba en Oriente Medio se le prohibió llevar laptops y teléfonos móviles.(Kyle, 2020). También y según información periodística del diario Infobae de la Argentina, de junio 2020, Twitter cerró miles de cuentas ligadas a los regímenes de China, Turquía y Rusia utilizadas para hacer propaganda de desinformación. Según este medio de prensa, la red social señaló que había desactivado un "núcleo" de 23.750 cuentas vinculadas a los estados de esos países y retransmitido por otras 150.000 cuentas que sirven como "amplificadores". (Infobae, 2020)

> Además de usar la reunión tecnológica disponible, los enemigos potenciales pueden explotar las tecnologías de información para comunicarse con facilidad, a bajo precio, y en forma segura. Desde el comienzo de la revolución tecnológica, los insurgentes han hecho un uso intenso de las capacidades que ello proporciona. Los somalíes usaron teléfonos celulares para construir un sistema de comunicación barato. Fácil para establecer y usar, relativamente seguro si se usa tecnología de encriptado comercial e inmediatamente disponible, estos teléfonos simples minimizaron el contacto físico entre células y a su vez complicaron nuestros esfuerzos para rastrear las comunicaciones de los insurgentes. Los somalíes usaron una tecnología de comunicación ya lista, que ampliamente mejoró su reunión táctica, distribución, comando y control.(Thomas Hammes, 2006)

La aplicación TikTok de origen chino, donde se lo conoce como Doyuin, es una difusora de videos populares que fue prohibida por el Ejército de Estados Unidos el 31 de diciembre de 2019, y no puede ser usada en los dispositivos oficiales, porque lo considera una amenaza a la seguridad. Una medida similar fue adoptada por la Marina de Estados Unidos 11 días antes.(Univisión, 2019)

Por su parte, el Chief Executive Officer (CEO) de Google, según los medios, aceptó que "no hay dudas" de que Huawei envía datos al régimen chino y aseguró que

las prácticas de esta empresa china comprometen la seguridad de los países. (Infobae, 2020) También en el ámbito de la Defensa Nacional de Estados Unidos, no se usa la aplicación Zoom por considerarla peligrosa para la seguridad nacional.

Todo lo expresado confirma que un débil tiene un arma poderosa para causarle problemas severos a alguien más fuerte en medios convencionales cinéticos, porque la victoria le corresponde al más astuto y no al más fuerte. Las formas más ingeniosas de ganar incluyen negar el enemigo las condiciones de victoria. O simplemente negarse a morir, y persistir con tenacidad, como George Washington hizo con el rudimentario Ejército Continental en 1781. “La guerrilla gana si no pierde. El ejército convencional pierde si no gana”, explicó Henry Kissinger durante la guerra de Vietnam.” (McFate, The New Rules of War Victory in the Age of Durable Disroder, 2019, pág. 173)

La globalización y la evolución de las TICs permitieron el desarrollo de CRI como herramientas que se aplican en un nuevo teatro de operaciones cibernético. Esto constituye una nueva arma no militar para poder modificar o influir en la percepción de la ciudadanía, que es el blanco principal, ya que puede modificar la opinión pública y esta ser usada como arma política. Quizás cuando Claussewitz escribiy que “la guerra no es sino la continuaciyn de la política por otros medios” nunca imaginó que “por otros medios” podría alguna vez no significar únicamente fuerza militar.

CAPÍTULO IV: ESTUDIO DE CASOS DONDE SE LLEVARON A CABO OPERACIONES DE INFORMACIÓN (OI) EN OCCIDENTE.

La finalidad de este capítulo es sintetizar las OI llevadas a cabo por Rusia en el sucesivo avance territorial luego de la caída del Pacto de Varsovia en Estonia (2007), Georgia (2008) y Ucrania (2014). Según Rusia, Occidente lleva a cabo las mismas actividades desde la finalización de la Guerra Fría, y llama a eso guerra híbrida. (Korybko, Guerras Híbridas Revolución de Colores y Guerra No Convencional, 2015). No se analizan las OI que eventualmente pudiera haber llevado a cabo Occidente, por carecerse de fuentes confiables sin que ello signifique negar que hayan podido existir.

LA EXPANSION RUSA EN ESTONIA, GEORGIA Y UCRANIA

Esgrimiendo el concepto de defensa propia, Rusia hizo uso intenso de OI en los casos que siguen

ESTONIA 2007.

Estonia es el país más digitalizado del mundo. Perteneció a la Unión Soviética hasta 1991. Luego alcanzó un desarrollo sin precedentes, en especial en informática, tanto es así que jocosamente se lo denomina E-stonia. La casi totalidad de los trámites que debe hacer una persona puede hacerse por internet.

En el año 2007, en represalia por la decisión de llevarse de la capital Tallin un monumento al soldado soviético, Rusia lanzó un ataque cibernético. Debe notarse que la ira popular se desató por una carta de disculpa falsa difundida por Internet, del Primer Ministro al Presidente Ruso.(Lenor-Grands Pons, 2017)

La minoría rusa de Estonia salió a la calle a protestar, luego de escuchar estas noticias falsas sobre que las tumbas militares soviéticas en el cementerio estaban siendo vandalizadas. El 26 de abril del 2007 hubo dos noches de saqueos.

A partir del 27 de abril Estonia también fue blanco de ataques cibernéticos que en algunos casos duraron semanas. Las páginas web de bancos, medios de prensa y organismos gubernamentales colapsaron debido a niveles sin precedente de tráfico en internet. Redes de robots informáticos -conocidos como botnets- enviaron cantidades masivas de mensajes basura (spam) y pedidos automáticos online para saturar los

servidores. El resultado fue que los estonios se quedaron sin poder usar cajeros automáticos y servicios de bancos online. Los empleados estatales no pudieron comunicarse por correo electrónico. Los diarios y medios de comunicación se encontraron repentinamente con que no podían transmitir las noticias.

Los atentados de 2007 se hicieron desde direcciones de IP rusas, las instrucciones online estaban en ruso y Moscú ignoró los pedidos de ayuda de Estonia. Sin embargo, no hay evidencias concretas de que estos ataques los realizara el gobierno ruso.(McGuiness Damien, 2017)

El ataque a Estonia fue una ofensiva de dos fases. Inicialmente, los atacantes se involucraron en poco más que vandalismo electrónico, como piratear el sitio web del partido político que dirigió el gobierno de coalición de Estonia, donde los atacantes publicaron una carta de disculpa falsa del primer ministro Andrus Ansip por mover una estatua al soldado desconocido ruso. En la segunda fase, los ataques se convirtieron en una campaña a gran escala. El objetivo era sobrecargar los servidores informáticos de Estonia con volúmenes masivos de tráfico de mensajes que los hacían colapsar, aprovechando redes de bots (grandes redes de computadoras que han sido controladas por malware y que se controlan desde una o más ubicaciones centrales) para bombardear a los objetivos. Los sistemas estonios fueron sobrecargados con millones de mensajes falsos. Algunas estimaciones sugieren que un millón de computadoras fueron cooptadas o empleadas de otra manera a nivel mundial para este ataque de Denegación de Servicio Distribuido (DDoS) en los servidores de un país de 1.3 millones de habitantes. (2018, pág. Cap 9 pag 154)

Debe notarse que el ataque cibernético a Estonia no incluyó las redes de datos médicos, ni las de transporte aéreo, ni las de control de tránsito, ni los servicios sanitarios de agua y cloacas, que podrían haber causado un desastre de proporciones mayúsculas. Todo indica que fue una prueba. Pero este trabajo no trata de las operaciones cibernéticas, sino de las OI. Nótese que todo comenzó cuando se decidió hackear el sitio web del partido político que dirigía el gobierno Estonia, como antes se mencionó para publicar una carta de disculpa falsa del primer ministro por mover una estatua del soldado desconocido ruso, acompañada de noticias falsas sobre profanación de tumbas rusas. Una carta de disculpa falsa y noticias falsas desencadenaron todo el movimiento y pusieron en vilo a un país, el más informatizado del mundo.

Fuente: Estonia Word Press.com

Estonia reclamó a la OTAN la puesta en vigencia del Artículo 5to de la Carta, en el sentido que era una agresión a un miembro de la OTAN que se podía enfrentar con medios cinéticos convencionales, pero la OTAN solo aceptó el Artículo 4to.

GEORGIA (2008)

En 1991 y después de la disolución del Pacto de Varsovia, Abjasia que anteriormente era una República Socialista Soviética asociada a Georgia, y Osetia del Sur que era una parte autónoma de la República Socialista de Georgia, llevaron a cabo una breve guerra con esa República desde enero de 1991 hasta junio de 1992. El resultado fue la independencia de facto para ambas regiones. Los georgianos permitieron que ambas regiones tuvieran autonomía con una fuerza de mantenimiento de la paz que consistía en fuerzas locales y tropas rusas. Los rusos comenzaron a

infiltrarse en ambas áreas, realizaron reconocimientos, establecieron redes de inteligencia y de insurgentes, y comenzaron a proporcionar ayuda financiera y humanitaria. Los "efectivos de mantenimiento de la paz" rusos también canalizaron armas a grupos separatistas y proporcionaron entrenamiento militar a futuros insurgentes. Muchos georgianos fueron expulsados a Rusia, y Rusia emitió pasaportes rusos masivamente a los ciudadanos de Osetia del Sur y Abjasia en 2002, esencialmente haciéndolos ciudadanos de Rusia. Rusia controlaba prácticamente todas las funciones cívicas, militares y gubernamentales en estas áreas en el momento de la Revolución de las Rosas de Georgia en 2004, que fue un movimiento donde el presidente electo prometió restaurar la integridad territorial nacional, revertir los efectos de la limpieza étnica y permitir que los refugiados de 1992 retornaran a sus hogares.

Debe aclararse que en Europa, prima el jussanguinis sobre el jussoliis. Más que el lugar de nacimiento de un ser humano para tener la nacionalidad, importa la herencia sanguínea, de donde muchos ciudadanos que pos siglos habían nacido en Osetia del Sur, eran según la ley europea, ciudadanos rusos. Existe una razón práctica para esto, los límites de los Estados de Europa están sometidos a tantos cambios debido a las guerras, que la población no puede cambiar la nacionalidad en un santiamén.

Fuente: Mapas del mundo.net

El nuevo presidente georgiano, Mikhail Saakashvili, intentó atraer a ambas regiones de Abjasia y Osetia del Sur a un estado georgiano unificado, pero esta propuesta fue rechazada. Osetia del Sur siempre se consideró parte de Europa, y luego de pretender entra a la OTAN, los rusos intensificaron sus esfuerzos en OI. Un elemento clave de esta táctica fue controlar la información a través de la televisión, la radio e Internet. Los rusos habían estado proporcionando acceso a las estaciones de televisión rusas desde la década de 1990, y los medios de comunicación pro-rusos / separatistas en Abjasia y Osetia del Sur proporcionaron un flujo constante de propaganda anti-georgiana. Internet también se utilizó para difundir temas pro-rusos y pro independentistas. Finalmente, los agentes de inteligencia rusa denominados "hombres de verde" y locales comenzaron a organizar manifestaciones y protestas contra el maltrato por parte del gobierno georgiano de las poblaciones rusas de Abjasia y Osetia del Sur, la mayoría de los cuales tenían pasaportes rusos y apoyaban la autonomía, en función del vigente jussanguinis.

Los rusos habían reconocido a los gobiernos de ambas regiones en abril de 2008 y enviaron aproximadamente 2.000 fuerzas de paz más a Abjasia y concentraron 1.500 soldados en la frontera entre Rusia y Osetia del Sur. A fines de abril, un vehículo aéreo no tripulado georgiano (UAV) fue derribado sobre Abjasia. Los rusos y abjasios culparon a la OTAN por el incidente, mientras que Georgia afirmó que los insurgentes o los rusos habían derribado el UAV. Independientemente de quién derribó el UAV, esto les dio a los rusos una excusa plausible para continuar agrupando tropas en las fronteras de Abjasia y Osetia del Sur mientras movían encubiertamente a las tropas del SPF (Special Purpose Forces/ Fuerzas de Propósito Especial).(TRADOG G-2 ACE, 2015, pág. 7)

Mientras se desarrollaba toda esta actividad encubierta de tropas, los rusos comenzaron un esfuerzo en las redes sociales, la prensa rusa y la prensa internacional para desacreditar la posición del gobierno georgiano y demostrar una situación conflictiva para los habitantes con ciudadanía rusa. Los expertos rusos de guerra electrónica también comenzaron a monitorear y bloquear las comunicaciones militares y gubernamentales de Georgia.

Una serie de incidentes ocurridos en mayo y principios de junio de 2008 que involucraron a funcionarios y tropas del gobierno georgiano y ciudadanos abjasios y osetios del sur de Rusia aumentaron la tensión en ambos lados. Sitios web, blogs y

medios de comunicación pro-rusos transmitieron historias que empujaron a la confrontación étnica. Parte de la campaña cibernética consistía en retratar al presidente de Georgia Saakashvili como nazi y al gobierno georgiano como opresivo y usando tácticas similares a la Gestapo. La respuesta georgiana a esta propaganda era prácticamente inexistente, excepto por algunos comunicados de prensa ineficaces.

Rusia también atacó el sistema informático georgiano, deshabilitando sitios civiles y gubernamentales con barreras de tráfico que resultaron en situaciones de denegación de servicio (DOS) durante y antes del conflicto. También se sospecha que los rusos atacaron los sistemas georgianos un mes antes del ataque, y luego usaron esta información para implementar medidas para evitar contramedidas georgianas. Además del inconveniente normal de tener sistemas informáticos caídos, el ejército georgiano y el gobierno no pudieron comunicarse efectivamente durante la guerra.

Elementos separatistas comenzaron a aumentar la actividad a lo largo de junio y julio. Los incidentes incluyeron un intento de asesinato de un funcionario georgiano y la captura de cuatro soldados georgianos por separatistas en Osetia del Sur. Se utilizó un IED (Improvised Explosive Device - Artefacto Explosivo Improvisado) contra la policía georgiana, y los insurgentes bombardearon Tsjinvali a principios de agosto, aumentando gradualmente la presión sobre el gobierno georgiano para que actuara. Finalmente, el 8 de agosto de 2008, el ejército georgiano avanzó hacia Tsjinvali en un intento de tomar el túnel Roki para negarle a las fuerzas rusas la capacidad de moverse a Tsjinvali. Los georgianos lograron asegurar las partes meridionales y centrales de la ciudad hacia el mediodía, pero este movimiento resultó ser demasiado tarde ya que los rusos ya habían comenzado a mover tropas regulares del ejército a través del túnel hacia Osetia del Sur. Junto con las tropas, los rusos desplegaron un gran contingente de "reporteros" que podrían cubrir la guerra en tiempo real para avanzar el mensaje ruso de "ayudar a los rusos étnicos oprimidos en Osetia del Sur y Abjasia".(TRADOG G-2 ACE, 2015, pág. 8)

En el nivel estratégico, la guerra se combinó con otras medidas, como las operaciones diplomáticas, cibernéticas y de información, pero militarmente no puede calificarse como una operación militar a gran escala. Los rusos comenzaron una campaña mediática en las redes sociales, la prensa rusa y la prensa internacional para desacreditar la posición del gobierno georgiano y mostrar la "situación" de los rusos étnicos "oprimidos". Además, atacaron los sistemas informáticos de Georgia,

desactivaron sitios web civiles y gubernamentales, bloquearon las comunicaciones entre el Ejército y el gobierno georgiano, que no se comunicaron efectivamente durante la guerra. En la guerra de cinco días, como también es conocido el conflicto, la estrategia militar rusa consistió en lograr rápidamente una superioridad de medios, combinando despliegues masivos en el terreno, con apoyo de operaciones aéreas y navales.(Pallin y Westerlund, 2009)

Las tropas terrestres rusas lograron con éxito el principal objetivo militar de la operación: tomar el control irreversible de Abjasia y Osetia del Sur. Los activos aéreos lograron la superioridad aérea local, necesaria para que los elementos terrestres y navales continuaran la operación. Para la armada rusa, la Guerra de los Cinco Días fue la primera misión de combate desde la caída de la Unión Soviética, por lo que la flota del Mar Negro rápidamente logró la supremacía del mar y cortó el acceso a los puertos más importantes de Georgia.(Pallin y Westerlund, 2009)

La estrategia estaba totalmente alineada con el pensamiento militar soviético, superioridad de medios combinados con la aplicación de medidas cibernéticas, guerra electrónica, y operaciones de informaciones. El conflicto de Georgia demostró que el Kremlin podía influir en su periferia empleando una capacidad militar significativa. Sin embargo, las bajas rusas, las deficiencias y los problemas encontrados durante la operación sirvieron como enseñanza para el desarrollo futuro de las fuerzas armadas.

Los ataques cibernéticos a los sistemas georgianos ya estaban en marcha antes de que Rusia invadiera en 2008. El día en que comenzaron los ataques terrestres, sitios como stopgeorgia.ru publicaron listas de objetivos georgianos para atacar, así como instrucciones sobre cómo lanzar esos ataques. Mientras Moscú acribilló a Georgia con movimientos de tropas en las fronteras de las provincias separatistas de Abjasia y Osetia del Sur, los bots ya estaban en el ataque, degradando los sitios web georgianos, incluidas las páginas del presidente, el parlamento, el ministerio de relaciones exteriores y las agencias de noticias. Los bancos, que también fueron blanco de ataques cibernéticos, cerraron sus servidores a la primera señal de ataque para evitar el robo de identidad o monetario. Esta fue la primera vez (reconocida) vez que los ataques militares rusos y cibernéticos tradicionales se realizaron en coordinación. Las encuestas de objetivos, los objetivos, los dominios y las instrucciones estaban listos y se publicaron en Internet junto con la incursión rusa inicial en Georgia. Esta no fue una

operación de vuelo nocturno organizada ayudando a los hacktivistas; más bien, el momento sugiere que se trataba de un ejército patrocinado por el estado que ordenó la incursión cibernética específicamente diseñada para ser lanzada en conjunto con la operación militar.(2018, pág. Cap 9 pag 154)

Georgia, un paso más allá de Estonia, consistió en redes preformadas enviando paquetes preformados, en un ataque de Denegación de Servicio a gran escala, pero ahora llevado a cabo simultáneamente con una incursión de tropas y tanques y un movimiento militar tradicional en el área de Osetia del Sur. A través de publicaciones en varios foros y sitios de Internet, la actividad cibernética paramilitar parece haber sido, si no alentada, tampoco desanimada, lo que solo sirvió para aumentar las filas de quienes realizaban ciberataques en nombre de Rusia. (2018, pág. Cap 9 pag 157)

El conflicto armado con Georgia en agosto de 2008 fue lo que proporcionó el ímpetu para revisar y transformar el esfuerzo de guerra de información de Rusia, junto con todas las Fuerzas Armadas rusas. Fue en este punto que Rusia intensificó significativamente los esfuerzos para explotar Internet como otro medio para controlar la información. El debate abierto sobre la mejor respuesta al desafío incluyó llamados a la creación de Tropas de Información, una rama dedicada que podría gestionar la guerra de información desde el interior de las fuerzas armadas. Reflejando la naturaleza de espectro completo del concepto de guerra de información ruso, estas tropas incluirían piratas informáticos, periodistas, especialistas en comunicaciones estratégicas y operaciones psicológicas, y, fundamentalmente, los lingüistas esenciales para superar el déficit de capacidad lingüística percibido por Rusia. Comenzó una fuerte inversión en capacidades lingüísticas, para llegar a audiencias objetivo que no hablaran ruso directamente.(Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 36)

UCRANIA

Aunque Ucrania logró la independencia en 1991 con la disolución de la URSS, la democracia y la prosperidad se mantuvieron esquivas ya que el legado del control estatal y la corrupción endémica paralizaron los esfuerzos de reforma económica, privatización y libertades civiles. Durante el gobierno de Nikita Kruschev, Crimea que era un territorio estratégico para la Unión Soviética por tener la base naval rusa de Sebastopol, fue cedido a Ucrania, en ese entonces parte de la Unión Soviética.

Una protesta masiva pacífica conocida por los rusos como la "Revolución Naranja" en los últimos meses de 2004 obligó a las autoridades a revocar una elección presidencial fraudulenta y permitir una nueva votación supervisada internacionalmente que arrasó con una lista reformista bajo el liderazgo del ucraniano Viktor Yushchenko. Las disputas internas posteriores en el campo de Yushchenko permitieron a su rival Viktor Yanukovych volver a las elecciones parlamentarias (Rada), convertirse en primer ministro en agosto de 2006 y ser elegido presidente en febrero de 2010. En octubre de 2012, Ucrania celebró elecciones en Rada, ampliamente criticadas por los observadores occidentales ya que tenían fallas debido al uso de recursos del gobierno para favorecer a los candidatos del partido gobernante, la interferencia con el acceso a los medios y el hostigamiento de los candidatos de la oposición. El retroceso del presidente Yanukovych en un acuerdo de comercio y cooperación con la UE en noviembre de 2013, a favor de lazos económicos más estrechos con Rusia, y el posterior uso de la fuerza contra estudiantes, activistas de la sociedad civil y otros civiles a favor del acuerdo condujeron a un acuerdo de tres meses de ocupación de protesta de la plaza central de Kiev. El uso de la violencia por parte del gobierno para desmantelar el campamento de protesta en febrero de 2014 condujo a batallas campales, decenas de muertes, condenas internacionales, un acuerdo político fallido y la abrupta partida del presidente hacia Rusia. Nuevas elecciones en la primavera permitieron que el presidente pro occidente, Petro Poroshenko, asumiera el cargo en junio de 2014; Volodymyr Zelensky lo sucedió en mayo de 2019.Poco después de la partida de Yanukovych a fines de febrero de 2014, el presidente ruso Putin ordenó la invasión de la península de Crimea en Ucrania, alegando que la acción era proteger a los rusos étnicos que viven allí.(CIA World Factbook, 2020)

Fuente: Shutterstock.com

Como se expresó anteriormente, la Península de Crimea, la región de la primera parte del conflicto en Ucrania, formó parte de la Unión Soviética hasta 1954, cuando el entonces líder ruso Nikita Khruschov decidió hacer un gesto simbólico para garantizar el apoyo de los ucranianos, ofreciendo la región al país. Sin embargo, los ciudadanos ucranianos pro occidentales exigieron una mayor integración del país con la Unión Europea (UE).

Un nuevo presidente interino fue elegido y reconocido por la UE y EEUU, pero Rusia se negó a reconocer el nuevo gobierno interino de Ucrania y comenzó a intervenir más directamente en el Este del país, llevando a cabo una serie de incursiones en el territorio, con el apoyo de movimientos separatistas pro-rusos. Rusia, a la vez, realizó importantes ejercicios militares en la frontera con Ucrania al parecer con fines disuasorios.

Aunque no fue asumida por Rusia, las tropas especiales se hicieron cargo del parlamento local, lo que permitió elegir a Sergei Aksenov, como nuevo primer ministro de Crimea. Además, las tropas especiales lideraron la toma del cuartel general por las fuerzas armadas ucranianas y otros objetivos estratégicos, como las instalaciones de comunicaciones y predios públicos. La operación de Crimea utilizó la velocidad y la sorpresa para establecer posiciones importantes en el terreno, obstaculizando así una respuesta militar rápida.

Durante las operaciones, Rusia llevó a cabo intensas campañas sistemáticas de desinformación, con el objetivo de desacreditar al gobierno de Kiev, acusándolo de fascista, además de utilizar todos los canales posibles para denigrar la democracia de Ucrania. Comenzando como una operación militar encubierta, combinando ambigüedad y desinformación, la anexión de Crimea se completó con una invasión militar tradicional. El referéndum sobre la adhesión a Rusia se celebró el 16 de marzo y contó con el respaldo del97% de los votantes. Los países occidentales rechazaron los resultados porque se creía que era una farsa. (Caliskan, 2017)

Rusia, además del control sobre la transmisión y los medios impresos, también obtuvo el control sobre las telecomunicaciones, aislando exitosamente a Crimea de las noticias del mundo exterior. Los mensajes, para dar credibilidad a la desinformación, se difundieron en las redes sociales, utilizando perfiles en línea controlados por seres humanos (trolls); perfiles controlados por procesos automatizados (bots) y secuestro de cuentas de redes sociales, entre otras técnicas de cibernética. Cuando el ejército ucraniano parecía moverse contra los rebeldes en el Este, el Kremlin cambió su posición presentándose como el defensor de los problemas humanitarios. La maquinaria de propaganda se utilizó para gestionar las percepciones de la comunidad interna e internacional durante las operaciones.(Caliskan, 2017)

Se mezclaron así las medidas militares con las no militares que plantea el General Valery Gerasimov(Makotzcenko, 2019) Una combinación de campañas políticas, económicas, de información, y tecnológicas fueron usadas ampliamente en forma de acciones indirectas y con medidas no militares. La estrategia militar empleada fue, en cierto modo, ayudada por una serie de factores que la facilitaron: apoyo del líder civil pro-ruso colocado en el parlamento, la infiltración de fuerzas de operaciones especiales, a las que llamaban "hombrecitos verdes" haciendo imperceptibles ocupaciones de objetivos estratégicos; un liderazgo político ucraniano debilitado; pero principalmente por la casi total falta de reacción de la comunidad internacional que se sorprendió por la velocidad de las acciones rusas por un campo que había sido preparado de antemano.

Además, las campañas rusas contra Ucrania continuaron en las regiones orientales de Ucrania, en las provincias de Donetsk y Lugansk, que afirmaban ser separadas e independientes. Las fuerzas rusas, además del uso de aeronaves pilotadas a distancia, lanzaron ataques cibernéticos y electrónicos contra las tropas ucranianas, que

al neutralizar sus sistemas de Comando y Control (C2), limitaron su capacidad de comunicación, tornando objetivos fáciles para el lanzamiento de ataques masivos con cohetes.

El presidente Putin negó la participación rusa en el conflicto, al tiempo que utilizó la amenaza de disuasión militar, incluida la nuclear, si eran demasiado provocados. La evidencia de las tropas rusas en la región fue rechazada, de forma tal que Rusia acusó a Occidente de entrometerse en los asuntos ucranianos y de intensificar las tensiones.

Durante las campañas, el empleo conjunto de las Fuerzas Armadas fue decisivo para el éxito ruso. En las acciones de Crimea, los remolcadores de la armada rusa remolcaron el barco Ochakov, fuera de servicio desde 2000, y lo hundieron en la entrada del lago Donuzlav, bloqueando la flota naval ucraniana con base en el puerto de Novoozerne y evitando que se enfrentara a los barcos rusos de la base de Sebastopol. A su vez, el mantenimiento de la superioridad aérea rusa permitió el avance de las tropas y la ocupación de infraestructura estratégica.

Fuente: www.dreamstime.com

Analistas militares y políticos sugieren que Rusia está utilizando a Ucrania como un campo de pruebas perpetuas de guerra cibernética, o como se lo describió en un extenso y detallado informe sobre el asunto el año pasado, un laboratorio para

perfeccionar nuevas formas de combate global en línea. Un ejército digital ha socavado sistemáticamente prácticamente todos los sectores de Ucrania: medios de comunicación, finanzas, transporte, militares, política y energía. Las intrusiones aparentemente imparables eliminaron datos, destruyeron computadoras y, en algunos casos, paralizaron las funciones más básicas de las organizaciones. No hay forma de saber exactamente cuántas instituciones ucranianas han sido golpeadas en la creciente campaña de ciberataques, y cualquier cargo puede ser subestimado. Por cada objetivo conocido públicamente, otros no han admitido ser víctimas. Aún más, ni siquiera han descubierto a los intrusos en sus sistemas.(2018, pág. 154)

Las intenciones de los atacantes se pueden resumir en una sola palabra rusa: polígono, traducido libremente como "campo de entrenamiento". Incluso en sus acciones más dañinas, los atacantes nunca parecen ir demasiado lejos; los atacantes podrían haber noqueado la estación de transmisión de Ukrenergo por más tiempo o haber causado daños físicos permanentes a la red, pero en cambio se conformaron con apagones repetidos. El atacante nunca parece estar comprometido con la destrucción total de sus objetivos en Ucrania. En cambio, los atacantes cesan antes de entregar un daño irreparable, jugando sus cartas cerca de su pecho como si reservaran sus verdaderas capacidades para alguna operación futura; casi se puede pensar en ello como la planificación del juego durante un juego de fútbol de pretemporada.(2018, pág. 155)

La relativa falta de hostilidad visible en la actividad cibernética durante el conflicto entre Rusia y Ucrania ha sido atribuido, entre muchos otros factores, al uso generalizado servidores de correo ruso por parte de funcionarios ucranianos, por lo que Rusia no necesitó piratear cuentas de correo electrónico a las que ya tenía acceso de forma predeterminada. No sería irrazonable suponer que los gobiernos extranjeros podrían ser capaces de inducir a los proveedores de servicios a hacer lo mismo con Rusia. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 39)

Para el propósito de guerra de información, armas cibernéticas costosas de un solo disparo, o los ataques DDoS ruidosos e impopulares son completamente innecesarios si se puede obtener control físico de la infraestructura de internet, como se demostró en una etapa temprana durante la toma de Crimea. La ocupación del Simferopol, punto de intercambio de Internet e interrupción de las conexiones de cable al continente contribuyó al dominio total de la información en la península para Rusia, facilitando en gran medida nuevas operaciones.(Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 49)

Las capacidades mostradas por Rusia en el este de Ucrania incluyeron una Capacidad de Guerra Electrónica muy mejorada, hasta para interferir GPS. Incluso cuando el acceso físico a las instalaciones no estuvo disponible, se describe un rol para las fuerzas de Guerra Electrónica en la supresión de los medios en línea y tradicionales. En la fase inicial del conflicto, asumieron la misión de bloqueo de señales de radio y televisión y el tráfico de señales en las redes sociales, para filtrar la información que llegaba a la población y a las Fuerzas Armadas. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 67)

Los ciberataques de diciembre de 2015 contra las redes energéticas ucranianas, con la campaña telefónica masiva que impidió a los consumidores de energía contactar a sus proveedores, fue un asunto innecesario por la relativa falta de la actividad cibernética visible que caracterizó al resto del conflicto en Ucrania. La especulación en fuentes abiertas continúa en cuanto a las motivaciones del ataque y el resultado previsto. Pero mientras divergen del patrón general de ciberataques visibles limitados en el contexto del conflicto ucraniano, la campaña telefónica que lo acompañó- que fue un ataque masivo de denegación de servicio que suprimió la distribución de información y obstaculizó las operaciones de recuperación - estuvieron vinculadas con la tendencia de probar y explotar nuevos métodos de conflicto de información dirigidas que involucraban a las comunicaciones masivas tomadas como blanco. La característica más peligrosa de esta orientación es que la información parece provenir de una fuente confiable, ya sea por mensaje de texto, medios sociales de comunicación o correo electrónico. Un escenario posible es que se use esta capacidad para difundir desinformación masiva y persuasiva o instrucciones falsas en un momento crítico en una crisis que involucra confrontación. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 72)

LA CRISIS DEL AGUA DE CRIMEA DE 2014

La anexión de Rusia de la Península de Crimea el 16 de marzo de 2014 se encontró con el descontento internacional y una sensación de imperialismo ruso para expandir su reinado de poder. Tanto las Naciones Unidas como el secretario general de la OTAN, Anders Fogh Rasmussen, condenaron la flagrante agresión de Rusia y el desprecio del derecho internacional. Las quejas, las solicitudes de ayuda y las cuentas sobre el terreno del conflicto en desarrollo se informaron a audiencias mundiales a

través de una variedad de plataformas de código abierto, incluidos blogs, sitios web de noticias, Twitter, Facebook y YouTube.

Varias historias publicadas por agencias de noticias rusas para engañar y confundir al público objetivo fue a través de la difusión de misinformation (es decir, mentiras, falsedades) y disinformation (es decir, información errónea). Ejemplos de estos esfuerzos coordinados a nivel nacional incluyen noticias de ITAR-TASS, que afirmaban que el gobierno ucraniano había dejado de trabajar en el Canal del Norte de Crimea, que transportaba agua desde el río Dnieper a Crimea. En otro ejemplo, la red de televisión internacional rusa Russia Today (RT) que informó las imágenes satelitales mostraban a Ucrania tratando deliberadamente de cortar el suministro de agua de la península de Crimea mediante la construcción de una presa, mientras que los científicos rusos intentaban encontrar formas de suministrar agua dulce a Crimea. Confiando en estas historias falsas y engañosas, en una nueva noticia posterior el artículo del New York Times informó que se observó una escasez de agua, las granjas de Crimea se estaban secando, los suministros de alimentos eran inadecuados y el precio de bienes básicos, como la leche y el gas, se habían duplicado. Durante todo el tiempo, las fuerzas armadas rusas participaron plenamente en operaciones convencionales contra las fuerzas ucranianas en el este de Ucrania en julio de 2014. El empleo de nuevas armas y métodos de empleo por parte de Rusia no se limitó a capacidades no cinéticas. En el este de Ucrania, todo un batallón ucraniano fue prácticamente destruido en cuatro minutos por una lluvia de explosivos racimos y municiones termobáricas[27]. Lo que queda claro en la participación rusa en el territorio de Ucrania es que emplearon una variedad de capacidades en nuevas e innovadoras formas de generar una ventaja relativa en el campo de batalla. La idea que debería mantener despiertos a los analistas militares occidentales en las noches es que los rusos seguramente no revelaron su bolsa llena de trucos. Los bots pro-rusos aprovecharon Internet para dar forma al entorno de información en forma de cámaras de eco. Esta información mal intencionada es así rebotada y multiplicada para dejar una marca y una duda en cada lugar que golpean, aunque después la información se refute. Los creadores de los robots entienden el efecto de una cámara de eco. En otras palabras, los bots estaban clonando la información

[27] Bombas termobáricas: Lo que diferencia a las bombas termobáricas de los explosivos convencionales **es** el uso del aire en el propio ambiente para producir una onda de choque mayor y consumir rápidamente el oxígeno en el lugar. Fuente: Infobae del 20 de Abril de 2017

[errónea], creando una cámara de eco y engañando al público objetivo sobre las operaciones militares que estaban en curso en Ucrania.(2018, pág. 166)

La invasión rusa de Crimea en 2014 proporciona un estudio de caso histórico de actividades de guerra híbrida que involucran operaciones terrestres y OI. Los bots sociales que operan durante este tiempo movieron mensajes especialmente diseñados a través del entorno de información. Los datos recopilados de las redes sociales, incluidos los blogs y Twitter, demuestran claramente la intención y la capacidad de Rusia de manipular la información mediante el uso de bots sociales. Los analistas occidentales utilizaron metodologías socio-computacionales para identificar las "sembradoras de información" (fuentes de información que suministran contenido a las botnets o un conjunto de cuentas de bots que trabajan juntas) y las estrategias de comunicación y coordinación utilizadas. Durante el evento antes mencionado, las botnets desplegadas para la difusión de propaganda evolucionaron al volverse cada vez más engañosas y bien coordinadas para engañar a audiencias específicas en el nivel directo de participación rusa, y objetivos estratégicos para confundir y retrasar la decisión de los líderes políticos occidentales.

Según Wesley White (Perceptions are reality, 2018)en el Capítulo 9 de la obra “Perceptions are reality”, la Federación Rusa ha impartido una clase magistral sobre el desarrollo e integración de las capacidades cibernéticas en conflictos modernos y parece totalmente comprometida con la idea de que las operaciones ciberespaciales y otras acciones indirectas son un medio principal de proyección de fuerza, en lugar de una equivalencia útil (o necesaria) con fuerzas cinéticas tradicionales.

En febrero de 2013, el general Valery Gerasimov, Jefe del Estado Mayor de Rusia (comparable con el presidente del Estado Mayor Conjunto de los EE. UU.), publicó un artículo titulado "El valor de la ciencia está en la previsión", en el periódico semanal ruso Military. -Kurier industrial. En él, Gerasimov sugirió que las "mismas" reglas de guerra "han cambiado", y que en muchos casos, los medios no militares han excedido el poder y la fuerza de las armas en su capacidad de efectuar cambios en el escenario internacional. Gerasimov sostiene que las nuevas tecnologías han reducido las brechas entre las fuerzas tradicionales y su comando y control, aunque también señala que "los enfrentamientos frontales de grandes formaciones de fuerzas a nivel estratégico y operativo se están convirtiendo gradualmente en algo del pasado". El futuro, sugiere Gerasimov, radica en "acciones sin contacto", realizadas a través de medios cibernéticos u otros medios electrónicos, que se utilizan como los principales medios de objetivos

militares o de inteligencia. Esta creencia: que las interacciones militares tradicionales están dando paso a algunas interacciones indirectas más nuevas y subjetivamente más efectivas a través de computadoras y dispositivos electrónicos han sido denominadas por algunos como la Doctrina Gerasimov. (Gerasimov, The Value of Science in the Foresight, 2016)

El momento del lanzamiento y publicación de la Doctrina Gerasimov es importante. Inmediatamente después del lanzamiento del artículo de Gerasimov, Rusia invadió Ucrania con tanques y malware. La incursión digital rusa en las redes ucranianas, junto con un asalto físico militar, fue algo que la Federación Rusa había estado practicando durante casi una década. Apuntando a Estonia en 2007, Georgia en 2008 y, finalmente, Ucrania en 2014, estos ataques utilizaron efectos cibernéticos, efectos más tradicionales (con unidades de tierra mecanizadas, tropas en tierra y aviones), o una combinación de ambos. En cada uno de los tres casos, la fuerza rusa aumentó tanto en alcance como en complejidad. Rusia ha establecido el plan para el entrenamiento y desarrollo de un cuerpo cibernético efectivo, y ha transmitido al mundo cómo ha integrado efectivamente las operaciones cibernéticas con las maniobras militares tradicionales a gran escala. Además, Rusia está dando a conocer cómo perciben el lugar de la cibernética y otras formas indirectas de conflicto, como formadores de políticas.(2018, pág. Cap 9 pag 152)

Desde una perspectiva militar, la progresión de las operaciones cibernéticas por parte de Rusia, que se lleva a cabo ignorando las normas y estándares de conducta internacionales, le ha permitido desarrollar su cuerpo cibernético a través de misiones del ciberespacio del mundo real, en coordinación con operaciones militares cinéticas.

El investigador Keir Giles identifica varios pasos a seguir en estas campañas de información llevadas a cabo en Ucrania. Para una prospectiva del futuro, Keir Giles analizó sus rasgos salientes. Concluyó que se ha enfatizado la forma en que una fuerza militar ya no es el primer determinante de efectos y puede ser un segundo lugar respecto a otros elementos del poder del Estado. Según lo expresado por el General Valeriy Gerasimov,

> En conflictos contemporáneos, el énfasis en los métodos de lucha se desplaza hacia la aplicación compleja de medios no militares, políticos, económicos y de

información, realizados con el apoyo de la fuerza militar. ((Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 64).

Para eso, Keir Giles analizó en el caso de Ucrania, la infraestructura de Internet, la convergencia, la preparación de los medios sociales, la elección de las personas como blanco y la explotación de información falsa. Este autor concluye que una indicación posible que existe preparación en este ámbito de información puede ser si se detecta investigación en la infraestructura civil de comunicaciones de internet, por ejemplo en los cables subterráneos y subacuáticos de internet. Se cree que ésta es una de las tareas de la Dirección Principal de Investigación de Aguas Profundas Rusas (GUGI), una organización secreta que ahora está recibiendo atención pública debido al aumento considerable en el ritmo y la importancia de sus operaciones.(Keir Giles, Russian Handbook of Information Operations, 2015, pág. 65) . Asimismo, la interrupción de los satélites de comunicaciones puede ser considerada un asunto clave en el dominio de la información y una ventaja considerable en guerra convencional.

Otra de las conclusiones que elabora Keir Giles es que se detectó que los oficiales están demasiado tecnificados, y que la OTAN puede encontrarse con que los recursos de internet podrían ser degradados o absolutamente ausentes, o comprometidos con acceso restringido al espectro electromagnético, incluyendo señales de GPS. Los oficiales podrían haber perdido las habilidades de una "guerra no técnica", es decir ya no serían capaces de trabajar sin sistemas de información, y deberían ser nuevamente entrenados en trabajar con mapas de papel en vez de mapas virtuales.(Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 80)

En la doctrina militar rusa las operaciones de informaciyn no son "exactamente cyber, no exactamente guerra electrónica, no solamente inteligencia, sino […] una integración efectiva de todas esas capacidades con medidas cinéticas para crear el efecto que sus comandantes quieren lograr. Tal cual asesoró un estudio sobre UAV [drones] en Ucrania "la experiencia de las operaciones de combate en curso muestra que la línea divisoria entre los diferentes tipos de guerra se está tornando cada vez más borrosa e irrelevante" (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 69)

"Las guerras futuras serán lanzadas por las fuerzas de guerra electrónica (EW), que protegerá a las fuerzas amigas, bloqueará la desinformación de propaganda extranjera, y atacará a las fuerzas y a los activos de Guerra Electrónica

enemigos, combinándolos con operaciones aeroespaciales, con esta última aumentada por misiles de crucero y elemento de reconocimiento (UAV, robots) que proporcionan ataques y fuegos".

CONCLUSIONES

En el futuro, la victoria se ganará y se perderá en el espacio
de la información, no en el campo de batalla físico.

Sean McFate, *Las nuevas reglas de la victoria*

La hipótesis formulada inicialmente en la Introducción decía que "El progreso de las TICs en la última década ha priorizado el uso de Operaciones de Información en todos los umbrales de la conducción, por lo que ahora se ha hecho imprescindible integrarlas completamente con las operaciones militares convencionales cinéticas. "Dentro de estos límites militares, y con la definición adoptada por Occidente, la hipótesis ha sido corroborada. No obstante, la investigación llevó por otros derroteros que deben ser explorados porque denotan otra forma de hacer la guerra diferente a la estrictamente militar, ya que algunos autores consideran las OI como operaciones de guerra no militares.

La hipótesis demostrada corresponde a la consideración de las OI como complementarias a las operaciones convencionales, que es la concepción propia o así enunciada por Occidente. En esta concepción, los militares pueden emplear el uso de información para afectar los resultados no solamente sobre formaciones militares adversarias. Según la concepción rusa las OI también influencian a múltiples audiencias simultáneamente, afectando actores estatales, sociedades e individuos no solo en el teatro geográfico del conflicto, sino globalmente. Estas características actuales y emergentes requerirían que las futuras fuerzas armadas aprovechen la información y tecnologías asociadas, para entender el ambiente operacional y emplear capacidades, para lograr efectos informativos a través de múltiples sistemas y audiencias para alcanzar objetivos militares. (Perceptions are reality, 2018, pág. 173). Por lo tanto, para los rusos, el uso de la información comenzaría en el nivel estratégico, porque alcanzaría a todos los componentes el poder nacional. Con los avances tecnológicos, se reduce la brecha entre los niveles estratégicos y tácticos.(Perceptions are reality, 2018, pág. 20). Aquí, de la estrategia militar se pasa a la estrategia política.

En cuanto a la adopción de definiciones doctrinarias para OI, habría que aclarar que la función conjunta inteligencia trata del enemigo, de sus fortalezas y debilidades,

de sus capacidades y limitaciones, de sus cursos de acción probables o posibles, y de la influencia del terreno en las operaciones militares. No obstante, la función conjunta información trata de las percepciones creadas y la narrativa de un conflicto que influyen en la opinión pública propia y adversaria para que pueda ser empleada en provecho de los propios objetivos políticos.

Se sugiere que una definición de Operaciones de Información sea incluida en el Glosario Conjunto de las Fuerzas Armadas, y que en razón de no identificarse con competencia de países centrales, se adopte como concepto básico el de la organización no gubernamental Facebook que dice

> Definimos las operaciones de informaciyn, […..] como acciones tomadas por actores organizados (gobiernos o actores no estatales) para distorsionar el sentimiento político nacional o extranjero, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una combinación de métodos, como noticias falsas, desinformación o redes de cuentas falsas destinadas a manipular la opinión pública (nos referimos a estos como "amplificadores falsos").(Facebook Inc , 2017, pág. 4)

Podría agregarse que buscan efectivamente "cambiar actitudes, creencias y comportamientos de audiencias propias, neutrales, adversarias y enemigas, para apoyar a los propios objetivos políticos", pero este agregado debería ser políticamente aceptado en países cuyos valores esgrimidos públicamente, sean la libertad de expresión y la representación popular como base de los sistemas democráticos.

También debería incluirse junto con los dominios militares, el nuevo ambiente "informaciyn" que influye en todos los dominios civiles y militares, y considerar la información como función conjunta. Una función es una actividad particular o tarea distintiva que realiza una persona o cosa dentro de un sistema (conjunto de partes relacionadas que llevan al mismo fin). La información es un ambiente nuevo derivado de la evolución de las tecnologías de información y comunicaciones (TICs). Sin embargo, antes de incluir la información como una función conjunta en la doctrina argentina, se debería incluir en la PC 00-01 Doctrina Básica para la Acción Militar Conjunta, las demás funciones conjuntas necesarias para coordinar, sincronizar y dirigir

operaciones conjuntas, que son comando y control, fuego, maniobra y movimiento, protección, sostenimiento e inteligencia.

Se debe tener en cuenta que en el nivel estratégico, cuando las OI se refieren directamente a la manipulación de la narrativa de un conflicto, se extienden más allá de los medios militares, y abarca todos los medios del poder nacional para lograr los intereses nacionales. En el nivel estratégico, es donde la guerra es más política, porque es en el nivel estratégico donde la guerra se une a los objetivos políticos. (McFate, The New Rules for War - Victory in the Age of Durable Disorder , 2019, pág. 177)

Las Capacidades Relacionadas con la Información (CRI) son las herramientas para generar efectos en y a través del ambiente de la información, pero estos efectos casi siempre se logran en combinación con otras CRI. Los efectos que generan estas CRI dan lugar a OI de aplicación a los tres niveles de guerra. Las CRI pueden ser útiles para categorizar las OI, siempre que se tenga en cuenta que las CRI son herramientas para generar efectos en el ambiente de la información. A las acciones para obtener esos efectos deseados se los denomina OI.

Estas CRI evolucionarán para incluir todos los elementos que tengan la capacidad de penetrar en el dominio de la información, dar forma a la actividad de combate físico y maximizar el potencial para las operaciones cinéticas. (Perceptions are Reality, 2018, pág. 17). En esta investigación se ha puesto énfasis en las redes sociales dado la importancia de desarrollo de las TICs.

Las Capacidades Relacionadas con la Información (CRI) propias de la estrategia nacional son mucho más amplias que las disponibles para la estrategia militar. En el nivel estratégico nacional, incluirían tanto a las operaciones de la red informática junto con otras disciplinas como las operaciones psicológicas, las comunicaciones estratégicas, las operaciones de influencia, las acciones en el campo de inteligencia, la contrainteligencia, la disuasión, la desinformación, la guerra electrónica, el debilitamiento de las comunicaciones, la degradación del apoyo informático, la presión psicológica y la destrucción de las capacidades informáticas enemigas. (Keir Giles, Handbook of Russian Information Warfare, 2016, pág. 15)

En cambio, las Capacidades Relacionadas con la Información de los niveles militares operacional y táctico son una extensa lista de capacidades que tengan el potencial de influir en el ambiente de información de esos niveles, tales como Actividades Ciber-Electromagnéticas (CEMA), Operaciones de Apoyo a la Información Militar (MISO) u Operaciones Sicológicas (PSYOP), Asuntos Civiles (CA), Cámara de Combate (COMCAM), Equipos Humanos en el Terreno (HTTs)[28], operaciones especiales, operaciones de Técnicas Especiales y Engaño, y Compromisos de Soldados y Líderes (SLEs).

Existen otras CRI en los ámbitos político, económico y social, que son propias de la comunicación estratégica del nivel nacional. Como ya se expresó, solo a través de la sincronización interagencial eficaz y efectiva de las CRI con las líneas de operaciones físicas los comandantes podrían obtener una ventaja decisiva sobre los adversarios, las amenazas y los enemigos.

Asimismo, hay que diferenciar la denominada Guerra de la Información, de las Operaciones de Información. Mientras que las Guerras de la Información en su mayoría se restringen a las acciones tácticas resultantes de amenazas de una competencia en la obtención, difusión y uso de la información, y por lo tanto una responsabilidad del campo de inteligencia dentro del conocido ciclo de la inteligencia, las OI incluyen no solamente el uso de tecnología, sino también los aspectos humanos relacionados con el uso de la información y su influencia en la opinión pública, por lo que son una responsabilidad del campo de operaciones. Como se señala en el libro Percepciones son Realidad, "En otras palabras, OI se refiere a acciones de propia tropa en el entorno de información, mientras que Guerra de la Información se usa para describir actividades basadas en amenazas." (Perceptions are Reality, 2018, pág. 34)

El aspecto humano y la dependencia humana en la tecnología son inseparables.(Perceptions are reality, 2018, pág. 146) . La información es vital para la toma de decisiones humana y automatizada. La discusión que persiste es si se trata de

[28] Los Equipos Humanos en el Terreno es un grupo de medios civiles y militares específicamente entrenados para interactuar con la población local para entender la mejor forma de ayudar la transición a un pais estable y seguro. Fueron inicialmente implementadas en Iraq 2003. También trata de una alerta cultural para poder evaluar las repercusiones futuras de acciones militares y evaluar los efectos de acciones propias. Ver https://www.army.mil/article/40079/htt_builds_experience_at_ntc , traducción propia.

una Revolución en Asuntos Militares, donde la guerra tendría una nueva forma de hacerse, un nuevo propósito y requeriría ser conducida de otra forma. La opinión generalizada es que toda Revolución en Asuntos Militares fue precedida por un salto tecnológico. No hay consenso en este tema, y la opinión general es que la naturaleza y el propósito de la guerra permanecen, pero lo que cambia es la forma en que se conducen las operaciones. Por lo tanto, lo que se parece esbozar es que nos encontramos en una forma nueva de hacer la guerra, al decir de los autores chinos Qiao y Wang, una nueva arma "bondadosa". (Qiao y Wang, Unrestricted Warfare, 1999, pág. 17). La situación de esta nueva forma de hacer la guerra es que la línea divisoria en niveles de guerra y entre lo que es ataque y defensa, quede muy desdibujada. Un Comandante debe tratar de negar, degradar o destruir las capacidades del enemigo con el que está enfrentado lo más rápidamente posible, entendiendo que su enemigo está tratando de hacer exactamente lo mismo al mismo tiempo, sin detenerse a pensar si ataca o se defiende. (Perceptions are Reality, 2018, pág. 157). Este tema acerca de una forma diferente de hacer la guerra a lo que se hace hasta ahora, debe ser motivo de otra investigación por separado, porque en algunas opiniones esta forma evolucionada de guerras de Cuarta Generación constituirían Guerras de Quinta Generación. Esta opinión no es compartida por muchos teóricos.

Por último, y tal cual se menciona en las limitaciones de la Introducción, se debe enfatizar que esta investigación no tuvo por finalidad discutir el marco legal argentino, sino conocer lo que está ocurriendo en el mundo. Como dijeron los autores chinos Qiao y Wang en "La guerra más allá de los límites" (1999),

> Dada esta situación, solo es necesario ampliar el punto de vista, en donde podremos ver que la seguridad nacional basada en el regionalismo ya está anticuada. La principal amenaza para la seguridad nacional está lejos de limitarse a la agresión militar de fuerzas hostiles contra el espacio natural del país. (Qiao y Wang, Unrestricted Warfare, 2002, pág. 96)

Aceptar este ambiente de actuación también significará delinear las capacidades necesarias, los ajustes a las estructuras de las Fuerzas Armadas y la preparación del personal militar para enfrentar estas nuevas circunstancias del ambiente de la información. Se esbozan ciertas medidas organizativas y para el personal en el Capítulo III de esta investigación.

Las Operaciones de Información como efecto de las CRI son un aspecto nuevo, parte de la aproximación indirecta con medios no militares, que todavía debe ser mejorado puesto que se encuentra en desarrollo, y las potencias centrales en pugna - EEUU, Rusia y China - se acusan mutuamente de usarlas en provecho propio. Los países periféricos deben cuidar sus alianzas para evitar ser campos de batalla marginales producto de la divergencia de intereses de los países mencionados.

Las campañas de información buscan dar idea de consensos y opiniones públicas generalizadas, para esgrimir clamores populares y poder hacer lo que se desee para llegar, ejercer y mantenerse en el poder. El riesgo más grande es que la desinformación, la manipulación y las redes sociales venzan el espíritu de resistencia de los hombres y las naciones haciéndoles ver como favorables a situaciones que van en contra de sus intereses legítimos, y su bienestar.

Al decir del prologuista Juan Grabois al libro de Andrew Korybo, el progreso de las TICs "Por otro lado, la revolución digital cambió radicalmente los parámetros de la vida social, política y cultural de buena parte del mundo. Se aceleraron los tiempos para todos los procesos de producción y distribución. La circulación de la información aumentó a un ritmo geométrico. Se consolidó la capacidad de las redes sociales de influir en las percepciones, ideas, emociones y acciones de grandes masas humanas. Así, el ciberespacio paso a ser otro teatro de guerra".(Korybko, Guerras Híbridas Revolución de Colores y Guerra No Convencional, 2015, pág. 21).

También es importante un concepto expresado por el Coronel Thomas Hammes en "The Sling and the Stone", que expresa que

> Las Guerras de 4ta Generación (G4G) usa todas las redes disponibles - políticas, económicas, sociales y militares- para convencer a los que toman las decisiones del enemigo de que sus objetivos estratégicos son inalcanzables o demasiado costosos por el beneficio percibido. Es una forma evolucionada de insurgencia[29]. Todavía enraizada en el precepto fundamental de que una voluntad política superior podrá, cuando sea empleada apropiadamente, vencer a una potencia económica y militar más grande, las G4G hace uso de las redes de la sociedad para llevar a cabo su lucha. Contrariamente a las previas generaciones de guerra,

[29] El subrayado es nuestro.

> no intenta ganar derrotando a las fuerzas militares del enemigo. En su lugar, usando las redes, ataca directamente la mente de los decisores del enemigo para así destruir su voluntad política. Las G4G son prolongadas y se miden en décadas antes que en meses o años. (Hammes, 2006, pág. 2)

Es el poder del ambiente de la información, que influye en los dominios militares de aire, mar, tierra y espacio.

ENCUESTAS DE OPINION Y CONFERENCIAS

ENCUESTAS DE OPINION 1

FECHA DE REALIZACION: 24 de agosto de 2020

ENCUESTADO: se encuestó a 1 (un) oficial argentino en actividad en Ecuador, 2 (dos) oficiales retirados argentinos, y a 5 (cinco) oficiales superiores extranjeros cursantes del Curso de Estrategia Militar y Conducción Superior, de la Escuela Superior de Guerra Conjunta de las Fuerzas Armadas de la República Argentina

PREGUNTAS: tuvieron 2 formatos, para oficiales argentinos y oficiales extranjeros.

RESPUESTAS: se agregan por separado.

PREGUNTAS PARA OFICIALES ARGENTINOS:

Pregunta 1: En la última década del Siglo XX hubo un creciente adelanto en la tecnología de Información y Comunicaciones, conocida por las TICs. ¿Estima Usted que ese progreso tecnológico modificó el carácter, el propósito y la forma de conducir la guerra?

Pregunta 2: Puede considerarse el progreso de las TICs una Revolución en Asuntos Militares?

Pregunta 3: Este crecimiento e influencia de las TICs dio lugar a las denominadas Operaciones de Información. En el año 2019 la Información fue introducida por las FFAA de EEUU como 7ma función conjunta, necesaria junto con las otras seis para liderar, coordinar, integrar y sincronizar las operaciones conjuntas. Al respecto, durante mi investigación he hallado que existen tres definiciones

En Occidente;

El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Información, en conjunto con otras líneas de operación para influenciar, interrumpir, corromper o usurpar el proceso de toma de decisiones de adversarios o potenciales adversarios mientras se protege a los propios.

En Rusia

Un conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y comunidad internacional en todos los niveles.

También una ONG (Facebook) las define como

Definimos las operaciones de información, […..] como acciones tomadas por actores organizados (gobiernos o actores no estatales) para distorsionar el sentimiento político nacional o extranjero, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una combinación de métodos, como noticias falsas, desinformación o redes de

cuentas falsas destinadas a manipular la opinión pública (nos referimos a estos como "amplificadores falsos").

Con cuál de estas definiciones está Usted más de acuerdo?

Pregunta 4: Cree Usted conveniente que se incluya en la doctrina militar argentina a la Información como una función conjunta para la conducción de las operaciones militares conjuntas?

PREGUNTAS PARA OFICIALES EXTRANJEROS

Pregunta 1:¿Las Operaciones de Información, entendidas como

El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Información, en conjunto con otras líneas de operación para influenciar, interrumpir, corromper o usurpar el proceso de toma de decisiones de adversarios o potenciales adversarios mientras se protege a los propios y según otras definiciones

Un conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y comunidad internacional en todos los niveles, o bien

las operaciones de información, […..] como acciones tomadas por actores organizados (gobiernos o actores no estatales) para distorsionar el sentimiento político nacional o extranjero, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una combinación de métodos, como noticias falsas, desinformación o redes de cuentas falsas destinadas a manipular la opinión pública (nos referimos a estos como "amplificadores falsos").

Son doctrinarias en su país?

Pregunta 2: Si están en la doctrina de su país, en que publicación conjunta o reglamento se encuentran definidas?

Pregunta 3: la cibernética es una de las formas de llevar a cabo Operaciones de Información. Se hace mención a ellos en la Política de Defensa o en los Libros Blancos de la Defensa?

Cualquier otra referencia al tema será agradecida.

Fin de texto

ENCUESTAS DE OPINION 2

FECHA DE REALIZACION: 26 de Septiembre de 2020

ENCUESTADO: TC EA (R) GUILLERMO CAMPOS

PREGUNTAS: Antecedentes de Operaciones de Información en la Argentina

RESPUESTAS:

Pregunta 1: En la última década del Siglo XX hubo un creciente adelanto en la Tecnología de Información y Comunicaciones, conocida por las TICs. ¿Estima Usted que ese progreso tecnológico modificó el carácter, el propósito y la forma de conducir la guerra?

> Sin duda modificó el carácter de la guerra y la forma de conducción. No así su propósito, puesto que éste siempre es de carácter político.

Pregunta 2: Puede considerarse el progreso de las TICs una Revolución en Asuntos Militares?

> Depende de la lo que entendamos por RAM. Si, si lo entendemos en el sentido que refiere George [Geoffrey]Parker, lo es, tal como lo fue la aparición del arma de fuego o su evolución hacia la retrocarga, la pólvora sin humo o el tubo cañón de ánima rayada; el telégrafo - bien lo señala Keegan en la Máscara del Mando - modificó la forma de conducción y promovió la aparición del moderno Estado Mayor y así con otras tecnologías. Sin embargo, pienso que la guerra en su carácter refleja el carácter de la sociedad que la libra. Me explico. El impacto de las TICs produjo profundos cambios en las formas de vincularnos, hacer política, comerciar, educar, ejercer el poder soberano por parte de los estados nación, etc. De igual modo, ese cambio social deviene en un cambio en las formas en que se libra la guerra. Cambio no absoluto ni universal, ya que convivimos con diferentes modos de hacer la guerra, algunos propios de nuestra cultura tecnológicamente avanzada y otros que podemos encontrar en las guerras coloniales del siglo XIX.

Pregunta 3: Este crecimiento e influencia de las TICs dio lugar a las denominadas Operaciones de Información. En el año 2019 la Información fue introducida por las FFAA de EEUU como 7ma función conjunta, necesaria junto con las otras seis para liderar, coordinar, integrar y sincronizar las operaciones conjuntas. Al respecto, durante mi investigación he hallado que existen tres definiciones

En Occidente;

El empleo integrado, durante operaciones militares, de Capacidades Relacionadas con la Información, en conjunto con otras líneas de operación para influenciar,

interrumpir, corromper o usurpar el proceso de toma de decisiones de adversarios o potenciales adversarios mientras se protege a los propios.

En Rusia

Un conjunto de sistemas, métodos y tareas para influir en la percepción y el comportamiento del enemigo, la población y comunidad internacional en todos los niveles.

También una ONG (Facebook) las define como

Definimos las operaciones de información, […..] como acciones tomadas por actores organizados (gobiernos o actores no estatales) para distorsionar el sentimiento político nacional o extranjero, con mayor frecuencia para lograr un resultado estratégico y / o geopolítico. Estas operaciones pueden utilizar una combinación de métodos, como noticias falsas, desinformación o redes de cuentas falsas destinadas a manipular la opinión pública (nos referimos a estos como "amplificadores falsos").

Con cuál de estas definiciones está Usted más de acuerdo?

> Las tres son válidas y las dos últimas similares. No son excluyentes. Si sólo nos posicionamos en el nivel EM, NO o Táctico, la más adecuada es la primera. Las dos últimas, son más abarcativas y apropiadas para el nivel Estratégico Nacional, aunque incluyen tácitamente la primera. Serían concepto similares a lo que John Arquilla y David Ronfeldt denominan Net War. En síntesis, si se trata de una definición para incluir en la doctrina específica o conjunta, la primera es válida. Las otras dos debieran ser consideradas como parte de una “doctrina” político - estratégica. Es en ese nivel en que la emplea Rusia, al igual que otro término que en los EEUU tiene un significado exclusivamente militar: la Net Centric Warfare y en Rusia tiene un significado político - estratégico.
>
> Una salvedad. La Información como función, tal como usted la describe, se corresponde con lo que se denomina Gestión de la Información. Las Operaciones de Información, en su faz defensiva, contribuyen a una adecuada Gestión de la Información, es decir que ésta llegue integra, oportunamente a la persona correcta, a quien la necesita y con el formato adecuado para que la pueda introducir en su proceso de toma de decisiones. En su faz ofensiva procura lo que expresa la definición citada. Por lo tanto, debemos distinguir la Función de las Operaciones de Información.

Pregunta 4: Cree Usted conveniente que se incluya en la doctrina militar argentina a la Información como una función conjunta para la conducción de las operaciones militares conjuntas?

Sin ninguna duda, pero también deberían ser incluidas las Operaciones de Información.

FIN DE TEXTO

ENCUESTAS DE OPINION 3

FECHA DE REALIZACION: 4 de agosto de 2019

ENCUESTADO: TC EA IVAN GNIESKO

PREGUNTAS: Antecedentes de Operaciones de Información en la Escuela de Guerra del Ecuador

RESPUESTAS:

El TC EA Iván Gniesko se desempeña como alumno de la EG Ecuador en el año 2019.

Adjunta como respuestas tres notas de Aula que trata cada una sobre el desarrollo de una Unidad Didáctica de Operaciones Psicológicas.

La Nota de Aula 1 es un documento de la Dirección de Comunicación Social del Ejército, sobre Operaciones Psicológicas, UD 1.

La Nota de Aula 2 es un documento de la Dirección de Comunicación Social del Ejército, sobre Operaciones Psicológicas, UD 2.

La Nota de Aula 3 es un documento de la Dirección de Comunicación Social del Ejército, sobre Operaciones Psicológicas, UD 3

Detalla el encuestado que el tema que se imparte en la Escuela de Guerra de Ecuador es Operaciones de Información/Operaciones psicológicas.

ENCUESTAS DE OPINION 4

FECHA DE REALIZACION: 24 de agosto de 2020

ENCUESTADO: Coronel Luftwaffe BERND PFAFFENBACH

PUESTO QUE DESEMPEÑA: Cursante del CEMCS/ESGC 2020

PREGUNTAS: las correspondientes a Oficiales Extranjeros

FECHA DE RECEPCION DE LA ENCUESTA: 01 Octubre 2020

RESPUESTAS:

Respuesta 1:

En Alemania no hay un debate intensivo sobre doctrinas. La mayor parte de esto se puede atribuir a los resultados de la Segunda Guerra Mundial. Pero eso no significa que no existan documentos estratégicos comparables. El tema de la información ya se trata de manera amplia en el Libro Blanco de 2016 en la sección CONDUCCIÓN. El tema se concreta en la concepción de las Fuerzas Armadas Federales 2018 derivada del Libro Blanco, donde se lleva a cabo en términos de superioridad y resiliencia informativa. El principal responsable es el área CIR (espacio cibernético y de información) de nueva creación, que debe trabajar en esta nueva dimensión para toda el área de la Bundeswehr tanto en tiempos de paz como en operaciones de crisis y guerra.

Parte de las operaciones en el espacio cibernético y de información son precisamente las operaciones de información indicadas anteriormente, que se supone que son capaces de reaccionar ante la propaganda y desinformación de un oponente.

Respuesta 2:

La información correspondiente sobre responsabilidades y contenido se puede encontrar tanto en el Libro Blanco de 2016 como en el concepto de la Bundeswehr de 2018. Esto es lo que dice el concepto de la Bundeswehr:

El entorno de la información es el espacio en el que se desarrollan los procesos cognitivos, sensoriales, interpretativos, intelectuales y comunicativos y sobre la base del cual las personas ajustan sus actitudes, voluntades y comportamientos.

La comunicación dirigida, coordinada y coherente de la Bundeswehr a través de palabras explicativas y acción militar se lleva a cabo de acuerdo con la narrativa política en el entorno de la información. El oponente utiliza el entorno de la información para la agitación, la demagogia, la desinformación y la propaganda. La Bundeswehr protege a su propio personal fomentando la resiliencia cognitiva.

Las operaciones en el espacio cibernético y de la información son cada vez más importantes. Las operaciones cibernéticas amplían la gama de opciones militares para la acción de manera complementaria, o sustitutiva en toda la gama de tareas de la Bundeswehr.

El combate electrónico (EK) comprende todas las medidas militares ofensivas y defensivas en la disputa sobre el uso del espectro electromagnético (EMS) como parte del espacio cibernético y de información en todo el espectro de capacidades militares. El EK contribuye a asegurar su propio liderazgo y capacidad operativa, protege sus propias fuerzas, apoya de la manera más eficaz posible el uso apropiado y la efectividad de sus propios sistemas de armas, perjudica la capacidad del oponente para usar el EMS y, por lo tanto, el uso y desarrollo de sus capacidades a largo plazo.

Además de los factores fuerzas, espacio y tiempo, la información factorial cobrará cada vez más peso en el futuro. Debido a la diseminación de información rápida y global, a menudo sin filtros, y la desinformación dirigida, la “batalla de la informaciyn” puede comenzar mucho antes del inicio de una operación militar. Por lo tanto, las acciones militares deben evaluarse en una etapa temprana con respecto a su efecto en el entorno de la información.

Respuesta 3:

Definitivamente sí. Todos los documentos estratégicos contienen pasajes claros sobre este tema. Los desafíos del espacio cibernético y de la información también se deben dominar mejor mediante el establecimiento de un área organizativa independiente. La Bundeswehr tiene hoy 6 en lugar de las 3 fuerzas armadas habituales (ejército, fuerza aérea, marina). A las 6 áreas las denominamos áreas organizativas. El espacio cibernético y de información es el área más joven. Fue creado en 2017.

Cualquier otra referencia al tema será agradecida. Muchas gracias.

FIN DE TEXTO

ENCUESTAS DE OPINION 5

FECHA DE REALIZACION: 24 de agosto de 2020

ENCUESTADO: Coronel EB MOACYR COUTO JUNIOR

PUESTO QUE DESEMPEÑA: Cursante del CEMCS/ESGC 2020

PREGUNTAS: las correspondientes a Oficiales Extranjeros

FECHA DE RECEPCION DE LA ENCUESTA: 24 Octubre 2020

RESPUESTAS:

Respuesta 1:

Si, las Operaciones de Información son doctrinarias.

En la doctrina brasileña, las operaciones de información (OpInfo) consisten en coordinar el empleo capacidades integradas relacionadas con la información, en contribución a otras operaciones o incluso constituir el esfuerzo principal, para informar e influir en las personas o grupos hostiles, neutrales o favorables, capaces de impactar positiva o negativamente con la finalidad de alcanzar objetivos políticos y militares, así como comprometer el proceso de toma de decisiones de los oponentes o potenciales oponentes, garantizando al mismo tiempo la integridad de nuestro proceso.

La OpInfo contribuye en gran medida a obtener la superioridad de la Información, que se caracteriza por el alcance de la ventaja, persistente o transitoria, resultante de la capacidad de brindar información útil a los usuarios interesados e interesados, en el momento adecuado y en el formato adecuado, negando la oponente las oportunidades para lograrlo.

Además, las operaciones de información se planifican y realizan a nivel estratégico, operativo y tatico en situaciones de guerra y no guerra. En el Nivel Estratégico, las OpInfo se diseñan en el marco de acciones estratégicas, las cuales se guían por condiciones y lineamientos políticos. Estas acciones pueden resultar de demandas u oportunidades relacionadas con el entorno interno y externo del país.

Respuesta 2:

En el ámbito del Ministerio de Defensa, las operaciones de informaciones están reglamentadas en la reciente publicación MD30-M-01 -“DOUTRINA DE OPERAÇ®ES CONJUNTAS” - (2ª Edição/2020), de 15 de Septiembre de 2020, en los volúmenes 1 y 2.

En el ámbito de las fuerzas singulares, el Ejército Brasileiro publicó el EB70-MC-10.213 “OPERAÇ®ES DE INFORMAÇÃO” (2ª Edição/2019), que trata sobre la temática

Respuesta 3:

Las capacidades relacionadas a las operaciones de información, según la visión brasileña, son: Operaciones Psicológicas, Acciones de Guerra Electrónica, Ciberdefensa, Comunicación Social y Asuntos Civiles.

Con respecto específico a la cibernética, ningún de los principales documentos de defensa del país, como el Libro Blanco de la Defensa, la Política Nacional de Defensa y la Estratégica Nacional de defensa, que están en vigor desde 2012, no citan la relación de la cibernética con las Operaciones de Información. Tampoco, la reciente revisión de los citados documentos encaminada, en junio de este año, para el Congreso Nacional para aprobación también no incluyó la presente temática.

Sin embargo, el documento doctrinario MD31-M-07, "DOUTRINA MILITAR DE DEFESA CIBERNÉTICA -(1ª Edição/2014), en el capítulo IV, aborda la participación de la Cibernética en el contexto de las Operaciones de Información en el ámbito del Estado Mayor Conjunto.

FIN DE TEXTO

ENCUESTAS DE OPINION 6

FECHA DE REALIZACION: 24 de agosto de 2020

ENCUESTADO: Coronel EPL China YIN ZIYHONG

PUESTO QUE DESEMPEÑA: Cursante del CEMCS/ESGC 2020

PREGUNTAS: las correspondientes a Oficiales Extranjeros

FECHA DE RECEPCION DE LA ENCUESTA: 01 Octubre 2020

RESPUESTAS:

NOTA: el Coronel EPL YIN ZHIYONG interrumpió el curso el 20 de octubre y regresó a China.

Por el carácter ideológico del régimen Chino, el Coronel Yin Zhiyong solo puede proporcionar respuestas aprobadas por el Comité del Partido y su Presidente Xi Jinping. Por lo tanto, antes de contestar las preguntas, se limitó a repetir los conceptos que aparecen en el Libro Blanco de Defensa China 2020.

> "Las redes de información son una nueva tendencia que ha cambiado profundamente el entorno ideolygico y de la opiniyn pública. [….] Se debe mantener el ritmo de la tecnología de la información, servir a la guerra de información, aumentar el nivel de la tecnología de la información, para poner las alas al trabajo política tradicional, para lograr la integración orgánica de los portadores de la red y el trabajo político propiamente dicha, así como la gran integración de las ventajas tradicionales con la tecnología de la informaciyn.[….] Debemos estudiar y comprender activamente las características y leyes del trabajo político en la era de las redes de información, llevar a cabo las luchas de la opinión pública en línea como si estuviéramos librando una guerra, seguir de cerca las características cognitivas de los jóvenes oficiales y soldados al llevar a cabo la educación ideológica y política en línea.[….] promover la integraciyn del trabajo política en el sistema de información de la red y el sistema de operación conjunta, y hacer de la red de información un "multiplicador" que dé pleno juego a las ventajas tradicionales del trabajo político."

FIN DE TEXTO

NOTA: Por lo que surge de la opinión general de los medios, mientras Occidente pone énfasis en la mejora tecnológica y estandarización de los medios militares convencionales, y China presuntamente copia los desarrollos tecnológicos occidentales, pero lleva su énfasis en las tecnologías y estandarización de los medios de comunicación e informaciones (plataforma TikTok, Huawei, 5 G, Zoom)

CONFERENCIA DEL CORONEL EB DR MARCIO SALDANHA WALKER

Fecha de la exposición: 23 de junio 2021, 1130 hs a 1300 hs

Modo de la exposición: remoto, *google meet*, link https://meet.google.com/oqm-gjrc-jtd?amp;authuser=1

La grabación y la transcripción del chat están disponibles en el Nivel 2, plataforma educativa virtual

Conferencia "Las Operaciones de Información" CR M. Saldanha Walker (2021-06-23 at 07:31 GMT-7)

Asistentes: 99 oyentes del N 1 y N2 de la ESGC año 2021

Presentador: Director de Carrera de la Maestría en Estrategia Militar (N2) Brigadier Mayor (Ret) Alejandro Moresi

Temas tratados: Operaciones de Información - Definición - Ambiente Operacional - dimensiones humanas, informacional y física - Capacidades Relacionadas con la Información (CRI) - Planeamiento Estratégico y Operacional - Conclusiones finales

Resumen de lo expresado

El CR Walker comenzó con una estadística sobre el conocimiento de los alumnos argentinos de la Especialización en Estrategia Operacional de la ESGC 2021sobre los conocimientos sobre Doctrina de Operaciones de Información, Operaciones Psicológicas, Guerra Electrónica, y Comunicación Social, concluyendo que los conocimientos son insuficientes.

Acerca de las definiciones de OI en Brasil, existe una en el Manual del Ejército (2014) y otra en el Manual del Ministerio de Defensa (2020). Se trata de la percepción, que trata de biología, experiencia y parámetros de medición, propia de la niebla de Clausewitz ya que se entrelazan conceptos sobre informaciones/inteligencia, tecnología, apoyo de la Información Militar, información pública y otros que detalló en los slides.

Las OI juegan cada vez más un rol importante en los conflictos y así están siendo consideradas en todo el mundo. Las OI son efectos integrados de las Capacidades Relacionadas con la Información.

En cuanto al ambiente operacional, hay tres dimensiones: la humana que también se llama cognitiva, la informacional que son medios no cinéticos que no respetan fronteras y alcances, y la física, que trata de la influencia sobre los medios cinéticos.

Las OI son un concepto ligado a las denominadas guerras híbridas o guerras en la zona gris. Por lo tanto, las amenazas vienen de todos lados, tanto de os medios cinéticos como no cinéticos.

Las Capacidades Relacionadas con la Información en Brasil son de multidominio: Comunicación social, Operaciones Psicológicas, Guerra Electrónica, Asuntos Civiles, Apoyo de Información Militar, y Guerra Cibernética. Es un trabajo inter agencial,

porque el nivel estratégico es el que asegura que los efectos sean en una misma dirección.

En el planeamiento estratégico y operacional, hay una diferencia entre Argentina y Brasil: mientras que para la Argentina el efecto deseado de las OI en la Estrategia Militar es sobre modos y acciones militares, en Brasil el efecto deseado de las OI es en el nivel estratégico, incluyendo todos los modos y acciones de todos los componentes del poder nacional.

En la conducción operacional se trata de líneas de operaciones de información que tiene en cuenta los efectos cinéticos y no cinéticos de ese nivel.

En Brasil, ya existe una estructura permanente de OI en el Comando de Operaciones Terrestres, y ahora se hará en el Estado Mayor Conjunto.

Como Conclusiones Generales, el CR Walker expresó que las OI son conjuntas; la gestión de las OI debe ser conjunta; los efectos y objetivos de las OI deben estar bien definidas entre las Fuerzas Armadas; y que los principales actores son el Ministerio de defensa y el Estado Mayor Conjunto de las Fuerzas Armadas.

Preguntas de los oyentes: si dado la nueva forma de hacer la guerra con armas bondadosas amerita que esta evolución de las Guerras de Cuarta Generación sea denominada Guerras de Quinta Generación, como sugieren algunos académicos, dijo que en Brasil no se consideran como Guerras de Quinta Generación, sino que se enfatiza el trabajo inter agencial.

De las otras preguntas, surge que para los argentinos, las OI son parte de la Estrategia Militar, porque las quieren incluir en la clasificación de las operaciones militares; y para Brasil se trata de una Estrategia Política de todos los componentes el poder nacional.

Fin de texto.

BIBLIOGRAFIA

LIBROS

EMC FFAA, (2015) Publicación Conjunta PC 00-02 Glosario de Términos de Empleo Militar para la Acción Militar Conjunta.

EMC FFAA, (2018) Publicación Conjunta PC 00-01 Doctrina Básica para la Acción Militar Conjunta.

Hammes Thomas USMC (2006) The Sling and the Stone, On war in the 21st Century, Zenith Press, Michigan, Ed 2006.

Korybko Andrew, (2019), Guerras Híbridas, Revoluciones de Colores y Guerra No Convencional, Editorial Batalla de Ideas, Buenos Aires

Le Bon Gustavo, (1972) Psicología de las multitudes, Editorial Albatros, Buenos Aires, Argentina.

Libicki Martin, (1995) What is Information Warfare, National Defense University, Institute for National Strategic Studies.

Lind William y otros (1989), The Changing Face of War: Into the Fourth Generation, Marine Corps Gazette, October 1989, Pages 22-26

National Defense University, (2009) Cyberpower and National Security, Edited by Franklin D. Kramer, Stuart H. Starr, y Larry K. Wentz, Potomac Books Inc 2009, Center for Technology and National Security Policy, National Defense University, Washington DC

PC 20-01 (2017) Planeamiento para la Acción Militar Conjunta - Nivel Operacional (Proyecto), Escuela Superior de Guerra Conjunta de las Fuerzas Armadas

Qiao Liang y Wang Xiangsui, (2002) Unrestricted Warfare, Panama Publishing Co, Panama.

Schiuma Carlos,(1976) El Ejército Argentino y la Revolución de Mayo, Su función política, las teorías del poder, Editorial Huemul, Buenos Aires , 1976

Schwarzkopf H. Norman, (1994) The Autobiography It doesn´t take a heroe, Plaza y Janes Editores, 1994, Globus Communications, Madrid 1994.

US Army, (2018) Perceptions are reality, Historical Case Studies of Information Operations in Large Scale Combat Operations, Edited by Vertuli Mark y Loudon Bradley, Army University Press, Fort Leavenworth, Kansas, 2018.

USA Guerra Convencional: Lind, William S., Nightengale, Keith, Schmitt, John F., Sutton, Joseph W., Wilson, Gary I. (1989) "The Changing Face of War: Into the Fourth Generation" Marine Corps Gazette, October 1989, Pages 22-26

PAGINAS WEB

Bartles Charles, (2016) artículoGetting Gerasimov Right, publicado en US Military Review, The Professional Journal of the IS Army, Ed January February 2016, disponibleenhttps://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art001.pdf

BBC Mundo, (2012) artículo Los riesgos de Facebook para los soldados, Redacción BBC Mundo, 10 Mayo 2012, disponible en https://www.bbc.com/mundo/noticias/2012/03/120309_soldados_riesgo_redes_sociales_jgc

Becara Barbara, (2016) Cómo Netflix y Uber aprovechan los Big Data, artículo en Siliconweek, 16 Marzo 2016, disponible en https://www.siliconweek.com/data-storage/bigdata/netflix-uber-aprovechan-los-big-data-70067

Catalinas Alvaro, (2019) Rusnet el nuevo intranet de Rusia, artículo publicado en Cyberseguridad Pyme, 30 Abril 2019, disponible en https://www.ciberseguridadpyme.es/actualidad/intranet-rusia/?cn-reloaded=1

Cicalese Carmine,(2013) Redefining Information Operations, artículo publicado en Joint Forces Quarterly (JFQ) Nro. 69, 2nd Quarter 2013, National Defense University Press, disponible en https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-69/

Çalişkan, M. (2015). A Critique of Hybrid Warfare in the Light of Russia-Ukraine Crisis and Military Strategy, disponibleenhttps://behorizon.org/a-critique-of-hybrid-warfare/

China, Libro Blanco de Defensa de China 2019, China National Defense in a New Era, publicado oficialmente por The State Council Information Office of the People's Republic of China, Foreign Languages Press Co. Ltd., Beijing, China, 57 páginas.

Colom Piella Guillemo y Fojón Chamorro Enrique. (2015) artículo ¿Oportunidad O Riesgo? Redes Sociales y Fuerzas Armadas, Revista de Aeronáutica y Astronáutica, Nro. 485 Julio/Agosto 2015, Madrid, España, disponible en https://www.academia.edu/25950091/_Oportunidad_o_riesgo_Redes_sociales_y_fuerzas_armadas

Comando Conjunto de las Fuerzas Armadas del Ecuador (2014), Manual de Operaciones de Información, disponible en http://www.coed.mil.ec/Manual_Operaciones_lnformacion.pdf

Christopher Paul, (2019) RAND Corporation, It is time to abandon the term Info Op, disponibleenhttps://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html

Delbert Ronald, (2019) The Road to Digital Unfreedom: Three Painful Truths About Social Media, publicado por la John Hopkins University Press, Journal of Democracy, Volume 30, Number 1, January 2019, disponibleenhttps://muse.jhu.edu/article/713720/pdf

Ecuador Comando Conjunto de las Fuerzas Armadas, (2014) Manual de Operaciones de Información, Dirección de Educación y Doctrina Militar, Quito. Disponible en https://es.slideshare.net/kaluco/manual-de-operaciones-de-informacin-resolucin-14-diedmild003-del-14-de-agosto-de-2014

Facebook Inc. (2017), Information Operations and Facebook, Facebook Security, 27 Abril 2017, disponibleenhttps://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf

Fedyk Nicholas, (2017) "Russian New generation" warfare: theory, practice, and lessons for u.s. strategists", artículo publicado en Small Wars Journal, Mayo 2017, disponibleenhttps://smallwarsjournal.com/jrnl/art/russian-%E2%80%9Cnew-generation%E2%80%9D-warfare-theory-practice-and-lessons-for-us-strategists-0

García Riesco Jesus, (2020) artículo Redes sociales y moral de combate, publicado en Instituto Español de Estudios Estratégicos (IEEE) 79/2020 del 1 de Junio del 2020, disponible enhttp://www.ieee.es/contenido/noticias/2020/06/DIEEEO79_2020JESGAR_redes.html

Gerasimov Valery, (2016) artículo The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, publicado en US Military Review, The Professional Journal of the IS Army, Ed January February 2016, disponibleenhttps://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art001.pdf

Giles Keir, (2016) OTAN Handbook Of Russian Information Warfare, disponibleenhttp://www.ndc.OTAN.int/news/news.php?icode=995

Hoffman Frank (2009) Hybrid Warfare and Challenges, Joint Forces Quarterly Número 52, disponibleenhttps://smallwarsjournal.com/documents/jfqhoffman.pdf

Hurst Luke, (2020) 'Informational chaos': Proposals made to regulate social media, Artículo aparecido en Euronews last update 12/11/2020. Disponibleenhttps://www.euronews.com/2020/11/12/informational-chaos-proposals-made-to-regulate-social-media

Infobae, (2020) artículo El ex CEO de Google dijo que "no hay dudas" de que Huawei envía datos al régimen chino, artículo publicado en la Sección El mundo, disponible en https://www.infobae.com/america/mundo/2020/06/22/el-ex-ceo-de-google-dijo-que-no-hay-dudas-de-que-huawei-envia-datos-al-regimen-chino/

Infobae Argentina,(2020) artículo Twitter cerró miles de cuentas ligadas a los regímenes de China, Turquía y Rusia utilizadas para hacer propaganda de desinformación, de fecha 12 de Junio de 2020, disponible en https://www.infobae.com/america/mundo/2020/06/12/twitter-cerro-miles-de-cuentas-ligadas-a-los-regimenes-de-china-turquia-y-rusia-utilizadas-para-hacer-propaganda-de-desinformacion/

Infodefensa (2019) Regimiento de Operaciones de Información del Ejército echa a andar, (2019) 23 de Julio de 2019, disponible en https://www.infodefensa.com/es/2019/07/23/noticia-regimiento-operaciones-informacion-ejercito-andar.html

JP 3-0 Joint Operations, (2018) con cambio 1, Joint Chief of Staff, disponible en https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

JP 1-0 (2017) Doctrine for the Armed Forces of the United States, Chairman Joint Chiefs of Staff, disponibleenhttps://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Khuel Dan, (2000) Information Operations, the Hard Reality of Soft Power, National Defense University, Information Resources Management College, Washington DC, Disponibleenhttp://www.iwar.org.uk/iwar/resources/jiopc/io-textbook.pdf

Kyle Rempfer, Army Times, (2020) No cellphones, laptops were allowed to go with Army 82nd paratroopers deploying to Middle East, artículo del 6 de Enero de 2020, disponibleenhttps://www.armytimes.com/news/your-army/2020/01/06/no-cell-phones-laptops-were-allowed-to-go-with-82nd-paratroopers-deploying-to-middle-east/#:~:text=No%20cellphones%2C%20laptops%20were%20allowed%20to%20go%20with%20Army,paratroopers%20deploying%20to%20Middle%20East&text=Paratroopers%20deploying%20to%20the%20Middle,Army%2082nd%20Airborne%20Division%20officials.

Lenoir-Grand Pons Ricardo, (2017) La batalla del Soldado de Bronce: lecciones del primer episodio de ciberguerra con Rusia, artículo del diario El Confidencial, 2 de Octubre de 2017, disponible en https://www.elconfidencial.com/mundo/2017-10-02/batalla-estatua-estonia-ciberguerra-rusia_1451408/

McGuiness Damién,(2017) Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país, BBC News Mundo, 6 Mayo 2017, disponible en https://www.bbc.com/mundo/noticias-39800133

Maltby William, (2008) Auge y caída del Imperio español, Ed, Palmgrave y Macmillan año 2008, disponible en https://www.macmillanihe.com/page/detail/The-Rise-and-Fall-of-the-Spanish-Empire/?K=9781403917928

Makochensko Miguel, (2016) Artículo Una nueva visión de la Estrategia Militar en la concepción del General de la Federación Rusa Valery Gerasimov, publicado en Visión Conjunta, Revista de la Escuela Superior de Guerra Conjunta, Año 11 Nro. 21; , disponible en http://www.esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-75.pdf

Martinez Pontijas Juan, (2020) Control reflexivo: mucho más que desinformación a la rusa, artículo de la Revista del Instituto de Estudios Estratégicos de España Nro, 159, Madrid, Diciembre 2020, disponible en http://www.ieee.es/contenido/noticias/2020/12/DIEEEO159_2020JUAMAR_controlreflexivo.html

McFate Sean, (2019) The New Rules of War- in the Age of durable Disorder, Harper Collins Publisher, New York, disponibleenhttps://www.harpercollins.com/products/the-new-rules-of-war-sean-mcfate?variant=32116378894370

Ministerio de Defesa do Brasil, (2014) EB20-MC-10.213, Manual de Campanha, Operações De Informação, Ed 2014, disponible en https://bdex.eb.mil.br/jspui/bitstream/1/2594/1/EB20-MC-10.213.pdf

OTAN, (2009) AJP 3-10 Allied Joint Doctrine for Information Operations, disponibleenhttps://info.publicintelligence.net/OTAN-IO.pdf

Padinger Germán, (2019) artículo Qué son las "granjas de trolls" de Rusia y cómo pueden afectar en las próximas elecciones en América Latina , diario Infobae del 5 agosto 2019, disponible enhttps://www.infobae.com/america/mundo/2019/08/05/que-son-las-granjas-de-trolls-de-rusia-y-como-pueden-afectar-en-las-proximas-elecciones-en-america-latina/

Pallin, Carolina Vendil&Westerlund, Fredrik (2009). Russia's war in Georgia: lessons and consequences, Small Wars & Insurgencies, 20:2, 400-424, DOI: 10.1080/09592310902975539. Disponible en https://doi.org/10.1080/09592310902975539.

Pardo de Santayana José, (2020) El desencuentro con Rusia y las claves de su estrategia militar, Artículo publicado en el Instituto Español de Estudios Estratégicos (IEEE) Documento de Análisis edición 22/2020 del 17 de Junio del 2020, disponible en http://www.ieee.es/Galerias/fichero/docs_analisis/2020/DIEEEA22_2020JOSPAR_Rusiamilitar.pdf

Pelleriti John y otros, (2019) The Insufficiency of U.S. Irregular Warfare Doctrine, artículo publicado en Joint Force Quarterly Nr. 93, 2do quarter 2019, National Defense University Press, Washington DC, disponibleenhttps://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-93/jfq-93.pdf

Portal Infodefensa.com, (2019) Artículo El regimiento de Operaciones de Información del Ejército echa a andar, Año 2019, disponible en https://www.infodefensa.com/es/2019/07/23/noticia-regimiento-operaciones-informacion-ejercito-andar.html

República Popular China, (2020), sitio web disponible en http://ar.chineseembassy.org/esp/jrzg/t1031676.htm

Romero Sanchez Gustavo, (2020) Granjas de Trolls Rusas, artículo publicado en Crónicas de Seguridad, aparecido el 30 de septiembre de 2020, disponible en https://cronicaseguridad.com/2020/09/30/granjas-de-trolls-rusas/

Sandoval CastellanosEdgar Jair,(2011) Ingeniería Social: Corrompiendo La Mente Humana, Revista Seguridad de Información de la Universidad Nacional Autónoma de Mexico, Número 10, 4 de Mayo de 2011, disponible en https://revista.seguridad.unam.mx/numero-10/ingenierí-social-corrompiendo-la-mente-humana

Strategy and Tactics, (1986) Articulo The New Empire - America in the Spanish - American War 1898, Nro 108, disponible en http://shop.strategyandtacticspress.com/ProductDetails.asp?ProductCode=ST108

Sandalio Francisco y Arauz Manuel, (2004) Técnicas de manipulación, artículo publicado en la Revista Autogestión 1955, Octubre Noviembre de 2004, disponible en http://ilustracioncritica.com/tecnicas-de-manipulacion-m-araus-y-f-sandalio/

Trama y otros (2019), Los ciegos y el elefante, la Guerra en ambiente operacional híbrido, artículo de la revista Visión Conjunta 21, disponible en http://www.cefadigital.edu.ar/bitstream/1847939/1330/1/ESGCFFAA-revista-VisionConjunta-21.pdf

Trama G y otros,(2018)Las operaciones cibernéticas en el planeamiento y ejecución de las operaciones militares de nivel operacional, investigación de la Escuela Superior de Guerra Conjunta 2018, disponible en http://www.cefadigital.edu.ar/handle/1847939/939

US DoD (2020) Dictionary of Military and Associated Terms, disponible en https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

US Army, FM 3-0 Operations (2011), Cambio 2011 al FM 3-0 2008, Headquarters Department of the Army, February 2011, disponible en https://people.uwplatt.edu/~hood/FM3-0.pdf

US Army University Press, (2018) Perceptions are Reality, Historical Case Studies of Information Operations in large scale combat operations, Editado por Mark Vertuli y Bradley Loudon Editors, Fort Leavenworth, Kansas, Ed 2018.

US Army Social Media, Medios Sociales en el Ejército, soldados y familias, apartado Seguridad, disponible en https://www.army.mil/socialmedia/soldiers/

US Army Command Policy, (2014) AR 600-20 Army Command Policy, 6 de Noviembre de 2014, disponible en https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/r600_20.pdf

S Joint Chief of Staff, (2016) US Online and Social Media Division, Public Affairs Officer, The United States Army Social Media Handbook, Abril 2016, disponibleenhttps://carson.armymwr.com/application/files/3915/5751/4186/CRSN_ACS_Army_Social_Media_Handbook_April_2016.pdf

Univisión noticias, (2019) Ejército de EEUU prohíbe a los soldados usar la aplicación TikTok en sus celulares, suplemento noticias para militares, 31 Diciembre 2019, disponible en https://www.univision.com/noticias/estados-unidos/ejercito-de-eeuu-prohibe-a-los-soldados-usar-la-aplicacion-tiktok-en-sus-celulares

US Army War College, (2011) Information Operations Primer, disponibleenhttps://apps.dtic.mil/dtic/tr/fulltext/u2/a555809.pdf

US Joint Staff, (2014) JP 3-13 Information Operations, 27 November 2012 incorporating changes November 2014, disponibleenhttps://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

US Army (2018) ATP 3-13 Conduct of Information Operations, 2018, disponibleenhttps://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910

US Training and Doctrine Command, Asymetric Warfare Group, (2016) Russian New Generation Warfare Book, Version 1 Unclassified, Fort Meade, MD, https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf

US Department of Defense (2020), Summary of the Irregular Warfare Annex to the National Defense Strategy, disponible en https://media.defense.gov/2020/Oct/02/2002510472/-1/-1/0/Irregular-Warfare-Annex-to-the-National-Defense-Strategy-Summary.PDF

Voz of América,(2017) Redacciyn, artículo “Ucrania comienza negociación para ingresar a la OTAN”, 10 de Julio de 2017, disponible en https://www.voanoticias.com/noticias-internacional/OTAN-ucrania-petro-poroshenko-jens-stoltenberg-europa-occidente

CONFERENCIAS WEB

Walker Marció Saldanha, Coronel Ejército de Brasil, Las Operaciones de Información en el Brasil, Modo de la exposición: remoto, google meet, linkhttps://meet.google.com/oqm-gjrc-jtd?amp;authuser=1. La grabación y la transcripción del chat están disponibles en el Nivel 2, plataforma educativa virtual Conferencia "Las Operaciones de Información" CR M. Saldanha Walker (2021-06-23 at 07:31 GMT-7)