CENTRO DE ESTUDIOS ESTRATÉGICOS Y AEROESPACIALES

Artículo Nº 07/2024

REDES SOCIALES Y GUERRA HÍBRIDA, UN DESAFÍO PARA LA DEFENSA

Por René Jorquera Escobar. Director de Tecnología e Innovación.
18 de marzo de 2024. 9 Min. de lectura.

I.- Introducción.

Las redes sociales son parte de nuestra vida cotidiana y de cómo nos relacionamos con nuestro entorno. Hoy en día pasamos muchas horas conectados a diferentes redes sociales y usamos tiempo importante en revisar publicaciones, interactuar con otros y revisar contenidos digitales, llegando estas redes a ocupar parte importante de nuestro quehacer cotidiano.

Fuente : www.inesdi.com

Esta nueva realidad también, como es lógico, ha permeado a las fuerzas militares. Las redes sociales constituyen en sí mismas un fenómeno difícil de manejar, y aun cuando tienen aspectos positivos, también aportan aristas negativas que deben ser miradas con especial atención, en particular cuando estas redes no son inocuas, ya que su uso sin control ni conocimiento puede afectar la seguridad de las fuerzas y comprometer gravemente el éxito de las operaciones, tal como veremos más adelante.

II.- La Guerra Híbrida y su relación con las Redes Sociales.

Uno de los elementos que debemos entender, en este nuevo escenario de interconexión global, inmediatez, redes sociales y tecnología es el advenimiento de una nueva forma de conflicto al que los teóricos han llamado amenaza, conflicto o guerra híbrida

Fuente: www.editorialgea.com.mx

En este sentido, el concepto de guerra híbrida combina estrategias y tácticas convencionales con elementos no convencionales, como las guerras asimétricas, la cibernética, de la información y la psicológica, utilizando una combinación de medios militares y no militares para lograr el control de la opinión pública, la desestabilización de la sociedad, o el colapso de la economía del adversario.

Una parte importante de las acciones llevadas a cabo en el seno de este tipo de conflictos se centran en el empleo de medios como ciberataques, desinformación y propaganda, aprovechando para ello los nuevos espacios de confrontación que han abierto las nuevas tecnologías de comunicaciones y redes sociales, realizando así operaciones de información a través de estas últimas orientadas a influir en la opinión pública propia, adversaria o neutral.

La manipulación de los contenidos que se difunden busca debilitar la confianza de los ciudadanos en sus instituciones o de las personas en el sistema. Es interesante destacar que parte importante de estos contenidos llegaran directamente al usuario final a través de las redes sociales, sin un control o verificación previa. Por lo anterior, no es casual que Internet y las redes sociales sean uno de los frentes más importantes al hablar amenaza o guerra

híbrida, ya que las especiales características que Internet y las redes poseen hacen que puedan ser fácilmente explotadas para viralizar información maliciosa.

III.- Los riesgos de las Redes Sociales.

Es interesante señalar que la guerra de la información no es algo nuevo, tal como lo señalará el general Vladimir Slipchenko, quien en 1998 , como vicepresidente de la Academia rusa de Ciencias Militares, afirmaba que "***la información es un arma al igual que los misiles, las bombas, los torpedos, etc. Ahora queda claro que la confrontación informativa se convierte en un factor que tendrá un impacto significativo en el futuro de la guerra en su origen, curso y resultado***". En este sentido, el advenimiento de Internet como una red global de comunicaciones ha permitido que cualquier actor interesado en influir en el enfrentamiento puede realizar operaciones de información con una facilidad y efectividad asombrosas.

La guerra Rusia-Ucrania y en el conflicto de Israel con Hamas, son un ejemplo de cómo el uso de redes sociales como Facebook, X (anteriormente Twitter), Instagram, Flickr o Youtube ha permitido que los contendientes o grupos parciales a uno u otro bando puedan recopilar información sobre las acciones y sus resultados. Estas imágenes o videos son presentadas conforme a los intereses que se tengan, buscando de esta forma influir a través de actividades de propaganda y contrapropaganda. De igual manera, muchas veces la información se presenta sesgada o bien es manipulada en un evidente intento de desinformar.

Otro aspecto que es interesante hacer notar es que las organizaciones gubernamentales y también las fuerzas armadas se han integrado a esta nueva realidad que representan las redes sociales, con el propósito de utilizar su potencialidad como herramienta de comunicación estratégica, ayudando así a sus comandantes a difundir el quehacer de las Instituciones ante la ciudadanía o ante su público interno.

Por último, las Instituciones armadas han visto el potencial que estas redes tienen como fuente inagotable de datos e información que puede ser usada para producir Inteligencia útil sobre el adversario y sus operaciones. Esta característica tiene una arista negativa, y es el hecho que el propio personal también hace uso profuso de éstas, convirtiendo a las tropas propias en un blanco para las operaciones de Inteligencia del adversario, constituyendo entonces también una debilidad que amenaza la seguridad de las operaciones propias.

A.- Filtración de Información, uso inapropiado y faltas a la disciplina.

Según una estimación de las Fuerzas de Defensa de Israel, el 70% de sus generales, oficiales y suboficiales y el 95% de sus soldados disponen de perfil personal en Facebook. Para las fuerzas armadas el principal temor de que los soldados publiquen información

en sus redes sociales es que quiebren la seguridad operacional, entregando información critica que puede llegar a generar bajas.

En agosto del 2019 un misil ucraniano impacto un edificio en la ciudad de Popasna destruyendo el cuartel general del grupo Wagner en dicha ciudad y provocando un número indeterminado de bajas. La ubicación del cuartel general fue identificada a partir de las fotografías que los soldados de Wagner subieron a sus redes sociales.

En el año 2010, se debió cancelar una operación militar luego que un soldado israelí publicó en su cuenta de Facebook el mensaje: "Limpiaremos Katana y el jueves volveremos a casa"; haciendo referencia a una operación militar a realizar en un pequeño pueblo cercano a Ramala (Cisjordania). También se ha dado el caso que muchos soldados israelíes han compartido fotografías en situaciones inapropiadas, por ejemplo posando con prisioneros palestinos o en ropa interior, lo que ha motivado a los mandos militares israelíes a aprobar un estricto código de conducta sobre el uso de las redes sociales en el que se contemplan importantes sanciones, incluidas penas de cárcel, en caso de incumplimiento.

La red social de mensajería WhatsApp también genera problemas. En el año 2013, doce oficiales de la Fuerza Aérea de Israel fueron condenados por compartir información clasificada como planos y coordenadas de vuelo, a través de la citada aplicación. Recientemente, durante la Operación Margen Protector, varios miembros de las FDI fueron detenidos tras difundir a través de la misma plataforma fotografías de varios soldados israelíes caídos en combate durante la incursión terrestre en Gaza. También en 2013, el soldado Mor Ostrovski fue arrestado tras compartir en su cuenta de Instagram una fotografía en la que se podía ver a un joven palestino en el punto de mira de su fusil.

Esta redes e Internet también están siendo utilizadas como medio de protesta. Por ejemplo, en una campaña realizada a través de Facebook de apoyo a un soldado israelí arrestado tras ser grabado mientras apuntaba con su arma a dos adolescentes palestinos en Cisjordania consiguió más de 120.000 "Me gusta", generando así una presión indebida sobre los mandos militares y sus decisiones disciplinarias.

Del mismo modo, durante la escalada militar en Ucrania, el inadecuado uso de las redes sociales por parte de soldados rusos comprometió la versión oficial de Moscú sobre su no implicación en el conflicto. En este sentido, las fotografías compartidas por un soldado ruso en su cuenta de Instagram lo geolocalizaban dentro de las fronteras ucranianas, colocando así en entredicho la información entregada por el Kremlin.

Al respecto, el Departamento de Defensa estadounidense se ha mostrado preocupado por el uso inapropiado de estas redes por parte de sus tropas durante las pasadas guerras de Irak y Afganistán. Laa publicación de una fotografía de catorce soldados estadounidenses

en posición poco respetuosa ante un ataúd - que según fuentes oficiales estaba vacío - cubierto con la bandera estadounidense generó controversias en Washington, dañando innecesariamente la imagen de las fuerzas armadas norteamericanas.

B.- Desinformación, engaño y manipulación de masas.

En el año 2019, miembros del Centro de Excelencia de Comunicaciones Estratégicas de la NATO realizaron una investigación de campo durante un ejercicio militar de dicha alianza militar. Usando redes sociales fueron capaces de identificar a participantes y engañarlos para que se unieran a un grupo de Facebook falso que simulaba ser parte de la organización del ejercicio. A partir de esto identificaron a soldados, precisaron la localización de tropas y accedieron a fotografías de equipos militares. Sin embargo, lo mas preocupante de esta investigación es que algunos soldados fueron persuadidos a abandonar sus posiciones y a no cumplir con sus deberes.

Internet, como ya se ha dicho, es un frente más de batalla, que hoy se ha transformado en una herramienta clave para la desestabilización del adversario. Timothy Snyder señala en su libro *El camino hacia la no libertad*, "***El elemento más importante de la invasión rusa de Ucrania en 2014 fue la guerra informativa concebida para desautorizar la realidad*".** En otras palabras, manipular a la opinión pública, dejando dudas respecto de que es verdad y que no lo es, mezclando de esta forma la confrontación regular tal como la conocemos con maniobras de desinformación perfectamente planificadas y coordinadas.

En este sentido, la desinformación tiene como objetivo desestabilizar sociedades, fomentar la polarización y el malestar, exacerbando de esta forma el conflicto interno. Su capacidad de penetrar en los debates públicos, de confundir o erosionar, por ejemplo, la confianza en instituciones o procesos electorales aprovecha muchas veces de divisiones socioculturales ya existentes; apunta hacia vulnerabilidades previas y hacia ciertos grupos supuestamente inclinados a confiar en dichas fuentes o narrativas, que pueden contribuir voluntaria o involuntariamente a su difusión. Los abusos de poder, los sistemas políticos disfuncionales, las desigualdades y la exclusión son caldos de cultivo para esta táctica.

Tal como lo vemos, el uso de la desinformación, un arma que nace para ser empleada en el conflicto contra un adversario militar en tiempos de guerra, es hoy por hoy también parte importante de esta amenaza híbrida, aprovechando las particularidades que ofrece la tecnología actual, lo que ha venido a potenciar y reverdecer esta antigua táctica, al permitirle una viralización y penetración nunca antes vista.

Esta manipulación que puede sufrir la sociedad civil a través de la información también se manifestará en las tropas, ya que estas conforman un subgrupo dentro de esta sociedad,

con similares características y cualidades, algo que debe ser tenido en consideración por los comandantes.

C.- Radicalización y polarización de individuos.

Uno de los inconvenientes que presentan las redes sociales tiene que ver con el hecho que estas son controladas por algoritmos e Inteligencia Artificial capaces de monitorear nuestras interacciones, y a partir de estas predecir nuestros gustos e intereses, entregándonos siempre contenidos afines con nuestro perfil de usuario, esto es algo que muchos no saben, por lo cual difícilmente se cuestionaran por qué siempre acceden a un cierto tipo de contenido.

Esta particularidad de los algoritmos nos hace vulnerables a dos efectos que se pueden producir debido a la exposición continua de un tipo de mensaje, más aún si este ha sido manipulado, pudiéndose exacerbar nuestra postura ante un tema en particular, corriéndose el riesgo, por una parte, de radicalización de nuestras posturas, y, por otra parte, polarizar a una comunidad frente a un tema.

La radicalización es en extremo peligrosa ya que hace que algunas personas sean más propensas a apoyar posturas ideológicas extremas, como el terrorismo, actos violentos de extremismo e incluso estén dispuestos a cometer actos violentos.

Hoy sabemos que los algoritmos pueden ser explotados por empresas u organizaciones, como hizo Cambridge Analytica, creando perfiles de las personas, considerando por ejemplo su sexo, orientación sexual, creencias religiosas o rasgos de personalidad, información con la cual se dirigió mensajes específicos a un grupo objetivo de usuarios con el fin de intentar influir en los resultados de una elección política. Esta misma forma de operar, con mensajes y contenidos especiales, podría intentar radicalizar o polarizar a una población objetivo respecto de temas religiosos, políticos, medioambientales, etc.

IV.- Como proteger a las tropas.

Como se ve, las redes sociales tienen amenazas que pueden afectar al personal militar, tanto en tiempo de paz como de conflicto, pudiendo verse este personal afectado tanto por contenidos manipulados como también por la acción de la Inteligencia adversaria que hurga en sus publicaciones en busca de información, por ello debemos preguntarnos que se puede hacer para evitar los efectos nocivos de la exposición a estas redes.

Como el fenómeno de la fuga de información no es algo nuevo muchas Fuerzas Armadas han adoptado políticas para controlar el uso de teléfonos móviles cuando su personal se encuentra desplegados en operaciones, sin embargo, esto no siempre es efectivo. Prueba de lo anterior es que el parlamento ruso votó, en el año 2019, prohibir al personal militar

desplegarse con teléfonos móviles, algo que conforme se vio en la invasión Ucrania en el 2022, no se cumplió, lo que es un indicio de que este tipo de medidas pueden no ser efectivas.

Además de este incumplimiento de la norma, por lo difícil que es de controlar, se ha presentado otro fenómeno que no había sido previsto. Hoy es difícil mantener a las tripulaciones jóvenes lejos de las redes sociales e Internet, tanto es así que para la Royal Navy está siendo muy difícil reclutar submarinistas para sus sumergibles nucleares debido al deseo del personal de tener acceso permanente a las redes sociales, algo que no es posible por las restricciones de comunicaciones que deben cumplir estos navíos durante los largos periodos de patrulla.

Al respecto, quienes han estudiado estos fenómenos señalan que la educación y la sensibilización respecto de los riesgos que implican las redes sociales pueden ser la mejor manera de mitigar estas vulnerabilidades. Por ello, el personal militar no debe ser un usuario acrítico de las redes sociales, sino que debe tener una noción clara de cómo y por qué les llegan determinados contenidos; por qué se le recomiendan determinados videos o tipos de noticias, como también saber que existen canales o medios creadores de contenido que actúan con evidente sesgo respecto de los temas que difunden.

En este sentido, el pensamiento crítico es fundamental, es algo que se debe fomentar para combatir esta amenaza ya que siempre será bueno cuestionarse el origen y la intención de un contenido o noticia, aun cuando ésta se alineé con nuestras preferencias ideológicas.

La clave para saber filtrar los contenidos que se consumen es las redes sociales es mejorar la alfabetización mediática y digital de los soldados. Esta alfabetización mediática y digital se define como un concepto que engloba todas las capacidades técnicas, cognitivas, sociales, cívicas, éticas y creativas que permiten a una persona acceder a información y medios de comunicación y utilizarlos de manera eficaz.

Otro aspecto a tener en cuenta es conocer cómo funcionan los canales digitales y la viralidad que estos canales en sí mismos poseen. Entender que estos espacios son utilizados para la difusión de fake news debido a la capacidad que tienen para difundir mensajes que lleguen a mucha gente, con rapidez. Si se entiende esta característica y capacidad se puede entender que no todo lo que aparece en las redes sociales es verdad o bien que aquello que se publica puede estar alterado o sacado de contexto.

De igual forma, otro elemento a considerar es la dificultad para determinar la autoría de los contenidos, esta particularidad debe poner en guardia al receptor para desconfiar de aquella información que encuentren sin una fuente de origen claramente identificable o confiable. Un punto que puede ayudar a identificar fuentes de fake news es recurrir a fact checkers o verificadores.

Por último, también a considerar es el hecho que solo comprendiendo que es la desinformación se puede hacer frente a ella. Solo entendiendo que la desinformación es

parte de una estrategia, que puede ser parte de una maniobra enmarcada en la guerra hibrida, entonces se puede entender que estas acciones buscan alimentar la desconfianza frente al sistema o frente a su organización, haciéndole creer que todo es mentira y que debe rebelarse.

IV.- Conclusión.

Las redes sociales innegablemente presentan muchas ventajas, pero tal como vemos, estos canales de comunicación pueden ser empleados con fines militares diversos, cuyos objetivos pueden ser muy heterogéneos, como la obtención de información para producir Inteligencia, generar confusión, desprestigiar a personas, organizaciones o medios, engaño, manipulación de la opinión pública o la instalación de una post verdad. Su uso, debido a los algoritmos que manejan la interacción de las personas con estas redes, puede ser un caldo de cultivo para radicalizar a las personas o bien a polarizar a la población respecto de temas políticos o de interés de la comunidad.

Estas redes sociales e Internet forman parte de un nuevo escenario del conflicto, que puede ser explotado tanto en tiempo de paz o de guerra, y que será utilizado en forma coordinada con otros medios, físicos y no tradicionales, en un contexto de amenaza o guerra híbrido. En este escenario, las redes sociales y la información que por ellas fluye son un arma, al igual que un misil o una bomba, y su empleo formará parte de una estrategia.

Ante estas vulnerabilidades, la educación de las personas, el conocimiento respecto como operan estas redes y los algoritmos que están detrás de ellas, como también el fomento del pensamiento crítico y el reforzamiento de la doctrina de seguridad, son hoy por hoy, las mejores herramientas que podemos encontrar para enfrentar esta nueva amenaza ya que desconectar a las personas de las redes sociales o prohibir completamente el uso de estas parece no haber sido la solución, sólo una educación y doctrina sólida parecen, hoy en día, ser el camino.

Fuentes:

1.- Soldiers and Social Media in teh Age of Connectivity Saturation, Major Patrick Hintorn, RUSI
2.- Las Redes Sociales y sus riesgos para las Fuerzas Armadas, Enrique Fojón Chamorro y Guillem Collon Piella.
3.- Ciberseguridad y Guerra Hibrida: LA ampliación del espectro, Sara Hernandez Calabrés, Universidad de Navarra.
4.- Guía: Cómo preparar a los ciudadanso para la guerra híbrida, Iván Gímenez Chueca,
5.- Guerras Híbridas Reto de las Fuerzas Armadas Mexicanas, Julio A. Millán Bojalil , *www.editorialgea.com.mx*
6.- Radicalización en redes sociales, LISA INSTITUTE, www.Lisainstitute.com