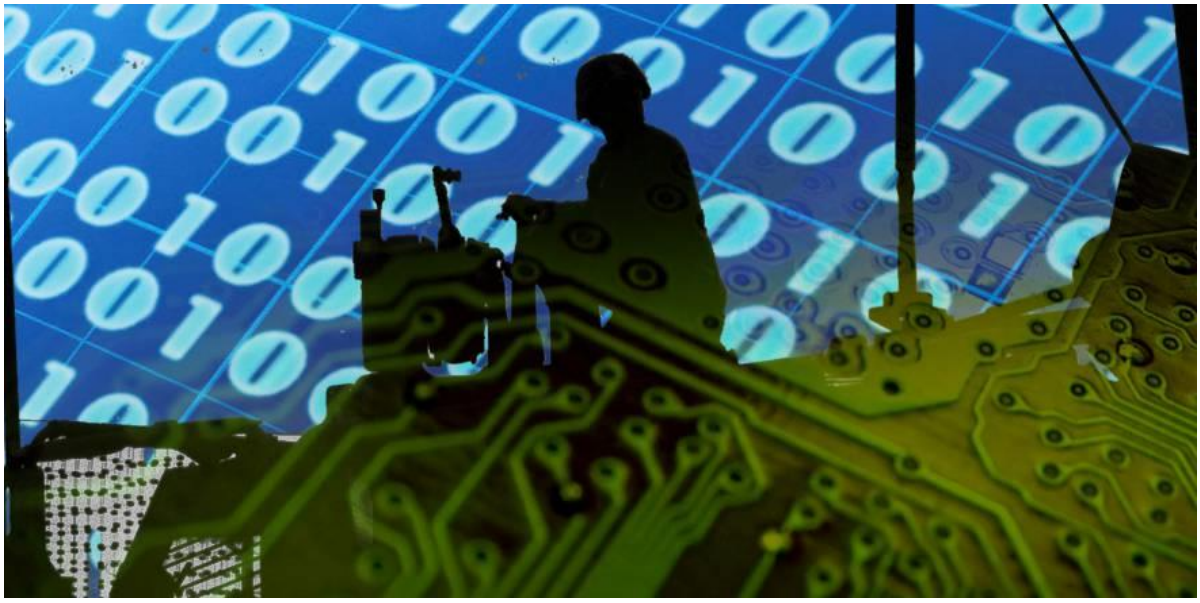
Las operaciones en el ciberespacio



Jesús Argumosa Pila
General de División (retirado) del Ejército de Tierra
Sección Futuro de las Operaciones Militares
Academia de las Ciencias y las Artes Militares

Siempre se ha dicho que los Estados preparaban sus Fuerzas Armadas para las guerras del pasado y cuando se enfrentaban a una próxima guerra sus doctrinas, medios y procedimientos de combate se encontraban obsoletos por lo que el resultado de la siguiente guerra se presentaba muy incierta e imprevisible.

En una síntesis histórica del concepto clásico de guerra se pueden considerar como rasgos consustanciales de dicho acontecimiento el acto de fuerza, la imposición de la propia voluntad al enemigo, el desarme consiguiente del adversario, la lucha armada y sangrienta y que sea entre agrupaciones organizadas.

Sin embargo, en las últimas guerras ocurridas a caballo entre el siglo XX y el siglo XXI, ya no se han respetado o cumplimentado algunos de los atributos que acabamos de mencionar. Es decir, se está cambiando o reorientando la naturaleza intrínseca de la guerra por otras condiciones o aspectos propios de diferentes estrategias, operaciones y tácticas del nuevo campo de batalla.

En concreto, podemos asumir que estamos entrando en una nueva era en la que el término guerra está adquiriendo una dimensión distinta de la existente hace apenas medio siglo: guerra sin restricciones, guerra irregular, guerra insurgente, guerra compuesta, guerra híbrida o guerra no lineal son algunos de los tipos de guerra que se han sucedido en los últimos 50 años, lo que indica la dificultad de identificar claramente a las denominadas "guerras modernas" o, incluso "guerras postmodernas".

En realidad, las operaciones reales en el ciberespacio tienen ya un largo recorrido. Para no irnos muy atrás en el tiempo y a modo de ejemplo podemos citar los ciberataques contra objetivos de la red de administración de Estonia en el año 2010 o el ataque a las instalaciones nucleares de Irán mediante el virus Stuxnet que tomó el control de 1.000 centrifugadoras que participaban en la producción de materiales y les dio instrucciones para autodestruirse.

Mucho más reciente han sido los ciberataques durante la última campaña electoral de los Estados Unidos, en 2016, atribuidas a actores rusos o las sombras de otros ciberataques durante la carrera presidencial francesa, en 2017.

Quizás el más relevante haya sido el ocurrido en mayo de 2017 cuando se difundió por todo el planeta el virus WannaCry que permite el secuestro de datos de un sistema. El Reino Unido aún está acabando de reponer los desperfectos que dicho ciberataque causó en su red de hospitales. Los atacantes para devolver los datos retenidos pidieron un rescate en bitcoins, moneda virtual de imposible rastreo.

En la cumbre de la OTAN de 2016, en Varsovia, se reconoció al ciberespacio como un nuevo dominio de operaciones, al lado del espacio terrestre, del espacio marítimo, el espacio aéreo y el espacio exterior y la Alianza se comprometió a mejorar la ciberdefensa de sus redes e infraestructuras como un asunto prioritario.

La estrategia y la orientación de la OTAN también se están adaptando. En junio de 2018, los Aliados aprobaron la Visión y la Estrategia en el ciberespacio como dominio de operaciones. Se comprometieron a completar, en 2019, la primera doctrina de operaciones del ciberespacio en la Alianza, sujeta a la aprobación de los aliados, que proporcionaría orientación a los comandantes de la OTAN. Hasta donde yo conozco, aún no se ha publicado.

Llegados a este punto, es preciso definir lo que entendemos por ciberespacio. A nuestros efectos, ciberespacio es un dominio global formado por los sistemas de Tecnologías de Información y de Comunicación (TIC) y otros sistemas electrónicos, su interacción y la información que es almacenada, procesada o transmitida por estos sistemas. También podemos considerarlo como una realidad virtual.

Así pues, el dominio del ciberespacio es el nuevo campo de batalla cuyas características más importantes son un entorno virtual sin límites geográficos, de escasa seguridad, en el que se desarrollan actividades vitales para la sociedad y en donde aparece la delincuencia, el terrorismo y el espionaje junto con conflictos armados y en el cual actúan actores anónimos en un marco bélico no sujeto a ninguna legalidad.

En una primera aproximación una operación militar en el ciberespacio es una operación en la que se emplean capacidades "ciber" con la misión principal de alcanzar objetivos estratégicos militares en el marco de un teatro de la guerra situado en el ciberespacio.

Por otra parte, se considera que el ciberataque es una acción agresiva originada en el ciberespacio en la que se producen daños a personas u objetos con unos efectos perjudiciales sobre los sistemas de información que afectan a la confidencialidad, integridad o disponibilidad de la información contenida en ellos.

A mayor abundamiento, los ciberataques pueden afectar a infraestructuras críticas que producen graves daños si se piensa en el sistema eléctrico nacional, el sistema energético, el sistema de control aéreo, el sistema sanitario o una central nuclear. En concreto, puede bloquear e inutilizar los servicios básicos de un país.

Los ciberataques en el ciberespacio están integrados en el marco de operaciones de una campaña que se está desarrollando a nivel táctico, operacional y estratégico en cualquiera de los otros cuatro dominios - señalados más arriba - donde se puede llevar a cabo la guerra. Actualmente, aún no existen tratados específicos sobre el ciberespacio.

En cuanto al origen de los riesgos y amenazas que se pueden presentar en el ciberespacio, en general, proceden de una variedad de actores como pueden ser los Estados -que son los más peligrosos-; actores transnacionales formales o informales; organizaciones criminales no sujetas a fronteras; entidades virtuales o no del salafismo yihadista junto con individuos o pequeños grupos que pueden prestar servicio o no al resto de actores u organizaciones.

Clausewitz, en su obra *De la Guerra*, al tratar la naturaleza de la guerra afirmaba que *la guerra es un acto de fuerza para obligar al contrario al cumplimiento de nuestra voluntad*. La fuerza, es decir, la fuerza física -continuaba el autor prusiano– es el *medio*, someter al enemigo a nuestra voluntad es el *fin*.

Pero el concepto de fuerza como medio de hace apenas dos siglos era distinto del actual. En el siglo XIX la fuerza se relacionaba muy directamente con la potencia militar materializada habitualmente en las armas de fuego. Hoy en día, el espectro de la fuerza es mucho más amplio y sutil. Así, al hablar de fuerza hoy tratamos la milicia, la tecnología, la economía, la industria, la cibernética en particular, la energía o los recursos en general.

Por ejemplo, ¿cómo se debe considerar a un ciberataque -un nivel de fricción superior a la ciberamenaza- que esté por debajo del umbral de un conflicto armado? No es un acto de fuerza de carácter tradicional pero si es una ciberactividad ilícita a la que debemos hacer frente. Nuestra respuesta debe ser la de emplear todas nuestras capacidades, incluyendo la cibercapacidad, para disuadir, defender y contrarrestar todo el espectro de las ciberamenazas, incluyendo aquéllas de campañas hibridas.

Y en cuanto al fin, también las concepciones han cambiado. Hace poco más de medio siglo todavía dentro del fin se incluía la destrucción del enemigo y su sometimiento a nuestra

voluntad. Hoy no es así, no necesitamos someter al enemigo en términos absolutos, se estima suficiente tenerle bajo nuestra influencia y que cumpla con los principales criterios políticos, económicos o de gobernanza establecidos por los vencedores.

En virtud de lo expuesto en estas reflexiones podemos considerar como conclusiones más relevantes las relacionadas a continuación. En primer lugar, el nivel de operaciones militares en el ciberespacio inferior al umbral del conflicto armado constituye una cuestión a dilucidar en el marco de la nueva naturaleza de la guerra. En segundo lugar, dada la preeminencia del ciberespacio en la guerra moderna es imperativo ser tan capaz de operar en este dominio como en el de los otros cuatro precedentes. En tercer lugar, las operaciones en el ciberespacio no son necesariamente militares y no únicamente se las debe hacer frente con medios militares. Por último, resulta imprescindible tanto el detectar lo más rápidamente posible cualquier ciberataque como establecer las reglas adecuadas en este dominio.

Como epílogo, las operaciones militares en el ciberespacio que, en general, estarán enmarcadas en el desarrollo global de las operaciones de una campaña, constituyen un desafío prioritario a superar especialmente condicionadas por el desconocimiento e incertidumbre que puede deparar la entrada del propio dominio del ciberespacio en la guerra del futuro.