



## **Los desafíos del Derecho Internacional Humanitario y las Guerras de Información y Cibernética**

Por. Dr. C. Leonel Gorrín Mérida. Prof. Titular

En medio de la revolución que vive el mundo en el terreno de la informática y las comunicaciones era de esperar que estas áreas se convirtieran en esferas de confrontación, no solo en tiempo de guerra, sino también en la paz. En la historia de la humanidad, prácticamente todos los adelantos conquistados por las ciencias y las tecnologías no solo han estado en función del progreso, sino que se le ha dado un amplio uso para el logro de objetivos políticos por vías violentas. Los descubrimientos en el campo de la energía nuclear, cuyo positivo uso con fines pacíficos son indiscutibles, terminaron con la construcción de miles de ojivas nucleares que pueden destruir más de cien veces todo lo existente sobre el planeta.

Así ha sucedido con la informática y las comunicaciones y es en ese marco en el que ha aparecido el concepto de “Guerra Cibernética”. Por ella se entiende el propósito de dominar el espectro informativo y sus soportes físicos en función de intereses políticos, económicos, financieros, militares. Es una guerra por el dominio de la información, de los sistemas y las infraestructuras que la sustentan. Ella comprende la capacidad para neutralizar, destruir, degradar, interrumpir las redes interdependientes de transmisión de información, los procesadores de información y de su transmisión y control, incluyendo los sistemas satelitales y por supuesto controlar la información y su percepción por parte de los diferentes destinatarios. La Guerra Cibernética abarca, por lo tanto, tres ámbitos muy bien definidos: 1.- la información en sí misma; 2.- los sistemas que le sirven de soporte; 3.- la percepción y asimilación de la información.

Mucho se ha hablado acerca de la inconsistencia legal de la guerra cibernética. Una primera hojeada a los documentos existentes dentro del Derecho Internacional nos puede conducir a la apreciación que no hay nada estipulado que la prohíba ni en tiempo de paz ni de guerra. Incluso, un documento reciente del Departamento de Defensa de Estados Unidos, denominado Manual de Derecho de la Guerra subraya – en un capítulo dedicado por completo a esta temática – que tal derecho puede ser aplicado a las operaciones cibernéticas, las que “de facto son plenamente legales”.

En el documento del Departamento de Defensa de Estados Unidos conocido por las siglas JP 3-12 “CyberspaceOperation”, de fecha febrero de 2013, se afirma que el ciberespacio y las tecnologías que le están asociadas le brindan a esa nación (Estados Unidos) “oportunidades sin precedentes” para alcanzar los objetivos deseados en el terreno internacional. Obsérvese que estamos hablando de un documento que supuestamente está destinado a precisar aspectos de la planificación, ejecución y control de operaciones en el contexto directo de las acciones militares, es decir en los conflictos armados. Sin embargo, la interpretación que se deduce de lo calificado como “oportunidades sin precedentes para alcanzar objetivos deseados” va mucho más allá de la violencia armada propiamente dicha.

Artículos comunes a los cuatro Convenios de Ginebra señala el ámbito material de aplicabilidad del Derecho Internacional Humanitario en términos que hasta hace unos años resultaban claros y bien definidos. Así señala que su aplicabilidad está limitada a las situaciones de “guerra declarada o cualquier otro conflicto armado”. Pero dichos Convenios no precisan el concepto de “conflicto armado”. Tampoco lo hacen los Protocolos Adicionales. Solo existen acercamientos doctrinales, siendo la más notable aquella que los define como “hostilidades abiertas” entre fuerzas o grupos armados dotados de cierta organización.

Los conflictos armados han experimentado grandes evoluciones a lo largo de la historia de la humanidad. Como regla el Derecho Internacional ha ido a posteriori de esos cambios. Los cambios en los métodos y medios de hacer la guerra han seguido sin cesar y no siempre los conceptos del Derecho se precisan con similar velocidad. ¿Cómo comprender la aplicabilidad del Derecho ante tales cambios? ¿Cómo hacerlo frente a la Guerra Cibernética? ¿Qué debemos esperar para considerar la existencia de los tradicionales ámbitos de aplicabilidad?

La Primera Guerra Mundial tuvo como elemento principal el desarrollo de nuevos tipos de tácticas y sistemas estratégicos desconocidos, hasta ese momento. Se desarrolló la llamada guerra de trincheras y de desgastes. Las tropas enfrentadas podían verse las caras desde esas obras ingenieras situadas a pocos metros una de la otra. En reducidos espacios se concentraban numerosas cifras de combatientes, mientras que la población civil se mantenía alejada de un teatro de operaciones bien definido. Un ejemplo de este tipo de táctica fue la conocida línea Maginot, construida por Francia a lo largo de la mayor parte de su frontera oriental con Alemania. El transporte militar estaba aún en una fase inicial de su surgimiento, que alcanzó en unos años un vertiginoso desarrollo.

Previo a la Segunda Guerra Mundial surgió una nueva táctica, la Blitzkrieg, que al utilizar los progresos en el campo de las transportaciones militares, introduce el concepto de la movilidad. Entre la Primera y la Segunda confrontaciones mundiales los vehículos blindados se utilizaban como apoyo a la infantería. Ahora sería la infantería la que debía apoyar a los tanques. Aparecieron unidades constituidas básicamente por tanques y otras por aviones. La batalla de Kurts, en la que se enfrentaron miles de tanques soviéticos y alemanes fue un ejemplo

clásico de esos nuevos conceptos de lucha armada, que no cambiaron las tres dimensiones esenciales de la guerra: el espacio (el teatro de operaciones), el tiempo real en que se desarrollaban los enfrentamientos y los principales actores.

En la actualidad hay varias dimensiones de la guerra que requieren de puntualizaciones. Uno de ellos es la dimensión espacial. Hoy no puede hablarse del “teatro de operaciones” en el sentido que tradicionalmente se le comprendía. Esa dimensión se ha globalizado. La otra dimensión que ha sufrido cambios es la del tiempo. El criterio conservado hasta el presente que un conflicto armado es un criterio “material” en el cual dos o más partes se enfrentan mediante la lucha armada, está siendo cuestionado. Hay acciones de la “guerra cibernética” tomadas desde la paz, que se hacen para que detonen durante un enfrentamiento armado. Esas acciones pueden causar daños en el componente militar del enemigo, pero también pueden afectar a la población civil, con consecuencias excesivamente dañinas.

La guerra, desde la época de Karl von Clausewitz, se ha definido con la continuación de la política por métodos violentos. Pero la propia definición de “violencia” requiere de precisiones a la luz de los actuales acontecimientos. El criterio de “materialidad”, en el sentido físico de su existencia, que se ha seguido hasta hoy para definir la “violencia”, está sujeto a variadas interpretaciones. Los diccionarios de la lengua española la definen como aquellos actos dirigidos a modificar bruscamente el estado natural de las cosas, la dinámica normal de los procesos. Y tales modificaciones se logran no solo mediante la violencia “física” de los conflictos armados.

La discusión en torno a la relación violencia-aplicación del DIH, gira hoy alrededor de su carácter, es decir si es aislado, esporádico o si es sostenido, concertado. Esta interpretación del término conduce a la conclusión que cuando los actos de violencia son aislados o esporádicos se aplican los ordenamientos jurídicos internos de las naciones y las convenciones internacionales referidas a los derechos humanos. En tales casos no hay aplicabilidad del DIH y lo más que puede considerarse es la aplicación del artículo 3 común a los cuatro Convenios de Ginebra de 1949, que establece normas mínimas de carácter humanitario. Tal enfoque no chocaba con el propio desarrollo de la violencia y de los conflictos armados hasta hace uno o dos decenios atrás. Hoy los acontecimientos se desarrollan bajo dinámicas totalmente diferentes, donde es difícil establecer fronteras precisas de cuando esas “violencias” son “aisladas” y “esporádicas” o cuando alcanzan un grado determinado de “generalización” o se define un conflicto armado.

Por otra parte, la violencia no es solo “física”. Hay también una violencia “psicológica”, una actuación (casi siempre sostenida y concertada) de modificar bruscamente la conducta de los hombres, aún en contra de su propia voluntad. El terror se alcanza no solo por medios físicos, sino (y hasta fundamentalmente) por medios psicológicos. Es en este sentido en el que hay que considerar la guerra

cibernética y muy concretamente la que se despliega en el campo de la información.

Últimamente se ha hablado mucho sobre la Guerra No Convencional. Dentro de las etapas que conforman tal tipo de “guerra”, según los propios conceptos norteamericanos, no hay siempre violencia física, pero si existe una “violencia” psicológica preparando el teatro para la “física”. El documento de las Fuerzas Especiales de Estados Unidos del 2010, conocido por las siglas TC-18-1, y sus posteriores actualizaciones, es una clara violación del Derecho Internacional, por cuanto, como define su propia letra: son acciones dirigidas a posibilitar los movimientos de resistencia o de insurgencia para forzar, afectar o derrocar gobierno o habilitar poderes para operar a través o con fuerzas clandestinas, auxiliares y guerrilleras en un área denegada. El citado texto, de carácter doctrinario, subraya que el efecto combinado de los movimientos armados de resistencia y los elementos clandestinos genera como resultado final una campaña de guerra no convencional y tales esfuerzos son: el conflicto armado y la subversión.

Más adelante el TC-18-1 revela la comprensión que tiene Estados Unidos en cuanto al propio término de “conflicto armado”, al considerar explícitamente que este “incluye tanto las operaciones de ataque como las que desgastan la moral del enemigo, su cohesión organizativa y la eficacia de sus operaciones y separan al enemigo de la población”. Obsérvese, como para el mando militar estadounidense el conflicto armado no se circunscribe al factor físico de la lucha armada.

La guerra cibernética, la guerra no convencional, la guerra psicológica, las operaciones de información, los postulados revelados en el Manual de Derecho de la Guerra de las Fuerzas Armadas norteamericanas, constituyen elementos de una misma concepción. No pueden verse como cuestiones aisladas.

Estas consideraciones preliminares nos conducen a una interpretación más amplia acerca de la aplicabilidad del Derecho Internacional Humanitario ante las nuevas características que presenta la guerra como medio para alcanzar determinados objetivos políticos. Su aplicación, en el caso de la guerra cibernética, no puede esperarse al estallido de una violencia física de cierta magnitud, por el simple hecho que tal tipo de guerra no es solo “física”, ni notablemente “violenta”.

La acción de destruir, neutralizar o degradar los sistemas informativos no puede ser considerada, de por sí, contraria a toda norma del Derecho Internacional y más concretamente a lo establecido por el Derecho Internacional Humanitario. Es lícito la destrucción de los sistemas de mando de las tropas enemigas durante el desarrollo de las acciones militares. Sin embargo, no es lícito cuando se ataca por medios cibernéticos estructuras que garantizan la subsistencia de la población civil, como puede ser el caso del sector de la economía. Tampoco es lícito el empleo de ese tipo de guerra para la actividad de espionaje. Destruir la infraestructura de un país mediante la guerra cibernética puede ser considerada como un acto de agresión y por tanto tal acción es contraria al Derecho.

Hay dentro de este fenómeno un campo con escaso reflejo en los ordenamientos jurídicos internacionales. Nos referimos a la manipulación de la información y las posibilidades que presenta la guerra cibernética de bloquear ciertos medios en función de otros y degradar contenidos informativos en función de los intereses de los principales actores de esta guerra. La manipulación informativa y la guerra cibernética van de la mano, preparan la opinión pública para los conflictos armados, crean el terror y la desinformación.

Resulta importante subrayar la diferencia relativa existente entre el concepto de "guerra cibernética" y el de operaciones cibernéticas, donde el primero es mucho más amplio y este último debiera limitarse a las acciones contra los soportes tecnológicos de la información en las situaciones concretas de los conflictos armados. El primer término engloba a las operaciones de información y a las variadas acciones que en el espectro cibernético se llevan a cabo en tiempo de paz. Sin embargo, la guerra, es decir el conflicto armado, puede desarrollarse en determinado teatro de operaciones y los públicos que se requieren afectar en función de esos conflictos estar diseminados en los más diversos confines del planeta. ¿Cómo proceder en tales casos respecto a la aplicabilidad del Derecho? En un lugar se está bajo la influencia directa de la violencia física, en otros tal influencia no existe, pero si se choca con otra no menor peligrosa. ¿Puede definirse la aplicabilidad a partir de los lugares concretos en los que se desarrollan los acontecimientos o debe tomarse como criterio la esencia misma de los objetivos que se persiguen en función de esos conflictos armados y el carácter de las víctimas?

¿Qué criterios sustenta el Departamento de Defensa para justificar el carácter legal de la guerra cibernética? Sencillamente plantean un hecho real: Las normas existentes dentro del Derecho no dependen del tipo de arma que se utiliza para llevar a cabo un ataque, sino de su alcance (principio de limitación) y sus efectos (principio de distinción). El propio manual de Derecho de la Guerra del Departamento de Defensa norteamericano subraya que todo lo estipulado en materia de ese Derecho no se opone al empleo de los avances de la ciencia y la tecnología en los conflictos armados por el contrario: "anticipa afirmativamente la innovación tecnológica" en función de la guerra y "establece las normas en cuanto a su alcance y efectos".

Resulta importante recordar la letra del artículo 2(4) de la Carta de las Naciones Unidas que establece que: "Todos los miembros se abstendrán, en sus relaciones internacionales de la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas". La guerra cibernética en su comprensión más amplia, es decir, no solo la limitada a las acciones en tiempo de guerra y dentro de un teatro de operaciones definido, es contraria a esa norma del Derecho Internacional.

Mediante la “guerra cibernética” se puede desencadenar una crisis en plantas nucleares, destruir los muros de contención de embalses de agua e inundar pueblos enteros en cuestión de minutos, desactivar los controles del tráfico aéreo, paralizar procesos productivos, explotar oleoductos, etc. Sería interminable la lista de efectos dañinos sobre la población y los bienes civiles. Para lograr tales daños mediante los medios tradicionales se requeriría de grandes movimientos de fuerzas. Mediante la guerra cibernética un operador de sistemas logra los objetivos desde miles de kilómetros de distancia. Todo eso es contrario al derecho.

En el JP- 3-12 se enfatiza que en las condiciones de los conflictos armados la guerra cibernética es legal por naturaleza propia. Consideramos que tal enfoque es erróneo, incluso a partir de las propias justificaciones que expone el mando militar estadounidense en sus documentos doctrinales. El empleo de los tanques en una guerra puede ser contrario a toda norma del Derecho si estos van encaminado a destruir los bienes civiles y causar muertes dentro de la población civil. La legalidad en caso de guerra está dado por el cumplimiento de su empleo con objetivos claramente militares. Si los instrumentos de tráfico aéreo que le pueden dar cobertura a la aviación del enemigo desde bases militares, pueden ser afectados mediante vías cibernéticas, estamos en presencia de una acción legal, en cuanto es lícito en una guerra neutralizar o poner fuera de combate al enemigo armado.

Pero si esa acción afecta la aviación civil y pone en peligro a personas inocentes, hay una evidente ilegalidad a la luz de las más elementales normas del Derecho Internacional y del Derecho Internacional Humanitario y en tales casos la guerra cibernética es ilegal. En este contexto, lo que se discute es hasta qué punto las acciones que se toman en una dirección no pueden tener incidencias notables en las otras. El espectro cibernético es muy amplio y en él se interconectan los más diversos sistemas. Es por ello que es válido poner en duda la legalidad de la guerra cibernética, por cuanto se conoce de antemano sus llamados efectos “colaterales”, que en esencia no son tan “colaterales”.

La ciber-guerra no tiene un teatro de operaciones definido. Tampoco está limitado por la dimensión del tiempo. Todo el mundo está bajo su influencia y lo está todo el tiempo. En sentido general la guerra en el campo de la cibernética no conoce amigos, aliados o enemigos. Las recientes denuncias de los gobiernos de Francia, Alemania, para solo citar a dos países demuestran la veracidad de lo anteriormente dicho.

Pero en este tipo de guerra no todo el mundo está expuesto a los mismos peligros. Tampoco todo el mundo tiene la misma capacidad de defensa. Hay naciones en las cuales las diferentes áreas de la sociedad están interconectadas y dependen por completo del desarrollo de las tecnologías de la informática y las comunicaciones. Esos países están más expuestos a los efectos de la guerra cibernética y el asunto es analizado como un tema de seguridad nacional. Otros, por el contrario carecen de tal nivel de interconectividad tanto hacia el interior

como hacia el exterior. Pero todos, de una u otra forma, están expuestos a sus acciones.

Estas últimas naciones – casi siempre subdesarrolladas – dependen de las ricas para la tenencia de los soportes informativos (computadoras, software, etc.) y ya esos pueden estar programados como parte de esa guerra cibernética y contar con software “maliciosos” que en un momento determinado pone fuera de servicio cualquier estructura.

A la luz de las normas del Derecho Internacional y en particular del Derecho Internacional Humanitario existen otros factores que requieren de un detallado estudio. En primer lugar, el ciberespacio no está bajo el control absoluto de una nación, sin embargo, los soportes físicos que conforman su existencia si están dentro de la soberanía de los Estados. En segundo lugar, en su desarrollo no solo participan los Estados, sino también una gran variedad de actores no estatales, de agencias e individuos independientes. En tercer lugar, la tecnología prolifera a una velocidad extraordinaria y de manera impredecible. En meses envejecen medios, que en su momento fueron una “revolución” y se extienden por el mundo rápidamente.

No es casual que el gobierno de Estados Unidos está interesado por legalizar la guerra cibernética en el ámbito del Derecho Internacional. Por un lado intentan legitimar sus operaciones en ese campo dado el alto grado de desarrollo que poseen y por la otra buscan la forma de defenderse ante la posibilidad real de que sus sistemas sean vulnerados.

La guerra cibernética ya es una realidad. Es una utopía intentar detenerla. En la medida que revolucione el campo de la informática y las comunicaciones su peso en el campo de las relaciones internacionales y en el desarrollo de los conflictos armados será aún mayor. Los documentos legales existentes hasta el presente son parcialmente suficientes para determinar su legitimidad. Sin embargo, este nuevo tipo de guerra nos debe conducir a un análisis más dialéctico de los conceptos de aplicabilidad del Derecho Internacional Humanitario, que pone su énfasis en el carácter material del tipo de conflicto y no precisamente en la protección de las víctimas. Hoy es difícil conceptualizar con exactitud si un conflicto es puramente “internacional” o “no internacional”. Los cambios que se han producido en los últimos años nos indican que lo importante no es color del gato, sino la situación de las víctimas.

Es válido a la luz del derecho la toma de medidas de autodefensa ante la presencia de la guerra cibernética. Todo Estado tiene derecho a defenderse ante tal tipo de guerra, que con frecuencia toma la vestidura de una agresión.

Siempre hemos afirmado que en el Derecho Internacional Humanitario se recogen las normas básicas para enfrentar cualquier cambio que se produzca en los métodos y medios de hacer la guerra. Pero también hemos sido del criterio que ese Derecho requiere de su constante actualización y desarrollo. No es fácil

alcanzar tal propósito, por cuanto cualquier precisión de las normas pasa inevitablemente por los intereses de quienes determinan en gran medida la propia aplicación de ese Derecho. Tenemos en nuestras manos la posibilidad de ponernos a pensar en aquellos conceptos que requieren de precisiones, difundir nuestros criterios. Hoy existen en la red de redes innumerables artículos de especialistas en Derecho Internacional Humanitario cuyos criterios han sido acogidos como doctrinales. Nosotros contamos con talentos suficientes para también llenar la red de nuestros propios puntos de vista. Los nuevos desafíos que nos impone la guerra cibernética es un momento ideal para ello.