Soft Power
Revista euro-americana de teoría
e historia de la política y del derecho

Vol. 9(2). Julio-Diciembre 2022
ISSN (online): 2539/2239 ISSN (print): 2389-8232
http://dx.doi.org/10.14718/SoftPower.2022.9.2.18

OTRA MANERA DE HACER LA GUERRA. GUERRA Y DERECHO EN LA ERA DIGITAL[1]

Stefano Pietropaoli
Università degli Studi di Firenze

ANOTHER WAY OF WAGING WAR WAR AND LAW IN THE DIGITAL AGE

La guerra global

Hasta principios del siglo XX, la decisión de recurrir a la guerra se consideraba un "derecho natural" del que todo Estado era titular (C. Schmitt, 2002). La guerra entre Estados no era justa ni injusta: era un asunto de Estado, y como tal no necesitaba ser justa (C. Schmitt, 1988). Pero a partir de 1919 cobró fuerza una idea opuesta, según la cual el uso de la fuerza debía considerarse una infracción del derecho internacional. Animando este impulso (solo aparentemente) irenista estaba la percepción de un conflicto cuya naturaleza trágica sin precedentes se expresaba en la entrada simultánea en escena de dos nuevos elementos: el aire y el fuego. El espacio de la guerra estalla en todas las direcciones. El cielo está surcado por bombarderos que traen la guerra desde arriba y se convierte en el teatro de los duelos aéreos. Esta verticalidad aérea se forja con el fuego de la técnica, en la misma fragua donde se construyen tanques, cañones de largo alcance y submarinos, y donde se desarrollan los gases tóxicos.

1. Fecha de recepción: 2 de abril 2022; fecha de aceptación: 4 de abril 2022. El presente artículo es el resultado de un proyecto de investigación desarrollado en el Dipartimento di Scienze giuridiche de la Università degli Studi di Firenze.

En el plano normativo, la inversión del derecho a hacer la guerra en su opuesto exacto (la guerra como crimen) ya se había elaborado —aunque de forma todavía aproximada— en el estatuto de la Sociedad de Naciones. Posteriormente, en el Pacto de París (o Pacto Kellogg-Briand) de 1928, casi todos los Estados del mundo expresaron su condena a la guerra como medio para resolver las diferencias internacionales y se comprometieron a renunciar a ella como instrumento de política nacional. Este punto de vista fue recogido y consagrado en la Carta de las Naciones Unidas tras la Segunda Guerra Mundial.

La guerra terrestre del viejo derecho público europeo era ya un recuerdo lejano. La Segunda Guerra Mundial fue una guerra aérea, una guerra mecanizada, una guerra submarina, una guerra química y una guerra atómica. Pearl Harbour y Dresde, Coventry e Hiroshima son los lugares que testimonian los efectos catastróficos de una nueva revolución espacial (Colombo, 2006).

Como es sabido, la Carta de las Naciones Unidas establece que sus miembros deben resolver las controversias internacionales por medios pacíficos, absteniéndose de recurrir a la amenaza o al uso de la fuerza (art. 2), y confiere al Consejo de Seguridad la responsabilidad de mantener la paz y la seguridad internacionales (art. 24), bien mediante medidas que no requieran el uso de la fuerza (art. 41), bien mediante acciones que impliquen el empleo de fuerzas aéreas, marítimas o terrestres (art. 42). En otras palabras, la Carta ha establecido la prohibición para todo Estado de recurrir autónomamente a la guerra con la única —pero fundamental— excepción de la legítima defensa, expresamente reconocida como "derecho natural de autoprotección individual o colectiva", que todo miembro puede ejercer "en caso de ataque armado contra un miembro de las Naciones Unidas, mientras el Consejo de Seguridad no haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales" (art. 51).

El uso de las armas se ha considerado así un fenómeno regulable desde el punto de vista jurídico, pero al mismo tiempo la guerra se ha convertido en un acto ilícito internacional con sólo dos excepciones fundamentales: la guerra como sanción adoptada por el Consejo de Seguridad; la guerra como medio de legítima defensa de un Estado ante una agresión en curso. Por lo tanto, puede decirse que, en el plano normativo, la relación entre la guerra y el derecho sigue estando determinada por las Naciones Unidas y por la atribución al Consejo de Seguridad del papel de árbitro de la guerra y la paz en el plano internacional. Sin embargo, debido a la elección de atribuir un poder de veto a los cinco miembros permanentes del Consejo de Seguridad, el mecanismo que regula el uso de la fuerza a nivel internacional ha resultado ser sustancialmente inadecuado o

ineficaz, ya que ninguna guerra emprendida por países como Estados Unidos, el Reino Unido, Francia, China o Rusia puede considerarse un delito internacional. Por lo tanto, nos encontramos ante un punto muerto. Incluso hoy, las cinco potencias vencedoras de la Segunda Guerra Mundial siguen teniendo el poder de decretar la legitimidad de una intervención bélica, y es evidente que no están dispuestas a renunciar al privilegio que les otorga la Carta, lo que hace que las Naciones Unidas sean irreformables de facto (Zolo, 2005).

Las consecuencias de esta situación son evidentes. Por un lado, el Consejo de Seguridad ha seguido siendo el único árbitro de la legitimidad del recurso a la guerra por parte de los Estados que se creen objeto de un acto de agresión, manteniendo firmemente en sus manos la facultad de interpretar las disposiciones del artículo 51 de forma extremadamente restrictiva o, por el contrario, absolutamente elástica, según la conveniencia política y estratégica de los cinco miembros permanentes. Por otra parte, en lo que respecta a la utilización de medidas apropiadas para proteger la paz y la seguridad internacionales, el Consejo de Seguridad —en particular debido a los vetos cruzados de Estados Unidos y la URSS— estuvo durante mucho tiempo en un punto muerto, que solo terminó con el fin de la Guerra Fría. Ninguna disposición de la Carta de la ONU impidió la matanza de cientos de miles de personas en Corea o el establecimiento de "Zonas de Fuego Libre" en Vietnam del Sur.

Solo a partir de la última década del siglo XX el Consejo de Seguridad ha comenzado a utilizar ampliamente los instrumentos previstos en el Capítulo VII de la Carta de la ONU (Cassese, 1993). En algunos casos se ha tratado de medidas que no implican explícitamente el uso de la fuerza, destinadas a garantizar el respeto de las sanciones ya establecidas por las Naciones Unidas. En otros, el Consejo de Seguridad ha autorizado un uso limitado de la fuerza en el contexto de las llamadas operaciones de mantenimiento de la paz. Otras veces, el Consejo ha llegado a autorizar el uso de "todos los medios y todas las medidas necesarias" para salvaguardar la paz. Y es fundamental a este respecto señalar que, debido a la falta de institución de una fuerza internacional dirigida por las Naciones Unidas (véase el capítulo VII, artículos 43-47 de la Carta), las organizaciones militares regionales, in primis la OTAN, han sido autorizadas a recurrir a la guerra. Pero aún más significativo es que en muchos casos el Consejo de Seguridad no ha autorizado el uso de la guerra y, sin embargo, se han llevado a cabo operaciones militares que no solo no se han considerado ilícitas, sino que se han justificado moralmente (y en algunos casos legalmente) en nombre de la doctrina de los derechos humanos (Zolo, 2002).

En los últimos años, la tensión entre dos de los principios fundamentales de la Carta de las Naciones Unidas se ha resuelto cada vez más en el sentido de la prevalencia de la protección de los derechos humanos sobre el principio de la integridad territorial de un Estado soberano. A muchos les ha parecido un éxito, pero cabe señalar que se ha conseguido cada vez con más frecuencia haciendo caso omiso de las normas establecidas por el derecho internacional sobre el uso de la fuerza. Además, los cinco miembros permanentes del Consejo de Seguridad (y Estados Unidos en particular), si por un lado han reclamado el derecho a intervenir en defensa de los derechos humanos incluso a costa de violar la soberanía de otros países soberanos, por otro han reclamado constantemente su propia intangibilidad ante posibles acusaciones de que ellos mismos están violando dichos derechos (Zolo, 2009). Por lo tanto, no parece excesivo hablar de una hipersoberanía sustancial de estos actores en la escena internacional.

Este es el contexto en el que la guerra tras el final de la Guerra Fría se ha convertido en una guerra global: global porque está desespacializada en un sentido geopolítico e indefinida en términos de tiempo, pero global también porque es ilimitada en términos jurídicos (Galli, 2002).

Guerra y ciberespacio

Los cambios en la conducción de las hostilidades siempre han estado estrechamente relacionados con la evolución de las tecnologías aplicables a las necesidades de la guerra. Al igual que la fusión del bronce, la producción de pólvora o la fusión del átomo, el desarrollo de las tecnologías de la información no podía sino implicar una transformación en la forma de hacer la guerra. Pero este último cambio es más profundo que muchos otros. Implica la dimensión espacial de la guerra, en la medida en que la guerra global "se manifiesta en el no-espacio (en el sentido moderno) de la globalización", llevando a término la lógica de la movilización total y la guerra discriminatoria que había sido provisionalmente frenada por la Guerra Fría (Galli, 2002, p. 53).

La guerra global como máxima expresión de la técnica no sólo se refiere a la mejora de los sistemas de puntería de los misiles, a la posibilidad de encriptar las comunicaciones estratégicas con sistemas inimaginables hasta hace unos años, o a golpear un objetivo a miles de kilómetros gracias a un dron controlado por satélite. En otras palabras, las tecnologías de la información no solo han innovado profundamente los

instrumentos "clásicos" de la guerra (armas, medios, comunicaciones, etc.), sino que ellas mismas son un instrumento y un objetivo de la guerra. Es en este último sentido que la guerra contemporánea se convierte en algunos casos en una guerra tan diferente de las formas anteriores que merece un nuevo apelativo: ciberguerra (Halpin, 2006).

El ciberespacio se ha convertido en uno de los campos de batalla en los que se miden las pequeñas y grandes potencias (Hildebrandt, 2013). Después de la guerra terrestre, marítima, aérea y submarina, ¿ha llegado la hora de una guerra librada en el espacio virtual? Para algunos, la idea puede evocar la imagen de un inmaculado teatro de guerra, pisado por técnicos con batas blancas y donde el único sonido audible es el rápido tic-tac de los dedos sobre el teclado de un ordenador. Y, sin embargo, sigue tratándose de la guerra, con o sin su tributo de sangre, los uniformes rotos, los gritos de los cuerpos destrozados por una granada (Gartzke, 2013).

El gran problema de la ciberguerra radica precisamente en esta representación ilusoria de una guerra menos violenta y brutal que el enfrentamiento entre falanges hoplitas, la caballería medieval o la artillería del siglo XIX. Como en todas las guerras, la ciberguerra también tiene la finalidad de golpear objetivos considerados fundamentales para asegurar la victoria sobre el enemigo. Y como en cualquier guerra, el mejor armamento y equipamiento de las tropas puede resultar una ventaja táctica decisiva.

Desde el final de la Guerra Fría, y aún más después del 11 de septiembre de 2001, la guerra contra el terrorismo se ha convertido en el arquetipo de un nuevo tipo de guerra. En contra de los deseos de muchos irenistas, la guerra no ha desaparecido. Ha cambiado de aspecto. Términos como uso de la fuerza, guerra contra el terrorismo, construcción de la paz, intervención humanitaria, operaciones de paz y otros se han convertido cada vez más en disfraces hipócritas de un fenómeno que afecta a la vida de millones de personas. El hecho de que la expresión más sencilla e intuitiva que indica el recurso colectivo a la violencia —la "guerra", de hecho— esté ahora prohibida en el léxico jurídico y político contemporáneo no debe engañarnos. Las consecuencias de esta eliminación son evidentes. La posibilidad de no utilizar el término guerra abiertamente es un recurso formidable para aquellos que pueden hacer uso de la propia guerra. Si ya nadie declara la guerra es porque recurrir a ella es ilícito en el plano jurídico y cada vez menos justificable ante la opinión pública. Si la guerra ya no se declara formalmente, es mucho más fácil eludir la responsabilidad relacionada con la observancia de las normas que disciplinan la actividad bélica (el llamado *jus in bello*).

En los últimos veinte años la guerra —independientemente del nombre con el que

se la denomine— se ha convertido así en una guerra sin espacio ni tiempo (Justicia Infinita era el nombre original de la operación Libertad Duradera puesta en marcha tras el ataque terrorista al World Trade Center). Las distinciones del antiguo derecho internacional humanitario —entre civiles y militares, entre neutrales y beligerantes, entre prisioneros y combatientes— han implosionado así, y junto con ellas se ha desvanecido la posibilidad misma de limitar el conflicto de la guerra. La ciberguerra es quizás la expresión más inquietante de esta nueva guerra. Accionando un joystick o un ratón, es posible golpear a cualquiera, en cualquier lugar y en cualquier momento.

Las armas empleadas son diferentes a las que estamos acostumbrados, pero no por ello son menos destructivas. La infraestructura informática de cualquier país es ahora tan esencial para el funcionamiento del aparato estatal como para la prestación de servicios a la población. Como tales, son objetivos principales de un ciberataque. No se trata solo de hacer inaccesible un sitio concreto (normalmente mediante ataques DDoS), o de piratear bases de datos confidenciales y revelar su contenido. Un ciberataque puede producir daños materiales y víctimas humanas de forma totalmente comparable a un arma analógica. Con el malware, es posible bloquear el suministro de electricidad, gas o petróleo de un país (recuérdese el episodio del oleoducto Colonial en mayo de 2021, que dejó fuera de servicio la planta que suministra el 45% del combustible a la costa este de Estados Unidos), abrir a distancia las esclusas de una presa, interrumpir la gestión del tráfico por carretera, aéreo o ferroviario (con las consecuencias imaginables) o dañar una central nuclear.

Un ejemplo que puede aclarar este punto mejor que cualquier explicación es el caso Stuxnet (Zetter, 2014). Este término denota un malware desarrollado con el fin de causar daños físicos a los sistemas de control de procesos industriales, típicos de grandes plantas como fábricas, refinerías, etc. En 2010, la central nuclear iraní de Natanz sufrió un ciberataque a través de Stuxnet. El "misil cibernético" provocó la destrucción de la sección de enriquecimiento de uranio de la planta al enviar órdenes anómalas a más de mil centrifugadoras, que se aceleraron de esta manera hasta destruirse. Al mismo tiempo, Stuxnet permitió camuflar los datos de control del sistema, impidiendo que el problema se detectara a tiempo para asegurar la planta. De este modo, el ataque se descubrió cuando el proceso era irreversible.

Si se conoce suficientemente la tipología del atentado y los daños causados por el mismo, es más complicado rastrear a la persona que lo ha concebido y ejecutado. Es un hecho que la ciberguerra no solo no se declara —y, por tanto, cada ataque es un ataque sorpresa— sino que, sobre todo, no se reconoce quién ataca, lo que dificulta

entender por qué lo hacen, cuáles son sus próximos movimientos y cómo reaccionar.

Desde el punto de vista jurídico, la cuestión de si, más allá de los clarísimos problemas de aplicación, el derecho internacional de los conflictos armados es aplicable a la ciberguerra es central (Brown & Poellet, 2012).

Desde Tallin hasta Kíev

El actual conflicto entre Rusia y Ucrania no es más que la enésima y llamativa confirmación de esta nueva forma de hacer la guerra (que complementa sus manifestaciones análogas), cuyos pródromos ya se podían vislumbrar a finales del siglo pasado y que se reveló por primera vez de forma muy clara en 2007, cuando Estonia fue protagonista de la recordada Primera Guerra de la Red. Durante al menos tres semanas, los sistemas informáticos de las principales instituciones políticas, financieras y medios de comunicación del país báltico fueron objeto de un ciberataque masivo (del que, por supuesto, el principal sospechoso fue Rusia) que impidió su correcto funcionamiento. Al año siguiente, la OTAN quiso enviar una señal de claro valor simbólico estableciendo en la capital estonia su cuartel general para la defensa de las infraestructuras estratégicas occidentales: el Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE). Como parte de las actividades de este grupo de expertos, se promovió la redacción de un documento que enmarca el problema de la aplicabilidad del derecho internacional a las operaciones de ciberguerra. El grupo de expertos encargado de la investigación elaboró algunas normas aplicables a la ciberguerra en el Manual de Tallin sobre el Derecho Internacional Aplicable a la Ciberguerra de 2013 (M. N. Schmitt & NATO Cooperative Cyber Defence Centre of Excellence, 2013).

El grupo de expertos encargado de la investigación identificó hasta 95 normas aplicables a la ciberguerra en el Manual de Tallin sobre el Derecho Internacional Aplicable a la Ciberguerra de 2013. El texto aborda una larga serie de temas agrupados por áreas temáticas: la relación entre el Estado y el ciberespacio, el uso de la fuerza y la legítima defensa, el derecho de los conflictos armados, el tratamiento del personal médico y religioso, la neutralidad, la ayuda humanitaria, etc. Según las intenciones de los autores (que oficialmente no reflejan las de la OTAN), el Manual debe interpretarse como un intento de limitar el potencial destructivo de las operaciones de ciberguerra mediante su encuadramiento en el derecho internacional de los conflictos armados vigente.

Uno de los puntos centrales del Manual (*Rule* 10) es que "a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful". Esta formulación recuerda la prohibición de la amenaza (del uso de la fuerza) y del uso de la fuerza sancionada por el art. 2.4 de la Carta de las Naciones Unidas ("All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations"), y que ahora se ha establecido indiscutiblemente como una norma de derecho internacional consuetudinario. El Manual propone inmediatamente después (*Rules* 11 y 12) las siguientes definiciones: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force"; "A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force".

Obviamente, estas definiciones no resuelven el problema central: ¿cuándo el ataque (cibernético) alcanza tal intensidad que puede considerarse un uso de la fuerza? La respuesta, como es fácil adivinar, no es unívoca. Al fin y al cabo, la historia del derecho internacional no es más que la historia de las posibles respuestas a esta pregunta. En cualquier caso, cabe señalar que el manual propone una lista de parámetros que deben tenerse en cuenta para llegar a una solución (gravedad, inmediatez, carácter directo, invasividad, mensurabilidad de los efectos, carácter militar, implicación del Estado y presunta legalidad). Además, considerar un ciberataque del mismo modo que un ataque militar "clásico" conlleva consecuencias jurídicas precisas. Entre ellos, una de los más relevantes es el reconocimiento del derecho del Estado atacado a reaccionar con la fuerza cuando el ciberataque alcanza el nivel de conflicto armado. De hecho, la *Rule* 13 prevé expresamente la autodefensa frente a un ataque armado: "A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects". Sin embargo, también en este caso, el problema se refiere a la decisión sobre la consecución del nivel de ataque armado.

El Manual de 2013 fue actualizado y ampliado en febrero de 2017 (M. N. Schmitt & NATO Cooperative Cyber Defence Centre of Excellence, 2017). La nueva versión —que consta de 154 disposiciones— complementa la anterior con secciones dedicadas

específicamente a la responsabilidad de los Estados, el derecho del mar y el derecho internacional de las telecomunicaciones. Aunque también trata del derecho internacional aplicable a las operaciones cibernéticas en "regímenes jurídicos de tiempo de paz", el nuevo nombre carece ahora de referencias explícitas a la guerra: "Manual de Tallin 2.0 sobre el derecho internacional aplicable a las operaciones cibernéticas".

Por muy desinteresada, independiente e imparcial que sea la labor de los expertos que han trabajado en las dos versiones del Manual, lo cierto es que el resultado de sus esfuerzos —además de no tener ninguna fuerza jurídicamente vinculante— se percibe claramente como "centrado en la OTAN", sin expresar en absoluto las diferentes interpretaciones y sensibilidades de actores internacionales clave como China y Rusia. Este carácter problemático se ve sin duda agravado por la consonancia del Manual con los objetivos fijados por la estrategia cibernética desarrollada por el Departamento de Defensa estadounidense en los últimos años. De hecho, la OTAN y Estados Unidos sostienen unánimemente no solo que el derecho internacional se aplica al ciberespacio, sino que su defensa se incluye entre las obligaciones de defensa colectiva para las que se creó la Alianza. Desde esta perspectiva, el gobierno estadounidense ha aumentado considerablemente en los últimos años el presupuesto de gastos del cibercomando (CYBERCOM) para crear una fuerza de misión cibernética compuesta por 6.200 operadores y 113 unidades.

El objetivo general de la defensa del ciberespacio es evitar o al menos contener los daños a las infraestructuras críticas, tanto militares como civiles. Pero este objetivo debe alcanzarse en un escenario en el que las distinciones del viejo derecho internacional, como las que existen entre civil y militar, neutral y beligerante, prisionero y combatiente, se han roto: la ciberguerra no solo no se declara —y por tanto todo ataque es por sorpresa— sino que, sobre todo, no se reconoce quién ataca, por qué, cuándo y cómo lo hace, cuáles serán sus próximos movimientos, cómo se debe reaccionar, etc.

Detrás de la mayoría de los ciberataques sigue habiendo Estados nacionales, pero hay numerosos casos de operaciones que pueden rastrearse hasta entidades no estatales (basta pensar en las actividades de grupos como Anonymous). En este sentido, desde hace algunos años se habla de ciberterrorismo para indicar los atentados perpetrados por grupos de hacktivistas que explotan las tecnologías de la información para generar miedo o intimidar a una sociedad considerada enemiga a partir de un juicio inspirado en una ideología precisa.

También, desde esta perspectiva, el conflicto actual atestigua que entidades como el colectivo bielorruso Conti o la organización rusa conocida como Killnet son capaces de

lanzar ataques capaces de interrumpir las infraestructuras estratégicas de países considerados enemigos.

Estas amenazas deben tomarse muy en serio. Hoy en día nadie puede considerarse inmune a esta otra manera de hacer la guerra.

Referencias

Brown, G., & Poellet, K. (2012). The Customary International Law of Cyberspace. *Strategic Studies Quarterly*, *6*(3), 126–145. JSTOR.

Cassese, A. (1993). *Los derechos humanos en el mundo contemporaneo*. Editorial Ariel.

Colombo, A. (2006). *La guerra ineguale: Pace e violenza nel tramonto della società internazionale*. Il Mulino.

Galli, C. (2002). *La guerra globale* (1. ed). GLF editori Laterza.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, *38*(2), 41–73. JSTOR.

Halpin, E. F. (A c. Di). (2006). *Cyberwar, netwar and the revolution in military affairs*. Palgrave Macmillan.

Hildebrandt, M. (2013). Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace. *The University of Toronto Law Journal*, *63*(2), 196–224. JSTOR.

Schmitt, C. (1988). *Die Wendung zum diskriminierenden Kriegsbegriff*. Duncker und Humblot.

Schmitt, C. (2002). *El Nomos de la Tierra en el derecho de gentes del «ius publicum europaeum»*. Comares.

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence (A c. Di). (2013). *Tallinn manual on the international law applicable to cyber warfare: Prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge University Press.

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence (A c. Di). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (Second edition). Cambridge University Press.

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon* (First Edition). Crown Publishers.

Zolo, D. (2002). *Invoking humanity: War, law, and global order*. Continuum.

Zolo, D. (2009). *Victors' justice: From Nuremberg to Baghdad*. Verso.

Zolo, D. (2005). Los Señores de la paz: Una crítica del globalismo jurídico / Danilo Zolo ; traducción de Roger Campione. In *Los Señores de la paz: Una crítica del globalismo jurídico*. Dykinson.