REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 10 NÚM. 2 (2021) • PÁGS. 43-68 • DOI 10.5354/0719-2584.2021.57077
RECIBIDO: 21/4/2020 • APROBADO: 7/12/2020 • PUBLICADO: 31/12/2021

DOCTRINA

El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra

International Law in the face of new medias and spaces in which to develop war: Cyberwarfare

Borja García Vázquez
Universidad Autónoma de Nuevo León, México

RESUMEN El derecho internacional ha regido las relaciones entre los Estados y los modos de hacer la guerra durante siglos. El desarrollo tecnológico ha ampliado los campos de batalla al ciberespacio, un medio favorable para escapar a cualquier cumplimiento normativo. Atendiendo al esfuerzo del Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN, con la promulgación del Manual Tallin 2.0, y en un ejercicio de adaptación y reinterpretación, por analogía, de la labor de la Asamblea General de Naciones Unidas, se propone la reflexión ante problemáticas que deben afrontarse desde el derecho internacional y que constituyen un riesgo para la democracia y la protección de los derechos humanos, para determinar la vigencia normativa ante el desarrollo tecnológico, la aparición de nuevas armas, con su capacidad para producir destrucción en masa, actores en los conflictos, como los contratistas, y las barreras en la determinación de responsabilidad por las operaciones cometidas en este medio.

PALABRAS CLAVE Ciberguerra, ciberarmas de destrucción masiva, cibercontratistas, cibermercenarios, ciberoperaciones.

ABSTRACT International Law has ruled international relations and ways of waging war for centuries. Technological development has expanded the battlefields to cyberspace, a favorable means to escape from any regulatory compliance. In response to the effort of the NATO Center for Cooperative Cyber Defense, with the promulgation of the Tallin 2.0 Manual, and in an exercise of adaptation and reinterpretation, by analogy, of the work of the General Assembly of the United Nations, it is proposed to reflect on problems that must be addressed from International Law and that constitute a risk for democracy and the protection of human rights, to determine normative validity in the face of technological development, the appearance of new weapons, with their capacity of mass destruction, actors in conflicts, such as contractors, and barriers in determining responsibility for the operations committed in this environment.

KEYWORDS Cyberwarfare, cyber weapons of mass destruction, cyber contractors, cyber mercenaries, cyber operations.

Introducción

El constante desarrollo y la innovación tecnológica ha generado, consolidado y posibilitado la evolución de un espacio virtual, que tiene un impacto directo en el mundo material: el ciberespacio. En septiembre de 2006, el Estado Mayor Conjunto de los Estados Unidos lo definió como «un dominio caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de sistemas en red e infraestructuras físicas asociadas» (Chairman of the Joint Chiefs of Staff, 2006: 3).

Otra definición oficial es la contenida en la Joint Publication (JP) 1-02, clave que recibe el diccionario de términos militares y asociados al Departamento de Defensa de los Estados Unidos, que contempla el ciberespacio como «un dominio global dentro del entorno de la información, consistente en la red interdependiente de infraestructuras de tecnología de la información, incluida internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados» (Cahanin, 2012; traducción propia).[1]

Nos encontramos con un medio artificial cuyo diseño y gobierno, netamente humano, responde a la fusión de un soporte físico (hardware) y virtual (software), que permite alterar las aptitudes y condiciones de este espacio, que es replicable y reparable de acuerdo con las necesidades (Bryant, 2013: 30), y cuya modificación tiene repercusiones en el mundo material, al afectar la vida de los usuarios de estos sistemas.

El problema que representa el ciberespacio es la ambigüedad que ofrece este medio para posibles elementos hostiles, y el amplio ámbito sobre el que se producen sus efectos, que sobrepasan las fronteras físicas y los mecanismos institucionales. Dada la generalización de percepción de impunidad ante los actos cometidos con las tecnologías de la información y la comunicación (TIC), se ha podido percibir erróneamente un sentimiento de ausencia del cumplimiento normativo, aunque las estructuras y mecanismos del derecho internacional sigan presentes. En el plano de las organizaciones internacionales, desde 1998 las TIC son objeto de debate anual en la agenda de trabajo de la Organización de las Naciones Unidas, y desde 2004, cuando se estableció el Grupo de Expertos Gubernamentales (GEG) con la Resolución A/RES/58/32, se emite un informe anual respecto a la situación global de la ciberseguridad.[2]

1. Traducción del original: «Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers».

2. «Fact sheet: Developments in the field of information and telecommunications in the context of

La dificultad radica en los medios para que se continúe aplicando la ley ante la porosidad del nuevo escenario ciber. Como consecuencia directa de la simbiosis que se está produciendo entre ambos mundos, digital y material, estamos de acuerdo con Barrio Andrés (2018: 78) al decir que «llegará un momento, no muy lejano, en el que todo el derecho será ciberderecho». Asimismo, el prefijo *ciber* en la realidad de los conflictos internacionales ha sido advertido por el GEG, al alertar en la Resolución A/65/201 que «cada vez son más numerosos los informes de que los Estados están desarrollando tecnologías de la información y las comunicaciones como instrumentos de guerra y para fines de inteligencia y políticos».

El derecho internacional ha respondido tradicionalmente al fenómeno de la guerra desde dos perspectivas: el *ius ad bellum*, encargado de identificar cuándo es lícito que los Estados utilicen la fuerza armada; y el *ius in bello*, que es el control de la guerra a través de sistemas normativos (Pérez González, 2017a: 30-31). Ante el desafío que representa al derecho internacional el desarrollo de conflictos en el ciberespacio, el Centro de Excelencia Cooperativa de Ciberdefensa de la OTAN (CCDCOE, por sus siglas en inglés) publicó el Manual de Tallin en 2013, luego revisado en 2017 en el conocido Manual de Tallin 2.0, sobre cómo se aplica el derecho internacional en las ciberoperaciones, en un intento de readaptar la tradición normativa al nuevo escenario propiciado por los cambios tecnológicos.

Otro elemento sobre el que debemos reflexionar es el concepto de *arma de destrucción masiva*, el cual ha quedado obsoleto al no haber adaptado su contenido a la evolución técnica. La Resolución 1.540 (2004) del Consejo de Seguridad de Naciones Unidas reconocía la necesidad de los Estados de evitar la proliferación de este tipo de armas, aunque su consideración quedaba circunscrita a los sistemas que emplean elementos nucleares, biológicos o químicos (NBQ); postura que ha sido adoptada en la comunidad internacional, la cual tiene en cuenta exclusivamente aquellas que hacen uso de agentes NBQ para producir daños a gran escala, mientras que existe una ausencia regulatoria respecto de las armas cibernéticas, cuyos efectos destructivos podrían llegar a ser equivalentes al de los sistemas mencionados.

En esta década se ha multiplicado la creación estatal de elementos de ciberdefensa —ligados a las fuerzas armadas y los servicios de inteligencia—, a fin de contar con la capacidad de responder a cualquier hostilidad que pueda darse por esta causa. Frente a las facultades que permitían los medios tradicionales, las TIC —haciendo uso del ciberespacio— ofrecen la posibilidad de desarrollar códigos maliciosos o *malware,* que pueden ejercer un poder de destrucción masivo, pues de darse las circunstancias idóneas, podrían causar la muerte o herir gravemente a la población mediante su uso.

Aznar Fernández-Montesinos (2011: 23) expresa que «el modo en que se lleva a

international security», United Nations Office for Disarmament Affairs, julio de 2019, disponible en https://bit.ly/2YAoKXD.

cabo la guerra obedece a los patrones culturales de las sociedades implicadas, y estos quedan a su vez delimitados por los modelos de producción y de organización». Hoy nuestra cultura es digital y, por extensión, la guerra se ha visto afectada por esta realidad. Retomando el planteamiento de Martín Serrano (2008: 56), quien considera la existencia de una contradicción entre el desarrollo de los medios de producción y comunicación frente al subdesarrollo de las relaciones sociales, cabría preguntarse si esta oposición se haría extensible al ámbito del derecho internacional, con la introducción de los nuevos medios y espacios con los que hacer la guerra, al entender que la ley va a remolque de la evolución científica.

Un ataque contra la infraestructura crítica de un Estado, como pueda ser una refinería, una central energética o los elementos que controlan el sistema bancario o aeroportuario, podría devastar una región sin tener que emplear un arma convencional o una fuerza militar sobre el terreno. Por ello, se debe meditar sobre las condiciones que ofrece el ciberespacio para determinar cuándo y cómo poder atribuir un ataque a un país, o si por el contrario las viejas normas han perdido su vigencia a la hora de precisar cómo conducir las hostilidades, enfrentándonos a un escenario de olvido del derecho internacional, en favor de la ambigüedad y la falta de responsabilidad que le ofrece a los Estados el empleo de sistemas ilícitos.

Atendiendo a esta exposición, el objetivo de este estudio es indicar la validez y actualidad que sigue poseyendo el derecho internacional en su uso aplicado al ciberespacio, los nuevos desafíos y obstáculos que afronta actualmente, y cómo debe ser su abordaje ante los elementos y actores clásicos de los conflictos armados en el espacio digital.

La seguridad estatal frente a las armas de destrucción masiva en la era digital

En el marco de las relaciones internacionales, impera el componente político frente al jurídico, en tanto que los Estados interactúan entre sí para cubrir sus intereses, mientras que el límite a su actuación se encuentra en la soberanía de los otros países (Pastor Ridruejo, 2016: 300). Cada Estado tiene un poder que ejerce sobre su territorio a través de los medios institucionales y normativos de que dispone, cuya demarcación se encuentra en la delimitación con otros países por medio de las fronteras.

Este poder es pleno en su territorio terrestre y subterráneo, y limitado en el espacio marítimo y aéreo, mientras que quedan excluidos los considerados espacios comunes, cuya asignación no es posible por ningún Estado (espacio ultraterrestre, cuerpos celestes, junto con la alta mar y los fondos marinos) y el régimen especial de la Antártida, que impide su apropiación (Ortega Carcelén, 2017: 255).

El paradigma de la soberanía estatal clásica parecería romperse con la irrupción

de la ficción del ciberespacio, pero para que este exista, se requiere de unas infraestructuras que estarán sujetas a las normas aplicables al territorio en que se encuentren. Por esta razón, el Manual de Tallin concebía como primera regla que «un Estado puede ejercer control sobre la infraestructura cibernética y las actividades dentro de su territorio soberano» (Schmitt, 2013: 25; traducción propia),[3] lo que se mantuvo igualmente, como primera regla, en el Manual de Tallin 2.0: «El principio de soberanía estatal aplica al ciberespacio» (Schmitt, 2017: 11; traducción propia),[4] por lo que el poder soberano puede ejercerse sobre todo el espacio que ocupa el medio digital en el territorio estatal.

La esfera jurisdiccional de los países abarca las infraestructuras físicas, y conforme al principio de personalidad activa y pasiva, también podrá aplicar su jurisdicción sobre las actividades virtuales ilícitas que hagan o sufran sus nacionales en o del extranjero (Barrio Andrés, 2018: 29), posición que era sostenida por la regla 2 del Manual de Tallin:

> Sin perjuicio de las obligaciones internacionales aplicables, un Estado puede ejercer su jurisdicción: a) sobre personas involucradas en actividades cibernéticas en su territorio; b) sobre ciberinfraestructura ubicada en su territorio; y c) extraterritorialmente, de conformidad con el derecho internacional (Schmitt, 2013: 27).[5]

Consecuencia de la práctica internacional, el Manual de Tallin 2.0 ha incluido un articulado más extenso, y destinado la regla 9 a la jurisdicción territorial:

> Un Estado puede ejercer la jurisdicción territorial en: […] b) ciberactividades originadas en, o completamente en su territorio; o c) ciberactividades que tengan un efecto sustancial en su territorio (Schmitt, 2017: 55; traducción propia).[6]

Y la regla 10, a la jurisdicción extraterritorial prescriptiva:

> Un Estado puede ejercer jurisdicción prescriptiva extraterritorial respecto a las ciberactividades: a) realizadas por sus nacionales; b) comprometidos a bordo de buques y aeronaves que posean su nacionalidad; c) realizado por ciudadanos extranjeros y diseñado para socavar gravemente los intereses estatales esenciales; d) realizado por ciudadanos extranjeros contra sus nacionales, con ciertas limitaciones;

3. Traducción del original: «A State may exercise control over cyberinfrastructure and activities within its sovereign territory».

4. Traducción del original: «The principle of State sovereignty applies in cyberspace».

5. Traducción del original: «Without prejudice to applicable international obligations, a State may exercise its jurisdiction: (a) over persons engaged in cyberactivities on its territory; (b) over cyberinfrastructure located on its territory; and (c) extraterritorially, in accordance with international law».

6. Traducción del original: «A State may exercise territorial jurisdiction over: […] (b) cyber activities originating in, or completed on, its territory; or (c) cyber activities having a substantial effect in its territory».

> o e) que constituyen crímenes de derecho internacional sujetos al principio de universalidad (Schmitt, 2017: 60; traducción propia).[7]

Estos preceptos dedican una delimitación más precisa al contemplar los casos en que el Estado podrá intervenir ante actividades cibernéticas, por lo que queda la jurisdicción extraterritorial limitada a lo dispuesto por el derecho internacional o el consentimiento de un gobierno extranjero (Schmitt, 2017: 66).

Las posibilidades que presentan la ambigüedad de las operaciones cibernéticas, y la falta de consenso internacional en la adopción de medidas comunes destinadas a combatir los efectos perniciosos de las mismas, se aprecian en la regla 12 del Manual 2.0 (Schmitt, 2017: 71), al reconocer la incapacidad de ejercicio de la jurisdicción sobre las personas e infraestructuras que, dotadas de inmunidad diplomática, desarrollen estas operaciones; y en la regla 13 (Schmitt, 2017: 75), que admite la falta de obligación de cooperación de los países para investigar y perseguir los ciberdelitos.

En materia penal, la competencia de la jurisdicción está limitada al territorio en que se aplica (Ortega Carcelén, 2017: 220), pero atendiendo al argumento de Barrio Andrés (2018: 31), al ser el ciberespacio un campo que no se encuentra en una concreta realidad física, «nada impide que un Estado ejerza su jurisdicción unilateralmente o en cooperación con otros Estados», entendiéndose que puede actuar individual o colectivamente en la defensa de las víctimas y contra los delitos cometidos en el ciberespacio desde su territorio.

La regla 6 del Manual de Tallin recogía la responsabilidad legal de los países: «Un Estado tiene responsabilidad legal internacional por la operación cibernética atribuible a él y que constituya un incumplimiento de una obligación internacional» (Schmitt, 2013: 35; traducción propia).[8] La dificultad que generan las TIC es demostrar el nexo de causalidad entre el agresor y los daños generados. Este hecho ha motivado la redacción de nuevas reglas en el Manual de Tallin 2.0, a fin de concretar el cumplimiento en las obligaciones por parte de los países, extendiéndola con el objetivo de garantizar la seguridad jurídica mundial, impidiendo la anomia de las relaciones internacionales.

Para ello, el Manual de Tallin 2.0 incorpora supuestos en los que el Estado es responsable por la ejecución de una ciberoperación por: órganos estatales, personas y entidades empoderadas con autoridad gubernamental (regla 15); órganos de un

7. Traducción del original: «A State may exercise extraterritorial prescriptive jurisdiction with regard to cyber activities: (a) conducted by its nationals; (b) committed on board vessels and aircraft possessing its nationality; (c) conducted by foreign nationals and designed to seriously undermine essential State imterests; (d) conducted by foreign nationals against its nationals, with certain limitatioms; or (e) that constitute crimes under international law subject to the universality principle».

8. Traducción del original: «A State bears international legal responsability for cyberoperation attributable to it and which constitutes a breach of an international obligation».

tercer Estado que opera por mandato directo atribuible a otro Estado (regla 16); o actores no estatales, ya sean personas o grupos, como son activistas, empresas de prestación de servicios informáticos, organizaciones de crimen organizado u organizaciones terroristas, que actúan por mandato de un Estado o con el conocimiento y beneplácito del mismo (regla 17).

La ambigüedad de las operaciones en el ciberespacio

El ciberespacio es propicio para el desarrollo de la *guerra híbrida*, concepto acuñado en 2005 por los militares estadounidenses James N. Mattis y Frank Hoffman, publicado en un artículo para el US Naval Institute, en el cual describían estos nuevos conflictos como una conjugación de métodos de lucha irregular —como las guerrillas, el terrorismo, grupos de narcotraficantes, etcétera—, junto con el empleo de los medios de comunicación y otras estrategias, sin que se respeten las reglas del derecho internacional (Mattis y Hoffman, 2005). Lo que caracteriza esta nueva realidad es la búsqueda de la irresponsabilidad, y el empleo de cualquier medio que posibilite escapar de la aplicación de la ley.

Se ha constituido la denominada *zona gris*, espacio actual donde se desenvuelven los conflictos, determinado por su ambigüedad, multidimensionalidad y gradualidad, y caracterizado por la presencia de múltiples intereses interconectados (Jordán, 2018: 131-133), con objetivos similares a los de una guerra —pero sin llegar a ella—, manteniéndose al límite de la legalidad, aunque su desarrollo pueda motivar un conflicto bélico (Baqués Quesada, 2018: 557). Los enfrentamientos armados se han vuelto amorfos, aprovechando la porosidad que ofrece la globalización, en que la interconexión material y digital ha permitido la creación de fórmulas elusivas de la ley, y medios de lucha opacos, que camuflan los intereses y los interesados en ellas, entremezclándose elementos en pugna indistinguibles, que aúnan objetivos legítimos e ilegales.

En palabras de Jordán (2018: 133), «la zona gris es un espacio intermedio en el espectro de conflicto político que separa la competición acorde con las pautas convencionales de hacer política, del enfrentamiento armado directo y continuado». Se trata de la evolución de los enfrentamientos internacionales, en que los Estados, en un intento de reducir la responsabilidad de sus acciones, buscan medios que les faciliten tales fines, a menor coste, con igual efectividad y con apenas consecuencias legales, como ocurren con las TIC, que ofrecen todas estas posibilidades.

En la práctica, el uso de la fuerza está prohibido, y las desavenencias entre países se han regulado de acuerdo con las normas relativas al arreglo de controversias, contenidas en la Carta de la ONU y en la Resolución 2.625 (XXV) de la Asamblea General de Naciones Unidas.

La regla 10 del Manual de Tallin adoptó la misma actitud que la Carta, al prohibir

el uso de la fuerza, replicada en la redacción de la regla 68 del Manual de Tallin 2.0: «Una operación cibernética que constituya una amenaza o uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o que sea de cualquier otra manera incompatible con los propósitos de las Naciones Unidas, es ilegal» (Schmitt, 2013: 45; 2017: 329; traducción propia).[9]

Si bien el conflicto estaría prohibido, cabría preguntarse qué ocurre cuando las hostilidades inevitablemente se dan en el medio digital. Estaríamos hablando en este caso de la *ciberguerra*, entendida como «la guerra realizada en el ciberespacio», es decir, los ataques militares ejecutados a través del medio digital, las infraestructuras de telecomunicaciones, y los sistemas informáticos y de información, incluido internet, que están interconectados globalmente (Melzer, 2011: 5).

La regla 11 del Manual de Tallin, recogida nuevamente en la regla 69 del Manual 2.0, estableció la definición del *uso de la fuerza* respecto de las ciberoperaciones: «Una operación cibernética constituye un uso de la fuerza cuando su escala y sus efectos son comparables a las operaciones no cibernéticas que se elevan al nivel de uso de la fuerza» (Schmitt, 2013: 47; 2017: 330; traducción propia).[10] Al igual que ocurre con los conflictos tradicionales, los efectuados en el medio digital admiten graduaciones, pero la realidad es que el mundo digital ha quebrado las reglas que marcaron el mundo analógico.

Las armas de destrucción masiva de la era digital

Con referencia a las armas nucleares, Kissinger (2016: 347) ha defendido que su existencia permitió el equilibrio internacional por medio de la disuasión. Sin embargo, hoy, frente a las circunstancias de que puedan darse ataques (digitales) sin previo aviso, el paradigma se ha roto. Ante las agresiones perpetradas desde el ciberespacio, no existe alerta previa, la amenaza se ha difuminado, pero el riesgo sigue latente y no ha desaparecido.

El concepto de *armas de destrucción masiva*, como puede comprobarse con la Resolución 1.540 (2004) del Consejo de Seguridad de Naciones Unidas, está limitado a los elementos NBQ y derivados, pero en ningún caso estos comprenden los diseños de computación, destinados a explotar vulnerabilidades de los sistemas de seguridad de instituciones, o elementos cuya alteración puede poner en grave riesgo a la población.

9. Traducción del original: «A cyberoperation 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 in consistent with the purposes of the United Nations, is unlawful».

10. Traducción del original: «A cyberoperation constitutes a use of force when its scale and effects are comparable to non-cyberoperations rising to the level of a use of force».

Teniendo en cuenta lo dispuesto en el Código Federal de los Estados Unidos —por la amplia experiencia en la investigación y almacenamiento de este tipo de armamento por este país—, su sección 2.332 define las *armas de destrucción masiva* como cualquier aparato destructivo (bombas, granadas, cohetes, misiles, minas o similares, que sean explosivos, incendiarios, o que emitan gas venenoso) diseñado para causar la muerte o herir gravemente con la emisión, diseminación o impacto de químicos tóxicos o venenosos, o sus precursores; así como armas que incluyan agentes biológicos, tóxicos o vectores; y cualquier arma diseñada para emitir radiación o radioactividad en niveles peligrosos para la vida humana.[11]

Los accidentes nucleares de Three Mile Island (1979), Chernóbil (1986) y Vandellós I (1989), así como incidentes en los que no concurrían elementos NBQ, pero que se caracterizaron por sus efectos catastróficos, como los hundimientos de los buques *Prestige* (2002) y *Sanchi* (2018), o los ataques terroristas del 11 de septiembre de 2001 contra los edificios del World Trade Center y el Pentágono, mostraron al mundo las devastadoras consecuencias que pueden desencadenar sobre la población este tipo de sucesos. Todos estos supuestos han sido imputables a las acciones de personas físicas determinadas, pero todos podrían repetirse por medio de ciberataques, sin la necesidad de contar con individuos en el escenario de los hechos, y sin que necesariamente la acción tenga que ser ejecutada por elementos humanos.

Hasta ahora no se han confirmado muertes provocadas por ciberataques, y los daños causados sobre infraestructuras no han sido de extensa gravedad (Mazanec, 2015: 82). En el caso del terrorismo, de acuerdo con el GEG, «hasta ahora ha habido pocos indicios de tentativas terroristas de comprometer o incapacitar la infraestructura» de las TIC «o de ejecutar operaciones utilizando estas tecnologías», las cuales se emplean en la actualidad «principalmente para comunicarse, reunir información, reclutar miembros, organizarse, promover sus ideas y actividades y solicitar fondos, pero en algún momento podrían llegar a usarlas para sus ataques».[12]

Una reinterpretación de las armas de destrucción masiva en la era digital

El potencial dañino de esta clase de medios se evidenció con Stuxnet, considerado la «primera arma autónoma con un algoritmo, y no una mano humana, apretando el disparador» (Liivoja, Naagel y Väljataga, 2019: 6), que fue empleado para atacar el programa nuclear iraní, destruyendo aproximadamente mil centrifugadoras nuclea-

11. «18 U.S.C. 2332a: Use of weapons of mass destruction», Govinfo.gov, disponible en https://bit.ly/30Zapis.

12. «Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional», Asamblea General de Naciones Unidas, A/65/201, 30 de julio de 2010, disponible en https://undocs.org/es/A/65/201.

res P-1, que representaban el 20% del total disponibles por el país (Mazanec y Thayer, 2015: 21). Respecto de estos sistemas destructivos, el problema que ha generado el ciberespacio, y que lo diferencia ante el armamento nuclear y su capacidad disuasoria —gracias a unos efectos visibles que generaban el terror de provocar el aniquilamiento de la humanidad—, es que en este medio no se perciben sus consecuencias, ni causa los mismos sentimientos de miedo (Burton, 2018: 7). Pese a que la disuasión es una cuestión estrictamente de defensa, al igual que ocurre con el armamento nuclear, la ciberdisuasión impacta de igual forma en el derecho internacional al ser un elemento de amenaza entre los Estados.

Nos encontramos así con el problema que generan las TIC, la falta de visibilidad de los medios empleados —aunque no de sus efectos—. Tradicionalmente, la fórmula utilizada para prohibir el empleo de nuevas armas no recogidas en los tratados fue la cláusula Martens, contenida en el Convenio II de la Haya, relativo a las leyes y usos de guerra terrestre de 1899, que demostró ser un elemento eficaz para limitar el empleo de armas que no reúnan los requisitos del derecho humanitario (Casanova y Rodrigo, 2016: 1.156-1.157), ante la incapacidad de prever nuevos dispositivos ante el desarrollo tecnológico. Así, pues, en caso de duda respecto de la permisividad o no de un sistema armamentístico, la interpretación del derecho internacional deberá ser acorde «a los principios de humanidad y los dictados de la conciencia pública» (Pérez González, 2017b: 80-81).

Lo que ha caracterizado a las armas nucleares es la incertidumbre respecto a la legalidad de su uso de acuerdo con el derecho internacional, ya que a pesar de la existencia del Tratado sobre la No Proliferación de las Armas Nucleares, que entró en vigor el 5 de marzo de 1970,[13] y la adopción el 7 de julio de 2017 del Tratado sobre la prohibición de las armas nucleares —la cual no ha entrado en vigor al no haber alcanzado el mínimo de ratificaciones—,[14] estos mecanismos siguen siendo empleados en las estrategias de disuasión de los Estados que las poseen (Rodríguez-Villasante Prieto, 2017: 582-584), lo que demuestra una prueba visible de la contradicción existente entre el espíritu de las normas internacionales y la *realpolitik* de los países. Si bien no existe, y parece improbable que se llegue a una situación en que se impida el uso o la amenaza a través de un tipo específico de arma, la cláusula Martens presenta las condiciones para concebir un límite al empleo de nuevas armas digitales.

En cualquier caso, el Manual de Tallin ha recogido en su regla 12 que «una ciberoperación, o una operación cibernética de amenaza, constituye un uso ilegitimo de fuerza amenazadora, y si se lleva a cabo, sería un uso ilegal de la fuerza» (Schmitt,

13. «Treaty on the Non-Proliferation of Nuclear Weapons (NPT)», International Atomic Energy Agency, disponible en https://bit.ly/2YJCors.

14. «Treaty on the Prohibition of Nuclear Weapons», United Nations Treaty Collection, 7 de julio de 2017, disponible en https://bit.ly/3AE8lii.

2013: 52; traducción propia).[15] Por lo tanto, cualquier ciberoperación o pronunciamiento público que tenga por finalidad amenazar con un ataque convencional o digital será considerado un uso ilegal de la fuerza.

La controversia surge cuando no se produce una advertencia, ni se conoce la identidad del sujeto que ejercita la fuerza. El empleo, difusión y efectos que provoca el *malware* comprende un fenómeno conocido globalmente, con ataques como Wannacry (2017) o Petya y Notpetya (2016), que dejaron inoperativos a millones de usuarios, en una situación de secuestro masivo, sin que pudiera concretarse la identidad de los atacantes. En otros casos, encontramos hackeos a centrales eléctricas, gaseoductos y oleoductos, como la estrategia que está adoptando Estados Unidos contra Rusia como respuesta a las operaciones digitales de este último,[16] que en 2015 y 2016 habría atacado con agentes externos, como el hacker Fancy Bear, los servidores del Partido Demócrata estadounidense, y los actos del grupo Sandworm, que hackeó docenas de organizaciones gubernamentales y empresas ucranianas.[17]

Hacia un nuevo paradigma de arma de destrucción masiva en la era digital

Junto con estos escenarios, si añadimos la utilización de estos métodos a los sistemas de control tanto de vehículos tripulados como no tripulados, en contra de la voluntad de los operadores, o simplemente por medio de la inhabilitación de los sistemas de navegación —volviéndolos ingobernables— empleando elementos autónomos no humanos, nos encontraríamos ante la necesidad de reformular la culpa tradicional y la responsabilidad internacional, atendiendo al medio digital.

Este es el razonamiento defendido por Navas Navarro, de supresión de la interpretación de culpa tradicional, en favor de la adopción «de criterios objetivos de reparto del riesgo de los posibles fallos o defectos del sistema experto» (Navas Navarro, 2017: 280), aunque esta posición serviría exclusivamente a la hora de determinar la responsabilidad por los actos producidos por un elemento no humano. El obstáculo que generan las TIC es demostrar el nexo de causalidad entre el agresor y los daños generados, por lo que al no poder precisar si nos encontramos ante un error o un verdadero acto de agresión podría conllevar a un escenario de guerra instantáneo.

Kissinger mencionaba las palabras del comandante del Ciber Comando de los Estados Unidos, el general Keith Alexander, el cual sostenía que «la próxima guerra comenzará en el ciberespacio» (Kissinger, 2016: 347). Aunque no sabemos cuál

15. Traducción del original: «A cyberoperation, or threatened cyberoperation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force».

16. David E. Sanger y Nicole Perlroth, «Estados Unidos apunta a la red eléctrica de Rusia en una guerra fría digital», *The New York Times*, 17 de junio de 2019, disponible en https://nyti.ms/3iTwECP.

17. Andy Greenberg, «The untold story of NotPetya, the most devastating cyberattack in history», *Wired*, 22 de agosto de 2018, disponible en https://bit.ly/2YNyWvO.

podría ser el motivo detonante, la velocidad que proporcionan las TIC y la presencia de componentes no humanos aumenta el riesgo de desencadenar conflictos por error. Además, en el contexto de lucha asimétrica, es previsible creer que países que no cuenten con una suficiencia física considerable incrementen su capacidad digital para compensar sus medios ofensivos ante su desproporción original, lo que les permitiría además operar en la ambigüedad, a modo de impedir —o al menos dificultar— que se sepa la procedencia de la ejecución.

Con independencia del prefijo *ciber*, una batalla a través de las TIC sería equivalente a un enfrentamiento con misiles intercontinentales, en que los contendientes pueden encontrarse separados por miles de kilómetros, pero sin que las operaciones queden limitadas a los procesos burocráticos de toma de decisiones y al tiempo de caída de un artefacto hasta su objetivo. El ritmo de la ciberbatalla lo marca la velocidad de procesamiento de unas máquinas, superiores a los humanos, más asequibles que toda la infraestructura necesaria para construir y mantener un sistema de lanzamiento de misiles balísticos.

En la Guerra Fría se partía de la premisa de que, en caso de producirse un ataque, quien comenzase el lanzamiento de armas nucleares sería quien tendría más oportunidades, frente a la parte que tuviese que soportar la agresión y preparar una contraofensiva, que de originarse sobrepasaría las facultades y medios de contención del derecho internacional. Antes de llegar a ese punto, existían canales de comunicación y un cierto tiempo de respuesta, estimado sobre la distancia que recorría un misil hasta su objetivo, en el que primaba el elemento humano frente a la máquina.[18] Hoy, en cambio, dada la rapidez de las TIC, vemos cómo progresivamente nos adentramos en la posible supresión del componente humano, lo que aumenta el riesgo de causar un ataque por error y desencadenar hostilidades no deseadas. Este es el motivo que debería hacernos pensar desde el derecho internacional sobre la necesidad de restringir el uso de *malware*, debido a la amenaza que representa para la paz mundial.

Los combatientes del siglo XXI: Una socialización de la guerra

El ciberespacio es un área que ha ganado relevancia para los Estados, dadas las implicaciones sociales, políticas y económicas que tiene este ámbito, sobre el que pueden aplicar su jurisdicción y en el cual deberían ser capaces de ejercer su poder y protección. En este sentido, la naturaleza dual de la tecnología, ambivalente a aplicaciones civiles o militares y dependiente del ejercicio del usuario, en opinión del

18. Gracias a este hecho fue que el militar soviético Stanislav Petrov impidió el comienzo de una guerra nuclear con los Estados Unidos el 26 de septiembre de 1983, al negarse a seguir el protocolo de actuación por una alerta de ataque nuclear que, como se demostró más tarde, correspondía a un fallo instrumental.

GEG, «hacen difícil la tarea de encarar las amenazas que enfrentan los Estados y otros usuarios»,[19] al poder emplearse estos sistemas «para fines tanto legítimos como malintencionados»,[20] por «la diversidad de agentes no estatales malintencionados, incluidos los grupos delictivos y los terroristas».[21]

En 2015, Estados Unidos creó el Departamento de Defensa Estratégica del Ciberespacio, y en febrero de 2016 su entonces presidente, Barack Obama, destinó un presupuesto de 19.000 millones de dólares a ciberdefensa (Burton, 2018: 12). Durante el mandato del presidente Donald J. Trump, se publicó en septiembre de 2018 la Ciberestrategia Nacional, documento en el que conscientemente se expresa cómo el ascenso de internet ha ido parejo al liderazgo de los Estados Unidos, como única superpotencia, el cual aborda el ciberespacio desde la promoción de los valores de la libertad individual, de expresión, de mercado y de la privacidad de su población para lograr la salvaguardia de la nación, la prosperidad, y el mantenimiento de la paz y seguridad de los estadounidenses.[22]

Al igual que los países han aumentado su actividad digital, otros grupos han expandido el uso de los medios que les brinda el ciberespacio, ya sea para fines pacíficos o violentos, encontrando una amalgama de usuarios entre los que se hayan activistas, terroristas y criminales, que abusan de los derechos de libertad de expresión y privacidad de las comunicaciones que amparan los regímenes democráticos liberales,[23] por el anonimato que ofrecen las redes y la capacidad que tienen para evitar, en parte, los controles gubernamentales.

19. «Grupo de Expertos Gubernamentales…», A/65/201.

20. «Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional», Asamblea General de Naciones Unidas, A/68/98, 24 de junio de 2013, disponible en https://undocs.org/es/A/68/98.

21. «Grupo de Expertos Gubernamentales sobre los Avances en la información y las Telecomunicaciones en el Contexto de la Seguridad Internacional», Asamblea General de Naciones Unidas, A/70/174, 22 de julio de 2015, disponible en https://undocs.org/es/A/70/174.

22. «National Cyber Strategy of the United States of America», The White House, septiembre de 2018, disponible en https://bit.ly/3p3nWWn.

23. La difusión de mensajes de odio ha encontrado en el ciberespacio el medio adecuado por la posibilidad de lograr el anonimato de las comunicaciones, lo que ha permitido una huida de la responsabilidad legal, como expresó la Resolución A/RES/73/157, del 17 de diciembre de 2018, con el título de «Combatir la glorificación del nazismo, el neonazismo y otras prácticas que contribuyen a exacerbar las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia», en la que se manifestaba que «observa con preocupación el uso que hacen de internet y los medios sociales los grupos neonazis para amplificar sus mensajes cargados de odio y reclutar nuevos miembros a escala internacional, si bien reconoce que internet también se puede utilizar para neutralizar a esos grupos y sus actividades». «Resolución aprobada por la Asamblea General el 17 de diciembre de 2018», Asamblea General de Naciones Unidas, A/RES/73/157, 14 de enero de 2019, disponible en https://undocs.org/es/A/RES/73/157.

Las redes virtuales privadas (VPN, por sus siglas en inglés) como Express VPN, Nord VPN o Tunnel Bear, garantizan a los usuarios recibir y enviar información a través de redes públicas como si los dispositivos estuviesen conectados a redes privadas, a través de la ocultación de la dirección IP y la encriptación de todos los datos. Aparte de las VPN, encontramos software como Psiphon o Ultrasurf, destinado a evitar la censura que se da en algunos países —como China, donde han sido declarados ilegales por ser capaces de evadir el control gubernamental—, o software como I2P o Tor, que obran igual que una VPN, pero sustentando su actuación sobre las conexiones de miles de voluntarios alrededor del mundo, que permiten que sus computadores personales sirvan de base a este sistema.

Actualmente, la visión mayoritaria tiende a menospreciar la actividad de los operadores no estatales, al considerar que su motivación se limita al lucro, la vigilancia y las protestas, negando su ánimo de combate (Burton, 2018: 15). Esta concepción es errónea, en la medida en que el combate no se limita a la agresión de infraestructuras. Ante situaciones de conflicto social, caracterizadas por el estado asimétrico en que estas se originan, encontramos operaciones de guerrilla informativa o *netwar*, en las que, por medio de la difusión de contenidos a través de la TIC, se busca la supremacía sobre los enemigos, refutando las ideas y opiniones que estos sostienen sobre una cuestión concreta (Carvalho y Esteban Navarro, 2012: 85).

Podrían encuadrarse este tipo de comportamientos dentro de las tácticas de decepción, en las que, por medio de la difusión de comunicaciones que ofrecen una imagen deformada de la realidad, se persigue perjudicar los intereses del contrario (Arcos Martín, 2012: 427), como han puesto de manifiesto en los últimos años el fenómeno de las *fake news* (noticias falsas que provienen de fuentes sin credibilidad ni contrastables).

Ejemplo de este tipo de técnicas fue la alteración en 2006 de unas imágenes con el programa de diseño Photoshop por un fotógrafo partidario de la organización terrorista Hezbolá, tras un ataque realizado por fuerzas israelíes, para simular unos daños superiores a los realmente producidos y causar la pérdida de apoyo público hacia los hebreos (Cahanin, 2012). También cabe la posibilidad de que tales acciones de divulgación se ejecuten junto con ataques contra sistemas para comprometer las fuerzas del contrario, a fin de operar como elementos desestabilizadores.

Así ocurre con el *doxing* o difusión pública de información privada, con la finalidad de causar oprobio sobre una persona o institución, cuya práctica no está prohibida en el derecho internacional por no alcanzar «el umbral del uso de la fuerza» (Sánchez de Rojas Díaz, 2018). Pensemos los efectos que podría tener una campaña de esta naturaleza contra un país que no disponga de medios de defensa suficientes, y tenga que afrontar un hackeo masivo de cuentas, ataques de sus páginas web, sus sistemas gubernamentales y de sus infraestructuras críticas.

Es el caso de la política adoptada por Rusia tras su intervención en Ucrania, don-

de desplegó su actividad digital mediante la filtración de una conversación sensible entre la asistente del secretario de Estado para Europa y el embajador estadounidense en Kiev; la difusión de noticias falsas internacionalmente que favorecían su labor en el conflicto; y el sabotaje de una central eléctrica en Ucrania.[24]

En ocasiones, el peligro que entraña el ataque contra una infraestructura crítica es que los efectos sobrepasen al objetivo —dañando a otros Estados— y que el elemento empleado caiga en poder de sujetos ajenos a las ciberoperaciones. Fue lo acontecido con el programa Stuxnet, que en su versión original consiguió extenderse a más de 100.000 ordenadores fuera de Irán, y cuyo código en la actualidad es empleado en nuevas variantes (Burton, 2018: 7), las que no necesariamente tienen por qué ser operadores estatales. Estos supuestos constituyen una socialización de la guerra, en el sentido de que son accesibles a individuos —con una determinada capacidad de acción— y los dota de una facultad destructiva tradicionalmente reservada a los Estados, con lo que rompe así el paradigma del monopolio estatal del uso de la fuerza.

Por un uso responsable del ciberespacio

El Estado es el poder, pero debe restringirse su uso despótico, pues si atendemos al preámbulo de la Declaración Universal de los Derechos Humanos, su respeto debe garantizarse «a fin de que el hombre no se vea compelido al supremo recurso de la rebelión contra la tiranía y la opresión», lo cual habría de ser visto como una reiteración de la libertad a la que aludía Stuart Mill (2017: 68) cuando decía que «el fin de los patriotas era fijar los límites del poder que al gobernante le estaba consentido ejercer sobre la comunidad».

Para evitar el surgimiento de patriotas que luchan contra el poder omnímodo, es necesaria la transparencia y la diligencia en el obrar gubernamental —incluido el ciberespacio— tratando de que no se inmiscuya y prive de libertad a sus ciudadanos y de que en el terreno del debate la mentira no se imponga como vencedora en perjuicio de las instituciones.

Sería preciso acomodar, atendiendo al símil que representa el espacio sideral, el planteamiento adoptado por la Resolución A/RES/73/72, del 13 de diciembre de 2018, sobre «Medidas de transparencia y fomento de la confianza en las actividades relativas al espacio ultraterrestre», a fin de lograr implementar estos sistemas en el ciberespacio y evitar los riesgos que provoca su perdida en la población.

En el mismo sentido, la Resolución A/RES/73/72 hace alusión al proyecto adoptado por la Unión Europea, de código de conducta internacional sobre las actividades que se realizan en el espacio ultraterrestre, que podría ser empleado análogamente,

24. Andrei Soldatov, «Cyber showdown: How Russian Hacking Works», *Foreign Affairs*, 31 de julio de 2016, disponible en https://fam.ag/3pjBQnA.

atendiendo a la realidad del ciberespacio. Sintetizando el contenido del documento de conclusiones del Consejo del 27 de septiembre de 2010 relativos a este proyecto,[25] podrían obtenerse los principios que deberían ser tenidos en cuenta, con la intención de aumentar la protección y la sostenibilidad de todas las actividades en el ciberespacio, mediante la aplicación de medidas de fomento de transparencia y confianza, debido al reconocimiento de la libertad de los Estados y de todos sus ciudadanos de acceder al ciberespacio, explorarlo y utilizarlo, con fines pacíficos, respetando plenamente la seguridad y la integridad de las infraestructuras; el derecho inmanente a la legítima defensa, individual o colectiva, acorde al sistema de Naciones Unidas; y la responsabilidad de los países en su actuación conforme a la buena fe, y en la ejecución de actividades científicas, comerciales y militares en el ciberespacio, evitando que se convierta en un escenario de disputas.

En la situación de enfrentamiento asimétrico y de constitución de la zona gris generada en las últimas décadas, los actores contrarios a un determinado poder pueden servirse del ciberespacio para sus operaciones, ya sea limitando su proceder al espacio digital —como sería a través de la difusión de contenidos privados o falsos—, pero, en todo caso, con la meta de provocar consecuencias en el mundo material, organizando personas o atacando infraestructuras. En este escenario es preciso identificar, de acuerdo con el derecho humanitario, qué categorías de sujetos se reconocen en las hostilidades.

Viejos actores, nuevos escenarios

En los enfrentamientos armados se distinguen tres elementos: combatientes, objetivos militares, y medios y métodos para alcanzarlos (Doménech Omedas, 2017: 175). Según lo dispuesto en los Protocolos Adicionales a los Convenio de Ginebra del 12 de agosto de 1949, el *combatiente* es el miembro de las fuerzas armadas que tiene derecho de atacar al adversario por cumplir con el siguiente requisito contenido en su artículo 43.1: «Estar sometidos a un régimen de disciplina interna que haga cumplir, *inter alia*, las normas de derecho internacional aplicables en los conflictos armados». A su vez, su artículo 43.3, admite la incorporación a las fuerzas armadas «de un organismo paramilitar o un servicio armado encargado de velar por el orden público», siempre que se notifique a las otras partes en conflicto.

La reinterpretación normativa plantea la duda sobre si estos cometidos podrían aplicarse hoy a empresas prestadoras de servicios de ciberseguridad, o a profesionales independientes dotados de este tipo de conocimientos, siempre que en su actuación se encuentren integrados en la disciplina interna de unas fuerzas armadas.

25. Consejo de la Unión Europea, «Conclusiones del Consejo sobre el proyecto revisado de Código de Conducta para las actividades en el espacio ultraterrestre», Bruselas, 11 de octubre de 2010, disponible en https://bit.ly/3nplWFA.

Como explica Laborie Iglesias (2017: 205), una empresa militar y de seguridad privada es una «entidad corporativa, con ánimo de lucro y legalmente establecida, que proporciona, de forma abierta y mediante contrato, servicios ligados, directa o indirectamente, al uso de la fuerza armada a un número amplio de clientes, tanto de carácter público como privado». Nos encontramos así con la figura del *contratista*, el profesional que, en este caso, pone a disposición de otro su conocimiento y capacidad de emplear la fuerza armada en virtud de un contrato, un hecho que, en opinión de Laborie Iglesias (2017: 206), ha sido visto como «una variación contemporánea de los tradicionales mercenarios».

Mercenarios y contratistas en ciberoperaciones

La definición de *mercenario* la encontramos en los artículos 1.1 y 1.2 de la Convención Internacional contra el reclutamiento, la utilización, la financiación y el entrenamiento de mercenarios, del 4 de diciembre de 1989.[26] El Grupo de Trabajo de la ONU sobre Mercenarios y su relator especial han expresado la necesidad de revisar este concepto a fin de adaptarlo a las nuevas formas de actividad mercenaria,[27] un reflejo del cambio de paradigma en los conflictos como consecuencia del ejercicio del uso de la fuerza por actores privados, como las empresas militares o de seguridad privada,[28] frente al tradicional monopolio estatal; y a fin de distinguirlo de nuevos fenómenos, como la figura de los combatientes terroristas extranjeros, recogidos en la Resolución 2.178 (2014) del Consejo de Seguridad de la ONU.[29]

26. Artículo 1.1: «Se entenderá por mercenario toda persona: a) que haya sido especialmente reclutada, localmente o en el extranjero, para combatir en un conflicto armado; b) que tome parte en las hostilidades animada esencialmente por el deseo de obtener un provecho personal y a la que se haga efectivamente la promesa, por una parte en conflicto o en nombre de ella, de una retribución material considerablemente superior a la prometida o abonada a los combatientes de grado y funciones similares en las fuerzas armadas de esa parte; c) que no sea nacional de una parte en conflicto ni residente en un territorio controlado por una parte en conflicto; d) que no sea miembro de las fuerzas armadas de una parte en conflicto; y e) que no haya sido enviada en misión oficial como miembro de sus fuerzas armadas por un Estado que no sea parte en conflicto». Artículo 1.2: «Se entenderá también por mercenario toda persona en cualquier otra situación: a) que haya sido especialmente reclutada, localmente o en el extranjero, para participar en un acto concertado de violencia con el propósito de: i) derrocar a un gobierno o socavar de alguna otra manera el orden constitucional de un Estado, o de, ii) socavar la integridad territorial de un Estado».

27. «Working Group on the use of mercenaries», Oficina del Alto Comisionado de Naciones Unidas para los derechos humanos, disponible en https://bit.ly/3jvwQIv.

28. Consejo de Derechos Humanos, A/HRC/42/42: «Entidad empresarial que presta servicios militares y/o de seguridad remunerados por medio de personas físicas y/o personas jurídicas».

29. «Los combatientes terroristas extranjeros, a saber, personas que viajan a un Estado distinto de su Estado de residencia o nacionalidad con el propósito de cometer, planificar o preparar actos terroristas o participar en ellos, o de proporcionar o recibir adiestramiento con fines de terrorismo, incluso en

Las características reconocidas en el plano internacional sobre los mercenarios les vuelven prácticamente indistinguibles de los contratistas, al tratarse de profesionales cuya motivación de ejercer la fuerza responde al interés pecuniario. Si nos limitamos a destacar el ánimo económico, nos encontramos con la advertencia que hacía Maquiavelo (2016: 97), contrario al empleo de mercenarios, al estar movidos exclusivamente por el afán de lucro, deduciéndose como expresaba el autor que «no puede haber buenas leyes donde no hay buenos ejércitos, y donde hay buenos ejércitos conviene que haya buenas leyes».

La legalidad va a ser el elemento determinante en que radica la diferencia entre ambas figuras, en tanto que deberá considerarse contratista cuando el profesional contratado para ejercer cometidos armados: se integre dentro de la fuerza armada de alguna de las partes en conflicto —siempre que se notifique a las contrapartes—; o sea miembro de una misión oficial de otro país aunque no sea uno de los beligerantes —si no existe una promesa lucrativa de acuerdo con el resultado de la contienda—; y si su contratación no tiene como finalidad derrocar un gobierno o socavar el orden constitucional o territorial de un Estado. Así, en todos estos casos, el contratista habrá de ser calificado de combatiente, y contará con la protección de los derechos que le reconoce el derecho internacional humanitario.

En el plano digital, los contratistas no son reconocidos por el Manual de Tallin, cuya única alusión es a los mercenarios, como dispone en su regla 28, al decir: «Los mercenarios involucrados en ciberoperaciones no disfrutan de la inmunidad del combatiente o del estatus de prisionero de guerra».[30]

Desde el momento en que se permite el uso de una fuerza armada privada que cumpla con la legalidad vigente, encontramos válido el uso de *cibercontratistas*, por evitar el peyorativo *cibermercenario*, al tratarse de una externalización de los servicios del Estado, quien no necesariamente ha de poseer el conocimiento y los profesionales adecuados con que afrontar las amenazas del ciberespacio; situación en la que debería exclusivamente determinarse sobre quién recae la responsabilidad por la actuación perjudicial de este tipo de profesionales.

De acuerdo con la exposición de Domínguez Bascoy (2017: 628), para atribuir una ciberoperación a un Estado, sería necesario que este tuviese «un genérico control estatal» cuando los actores «formen parte de un grupo organizado», o «un control efectivo sobre todas y cada una de las ciberoperaciones realizadas por esos actores no estatales». El marco de referencia a este argumento se encuentra en la actividad del Tribunal Internacional de Justicia con los asuntos *Nicaragua,* de 1986, y *Aplicación de la Convención sobre el genocidio*, de 2007, que establecen que en la determinación

relación con conflictos armados, y decidido a hacer frente a esa amenaza».

30. Traducido por el autor del original: «Mercenaries involved in cyberoperations do not enjoy combatant immunity or prisoner of war status».

de la responsabilidad del Estado no basta con que exista una «situación general de dependencia y apoyo», sino que debe demostrarse que tiene el control efectivo sobre cada una de las operaciones realizadas por individuos o grupos organizados (Diez de Velasco Vallejo, 2013: 856).

Actores no estatales: Delincuencia organizada y terrorismo

La problemática de las ciberoperaciones radica en su original ambigüedad, una extensión de la zona gris al marco digital, ya que en ocasiones las acciones de las partes en conflicto no se limitan a la agresión, sino que pueden manifestarse en otras intervenciones, como serían las labores de inteligencia.

Sun Tzu decía:

> Lo crucial es extraer información de alguien que lo conozca desde adentro […] entre las tropas nadie es más preciado que un espía, nadie es mejor recompensado que un espía, nada es más secreto que el espionaje […] ¡el espionaje es omnipotente y omnipresente! (Sun Tzu, 2017: 75-76).

Por lo tanto, las operaciones cibernéticas podrían incurrir en actividades ilegales, al estar destinadas a explotar la vulnerabilidad de instituciones, organizaciones, empresas o sujetos, con objeto de promover chantajes en perjuicio del enemigo, debido a la monitorización de su actividad en el medio digital, encontrándonos adicionalmente con acciones de piratería, secuestro digital, etcétera.

Se muestra una situación en la que el desarrollo tecnológico pone en riesgo la libertad y la privacidad de los individuos. Estas conclusiones son sostenidas en la Resolución A/RES/73/179, del 21 de enero de 2019, sobre «El derecho a la privacidad en la era digital», al reconocer que

> el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar las nuevas tecnologías de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos […] las violaciones y las transgresiones del derecho a la privacidad en la era digital pueden afectar a todos los individuos y tener repercusiones particulares en las mujeres, así como los niños y las personas vulnerables y marginadas […] reconociendo que el ejercicio del derecho a la privacidad es importante para materializar el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y de asociación pacíficas, y es una de las bases de una sociedad democrática.

Comprobamos cómo la democracia descansa sobre la libertad y la privacidad de las personas, razón por la cual desde la Resolución A/RES/73/179 se recuerda que

cualquier injerencia contra estos derechos debe responder a razones de legalidad, necesidad y proporcionalidad. La dificultad en llevar a la práctica estas medidas reside en la falta de homogeneidad ante la adopción de la democracia y el respeto de los derechos humanos en el mundo, la ausencia de transparencia en las ciberoperaciones y el ser una actividad que no se limita a los actores estatales, lo que hace que el ciberespacio pueda dar lugar a una socialización de la guerra, al facilitar la intervención de civiles en conflictos bélicos por estos medios.

Por otra parte, actuaciones cuya ilicitud es incuestionable hallan acomodo entre grupos que no responden a ninguna misión estatal y solo persiguen el lucro personal, comenzando así un deslizamiento hacia un espacio confuso, profuso y difuso, en cuyo estrato más bajo se encuentran aquellos elementos que, fuera de la ley, amenazan el orden existente: las organizaciones terroristas y delincuenciales. Se trata de categorías cuyos límites se entremezclan habitualmente, y cuyas operaciones pueden ser apoyadas por Estados, con la finalidad de debilitar y desestabilizar a posibles adversarios.

Naciones Unidas es consciente de los recursos que otorgan el ciberespacio a estos grupos, como se aprecia en la Resolución A/RES/73/218, sobre «Las tecnologías de la información y las comunicaciones para el desarrollo sostenible»:

> Consciente de las dificultades que afrontan los Estados en la prevención y lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos, incluso por terroristas, y haciendo hincapié en la necesidad de proseguir la cooperación internacional a este respecto y fortalecer las actividades de asistencia técnica y desarrollo de la capacidad, a solicitud de los interesados, para prevenir, enjuiciar y castigar dicho uso con arreglo al derecho nacional e internacional.

Esto ha motivado la aprobación de distintas resoluciones de la Asamblea General, dirigidas a suprimir estas vías en perjuicio de los grupos al margen de la ley que se sirven de las TIC para difundir sus ideales, captar nuevos adeptos y recaudar fondos para sus causas. Así, la Resolución A/RES/73/157, del 17 de diciembre de 2018, sobre «Combatir la glorificación del nazismo, el neonazismo y otras prácticas que contribuyen a exacerbar las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia», dispone que

> los grupos que propagan el odio se valen de las plataformas en internet para planificar, recaudar fondos, hacer circular información sobre actividades públicas, como mítines, manifestaciones actos de violencia, encaminadas a promover el racismo, la xenofobia las formas conexas de intolerancia.

En el mismo sentido encontramos la Resolución A/RES/73/174, del 17 de diciembre de 2018, sobre «Terrorismo y derechos humanos», la cual

> exhorta a los Estados a que se abstengan de prestar apoyo a entidades o personas involucradas en actos terroristas, incluido el apoyo para el establecimiento de pla-

> taformas de propaganda que hagan apología del odio que constituya incitación a la discriminación, la hostilidad o la violencia, a través de internet o por cualquier otro medio […] Exhorta a los Estados miembros a que se mantengan alerta ante el uso de las tecnologías de la información y las comunicaciones con fines terroristas y a que cooperen con el fin de prevenir y contrarrestar la propaganda extremista violenta y la incitación a la violencia en internet y los medios sociales.

Junto con estas medidas, volvemos a abordar la problemática en el planteamiento de armas de destrucción en masa. El potencial aniquilador de estos artefactos y la incertidumbre de que lleguen a manos de grupos fuera de la ley comprende un motivo de preocupación para los Estados, razón por la que desde Naciones Unidas se han creado instrumentos como la Resolución A/RES/73/55, sobre «Medidas para evitar la adquisición por terroristas de armas de destrucción en masa», en la que se reconoce la necesidad de cooperación internacional para evitar que los terroristas puedan obtenerlas; o la Resolución A/RES/73/74, sobre «Consecuencias humanitarias de las armas nucleares», en que se muestra la conciencia en torno a la imposibilidad de «hacer frente adecuadamente a los catastróficos efectos de la detonación de un arma nuclear, que se produzca por accidente, por error de cálculo o deliberadamente», y que podría hacerse extensible a cualquier infraestructura crítica que, de ser atacada, provocaría la devastación de una región, como ocurre respecto de una central nuclear.

Desde el plano internacional, se sostiene la restricción del concepto de *arma de destrucción masiva* a los elementos NBQ, ignorando las posibilidades destructivas de un *malware*, que podría desencadenar efectos como los experimentados con accidentes nucleares, atentados como el 11 de septiembre de 2001 o derrames petrolíferos, en caso de que se manipule una central nuclear, una aeronave o una embarcación petrolera[31] (sin omitir los efectos económicos ante un atentado contra el sistema financiero, bancario, empresarial, etcétera).

Teniendo en cuenta la fragilidad y complejidad de nuestro sistema, debemos pensar en las consecuencias que podría causar un ataque con *malware*, dado el nivel de interconexión existente, que llegaría a todos los estratos y sectores de la sociedad. Para ello, el ejemplo del alcance por la difusión de un agente biológico serviría de enseñanza por analogía respecto de cuáles podrían ser los resultados de la propagación de un *malware*.

31. Se ha demostrado cómo es posible acceder a los sistemas de control de aeronaves como el Boeing 787 Dreamliner, o los Airbus 350 y 380, gracias a que disponen de red wifi para sus pasajeros. Por este motivo, podría hacerse extensible la amenaza del control remoto a cualquier infraestructura, aeronave, embarcación o sistema de armas tradicional, cuyos elementos de gobierno estén conectados al mundo vía internet. Kim Zetter, «Hackers could commandeer new planes through passenger wi-fi», *Wired*, 15 de abril de 2015, disponible en https://bit.ly/3jwhunq.

Prepararse ante lo imprevisible

El 22 y 23 de junio de 2001, el Johns Hopkins Center for Civilian Biodefense Strategies, en colaboración con el Center for Strategic and International Studies, el Analytic Services Institute for Homeland Security y el Oklahoma National Memorial Institute for the Prevention of Terrorism, llevaron a cabo un ejercicio conocido como Dark Winter (invierno oscuro), que simulaba un ataque con viruela en los Estados Unidos, para averiguar los desafíos a que se enfrentarían las instituciones del Estado en caso de un ataque bioterrorista. O'Toole, Mair e Inglesby (2002: 972-983), considerando la información obtenida en el ejercicio, identificaron la falta de planificación existente en la clase política y el sistema sanitario estadounidense, la ausencia de unidad de objetivos entre la administración federal y estatal, y la importancia de preparar a la población para afrontar una epidemia.

Los efectos de un ciberataque, a diferencia de un ataque bacteriológico, no entrañan riesgo de trasmisión entre las personas, pero sus consecuencias, que podrían llevar a una inoperatividad de cualquier sistema que se encontrase conectado a internet, la pérdida, sustracción o secuestro de datos, conforman una amenaza a la salvaguardia del Estado. Del ejercicio Dark Winter podríamos obtener las siguientes conclusiones en caso de producirse un ciberataque:

- Los líderes no están familiarizados con el carácter de los ciberataques, las opciones políticas disponibles y sus consecuencias.
- Después de un ciberataque, las decisiones de los líderes dependerían de los datos y la experiencia de los sectores de ciberseguridad pública y privada.
- La falta de medios para prevenir la propagación del *malware* limita severamente las opciones de manejo de un ciberataque.
- Para poner fin a los efectos de un ciberataque, los responsables de la toma de decisiones requerirán del asesoramiento continuo de expertos de ciberseguridad de alto nivel.
- Las prioridades federales y estatales pueden no ser claras, diferir o entrar en conflicto, las autoridades pueden ser inciertas, y pueden surgir problemas constitucionales.
- Las acciones individuales de los ciudadanos serán fundamentales para poner fin a la propagación de *malware*; los líderes deben ganarse la confianza y la cooperación sostenida del pueblo.

Al igual que en cualquier ámbito que implique un cierto grado de conocimiento técnico, los líderes políticos necesitan asesores que les permitan suplir su ignorancia y carencias sobre asuntos a tratar, y les sirvan de apoyo en la toma de decisiones.

La ciberseguridad es un campo que implica a la esfera pública y privada, por lo que se necesita tener órganos que garanticen una comunicación entre los expertos de ambos sectores, una delimitación de las competencias estatales y federales cuando corresponda, sistemas para lograr la comunicación y colaboración de la ciudadanía —y su responsabilización a la hora de mantener actualizados los equipos y contar con copias de seguridad diarias— y, en cualquier caso, cada país debería preguntarse si dispone de los medios para afrontar un ciberataque, tanto en su contención como en la anulación de sus posibles efectos; hechos que han sido evidenciados globalmente con las consecuencias de la pandemia de covid-19 en 2020, que demostró la falta de preparación de los gobiernos ante una situación que ha desbordado sus sistemas de contingencia, razón que exige prever la resiliencia estatal contra ciberamenazas, por analogía a lo acontecido con una amenaza biológica.

Otro aspecto que debe ser atendido, extraíble del razonamiento de la Resolución A/RES/77/66, sobre «Prevención de la adquisición de fuentes radioactivas por terroristas», es la necesidad por los Estados de restringir el desarrollo y producción de *malware*, y los controles de su acceso, para evitar su uso por organizaciones criminales o terroristas.

A pesar de ser medios inocuos físicamente, en comparación al material nuclear y radiactivo, son de igual modo destructivos, sin que estén sometidos a control reglamentario, lo que posibilita que sean objeto de tráfico comercial, razones por las que se observa la importancia de una mayor transparencia en las actividades digitales para generar confianza, no solo en las relaciones internacionales, sino en la población, por ser esta el alfa y el omega de la democracia y los derechos humanos.

Consideraciones finales

La porosidad de las fronteras y el anquilosamiento de las instituciones precisan el desarrollo de mecanismos que permitan trascender a los tradicionales anclajes nacionales, y responder a las necesidades y demandas de la ciudadanía global, presentándose el ciberespacio como un medio que requiere de esta atención.

La democracia y los derechos humanos se muestran vulnerables en un sistema que consiente operaciones de desprestigio de las instituciones, y de elementos subversivos contrarios al sistema; por lo que es indispensable una mayor transparencia y supervisión de las acciones llevadas a cabo en el mundo digital, para impedir violaciones sobre la libertad y privacidad de las personas, y evitar el aprovechamiento de la ambigüedad de dicho medio para cometer actos que puedan ser contrarios a la vida. De igual forma, la colaboración y cooperación en materia policial y judicial entre los Estados es vital para impedir que los grupos transnacionales que operan al margen de la ley se sirvan de la opacidad digital para difundir su mensaje, ganar adeptos y atacar el sistema.

El mundo digital compone un espacio en el que las labores de defensa, policía e inteligencia se encuentran combinadas, por lo que, dada su complejidad, se requiere revisar conceptos como el de *contratista*, a fin de dotar con seguridad jurídica a los profesionales de la ciberseguridad, permitiendo distinguirlos de otros sujetos, como los *mercenarios*, que son empleados con la finalidad de eludir la aplicación del derecho.

Es necesario revisar el concepto de *arma de destrucción masiva*, a fin de hacerlo extensible a los sistemas digitales, y comenzar a reflexionar sobre la existencia de ciberarmas de destrucción masiva. Vivimos una situación de laguna legislativa, que faculta a todos los interesados a desencadenar elementos capaces de crear riesgo para el orden público internacional, sin que estén sujetos a ningún tipo de control, tanto en los fines con que son creados, como en su distribución.

Para limitar la existencia de las armas de destrucción masiva de las TIC, se requeriría de tratados formulados para restringir la producción y distribución de tales sistemas, a imagen y semejanza de los tratados de no proliferación nuclear, pero sin abordar cuestiones como el despliegue de estas armas —al no requerir de una distribución física— o sus ensayos —pese a que se sucediesen en circunstancias controladas—.

Ante la inexistencia de un documento que contenga estos lineamientos, queda a la sensatez de los países con capacidad de generar estos elementos el dotarse de protección interna que impida su crecimiento y uso pernicioso, prohibiendo el acceso a todos aquellos grupos que buscan causar daños en la población.

La realidad superará de manera inmediata las conclusiones de este estudio, confirmando la lentitud del legislador frente a la evolución tecnológica, pero hay una afirmación que no debe ser olvidada y con la que concluye el presente trabajo: no se puede suprimir el elemento humano de cualquier cadena de toma de decisiones, pues siempre habrá de ser una persona el responsable último de cualquier acción que se ejecute en el ciberespacio.

Referencias

Arcos Martín, Rubén (2012). «Comunicación, cultura y reserva de inteligencia». En José Luis González Cussac (coordinador), *Inteligencia* (pp. 411-462). Valencia: Tirant lo Blanch.

Aznar Fernández-Montesinos, Federico (2011). *La ecuación de la guerra.* Barcelona: Ediciones de Intervención Cultural/Montesinos.

Baqués Quesada, Josep (2018). «La versión china de la zona gris». *Revista General de Marina*, 275: 557-564. Disponible en https://bit.ly/3ntkou6.

Barrio Andrés, Moisés (2018). *Ciberderecho.* Valencia: Tirant lo Blanch.

Bryant, William D. (2013). «Cyberspace superiority». *Air & Space Power Journal,* 27 (6): 25-44. Disponible en https://bit.ly/2Zi5s9Y.

Burton, Joe (2018). «Cyber deterrence: A comprehensive approach?». NATO Cooperative Cyber Defence Centre of Excellence. Disponible en https://bit.ly/2Zfxm6m.

Cahanin, Steven E. (2012). *Principles of war for cyberspace*. Alabama: Air War College.

Carvalho, Andrea V. y Miguel A. Esteban Navarro (2012). «Los servicios de inteligencia: Entorno y tendencias». En José Luis González Cussac (coordinador), *Inteligencia* (pp. 73-109). Valencia: Tirant lo Blanch.

Casanova, Oriol y Ángel J. Rodrigo (2016). *Casos y textos de derecho internacional público.* Madrid: Tecnos.

Chairman of the Joint Chiefs of Staff (2006). *The national military strategy for cyberspace operations.* Washington D. C.

Diez de Velasco Vallejo, Manuel (2013). *Instituciones de derecho internacional público*. Madrid: Tecnos.

Doménech Omedas, José Luis (2017). «Los sujetos combatientes». En José Luis Rodríguez-Villasante y Prieto y Joaquín López Sánchez, *Derecho internacional humanitario* (pp. 175-204). Valencia: Tirant lo Blanch.

Domínguez Bascoy, Jerónimo (2017). «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio». En José Luis Rodríguez-Villasante y Prieto y Joaquín López Sánchez, *Derecho internacional humanitario* (pp. 621-646). Valencia: Tirant lo Blanch.

Jordán, Javier (2018). «El conflicto internacional en la zona gris: Una propuesta teórica desde la perspectiva del realismo ofensivo». *Revista Española de Ciencia Política*, 48: 129-151. DOI: 10.21308/recp.48.05.

Kissinger, Henry (2016). *Orden mundial.* Ciudad de México: Debate.

Laborie Iglesias, Mario (2017). «Empresas militares y de seguridad privadas». En José Luis Rodríguez-Villasante y Prieto y Joaquín López Sánchez, *Derecho internacional humanitario* (pp. 205-220). Valencia: Tirant lo Blanch.

Liivoja, Rain, Maarja Naagel y Ann Väljataga (2019). «Autonomous cyber capabilities under international law». NATO Cooperative Cyber Defence Centre of Excellence. Disponible en https://bit.ly/2ZkmDIp.

Maquiavelo, Nicolás (2016). *El príncipe.* 3.ª ed. Ciudad de México: Planeta.

Martín Serrano, Manuel (2008). *La mediación social.* Madrid: Akal.

Mattis, James N. y Frank Hoffman (2005). «Future warfare: The rise of hybrid wars». *US Naval Institute*, 132/11/1.233.

Mazanec, Brian M. (2015). «Why international order in cyberspace is not inevitable». *Strategic Studies Quarterly,* 9 (2): 78-98. Disponible en https://www.jstor.org/stable/26271076.

Mazanec, Brian M. y Bradley A. Thayer (2015). *Deterring cyber warfare: Bolstering strategic stability in cyberspace*. Nueva York: Palgrave Macmillan.

Melzer, Nils (2011). «Cyberwarfare and international law». UNIDIR Resources. Disponible en https://bit.ly/3mdbNwe.

Navas Navarro, Susana (2017). «Conclusiones». En Susana Navas Navarro (directora), *Inteligencia artificial* (pp. 279-292). Valencia: Tirant lo Blanch.

Ortega Carcelén, Martín (2017). *Derecho global.* Madrid: Tecnos.

O'Toole, Tara, Michael Mair y Thomas V. Inglesby (2002). «Shining light on Dark Winter». *Clinical Infectious Diseases,* 34 (7): 972-983. DOI: 10.1086/339909.

Pastor Ridruejo, José Antonio (2016). *Curso de derecho internacional público y organizaciones internacionales*. Madrid: Tecnos.

Pérez González, Manuel (2017a). «El derecho internacional humanitario frente a la violencia bélica: Una apuesta por la humanidad en situaciones de conflicto». En José Luis Rodríguez-Villasante y Prieto y Joaquín López Sánchez, *Derecho internacional humanitario* (pp. 25-52). Valencia: Tirant lo Blanch.

—. (2017b). «Fundamentos del derecho internacional humanitario». En José Luis Rodríguez-Villasante y Prieto y Joaquín López Sánchez, *Derecho internacional humanitario* (pp. 77-118). Valencia: Tirant lo Blanch.

Rodríguez-Villasante Prieto, José Luis (2017). «El arma nuclear y el derecho internacional humanitario». En José Luis Rodríguez-Villasante y Prieto y Joaquín López Sánchez, *Derecho internacional humanitario* (pp. 579-600). Valencia: Tirant lo Blanch.

Sánchez de Rojas Díaz, Emilio (2018). «El *soft power* en las guerras de información: Las operaciones de influencia de grandes potencias». Instituto Español de Estudios Estratégicos. Disponible en https://bit.ly/3bobfO5.

Schmitt, Michael N. (2013). *Tallinn manual on the international law applicable to cyber warfare.* Cambridge: Cambridge University Press.

—. (2017). *Tallinn manual 2.0. on the international law applicable to cyber operations.* Cambridge: Cambridge University Press.

Stuart Mill, John (2017). *Sobre la libertad*. 3.ª ed. Madrid: Alianza.

Sun Tzu (2017). *El arte de la guerra.* Ciudad de México: Mirlo.

Sobre el autor

Borja García Vázquez es abogado. Doctor en Métodos Alternos de Solución de Conflictos de la Universidad Autónoma de Nuevo León, México. Profesor de Derecho Internacional Público de la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León. Investigador nivel 1 del Sistema Nacional de Investigadores, México. Su correo electrónico es bgarciav@uanl.edu.mx. http://orcid.org/0000-0003-0055-6917.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).