DOI: http://dx.doi.org/10.20983/reij.2022.2.9

Mariano César Bartolomé[11]

Fecha de recepción: 20 de julio de 2021
Fecha de aceptación: 23 de agosto de 2021

LA INSTITUCIONALIDAD LIMITADA EN EL CAMPO DE LA CIBERSEGURIDAD Y EL CASO DE LA CIBERGUERRA

Limited institutional framework in the field of cybersecurity and the case of cyberwarfare

Resumen

En el presente trabajo se aborda la cuestión de la ciberseguridad, una disciplina que atiende las amenazas que surgen y se despliegan en el "quinto dominio" o ciberespacio. Su objetivo principal consiste en determinar si en esta cuestión de tanta importancia dentro de la agenda de la Seguridad Internacional contemporánea, la comunidad internacional ha desarrollado instituciones que permitan alcanzar acuerdos y reducir los niveles de conflictividad. Desde el punto de vista metodológico, se utilizó un abordaje lógico deductivo, el análisis fluctuó entre los niveles descriptivo y explicativo, y se utilizó información cualitativa obtenida de fuentes secundarias. El trabajo permitió identificar los aspectos centrales de la ciberseguridad, su grado de institucionalidad desde el punto de vista teórico de las relaciones internacionales y, finalmente, la situación de un área específica de la ciberseguridad: la ciberguerra. Se concluye que el grado de institucionalización en materia de ciberseguridad, en el plano internacional, es limitado. No existe una convención multilateral que aborde el tema de manera integral y se articulan mecanismos alternativos de gobernanza para mejorar la situación en diferentes aspectos de esa cuestión. En el caso de la ciberguerra, la utilidad de los mecanismos de gobernanza es controversial, pues no resulta claro si son empíricamente aplicables los consensos alcanzados en el plano nominal.

Palabras clave: ciberespacio; ciberguerra; ciberseguridad; gobernanza.

Abstract

This paper addresses the issue of cybersecurity, a discipline focused on the threats that arise and unfold in the "fifth domain" or cyberspace. Its main objective is to determine whether the international community has developed institutions that make it possible to reach agreements and reduce the levels of conflict in this important issue on the contemporary International Security agenda. From a methodological point of view, a logical deductive approach was used, the analysis was developed at the descriptive and explanatory levels, and qualitative information obtained from secondary sources was used. The article made it possible

1 Profesor investigador del Colegio Interamericano de Defensa, Washington, EE. UU.; marianobartolome@yahoo.com.mx. ORCID: 0000-00026409-0880.

to identify the central aspects of cybersecurity, its degree of institutionalization from the perspective of the Theory of International Relations, and finally the situation of a specific area of cybersecurity: cyberwarfare. It is concluded that the degree of institutionalization of cybersecurity at the international level is limited. There is no multilateral convention that addresses the issue in a comprehensive manner and alternative governance mechanisms are articulated to improve the situation in different aspects of this issue. In the case of cyberwarfare, the usefulness of governance mechanisms is controversial as it is unclear whether the consensus reached at the nominal level is empirically applicable.

Keywords: cybersecurity; cyberspace; cyberwarfare; governance.

Introducción

El sostenido avance de las tecnologías de la información y la comunicación (TIC), a lo largo de las últimas décadas, ha posibilitado la constitución y consolidación del ciberespacio, entendido como un entorno virtual de información e interacción entre las personas. En este dominio hoy participa cotidianamente más del 60 % de la población mundial, desplegando un heterogéneo listado de actividades que afectan casi todas las facetas de la interacción social. Entre esos aspectos, se incluye el de la seguridad; de hecho, las cuestiones de seguridad ocupan un lugar particularmente relevante en el ciberespacio, configurando el campo de la ciberseguridad, que puede ser entendido preliminarmente como el área de los estudios de seguridad que refiere a las amenazas y riesgos que se despliegan en ese entorno cibernético.

Con este contexto, el objetivo principal del presente trabajo consiste en señalar el limitado grado de institucionalización existente en materia de ciberseguridad en el plano internacional. Es decir, la sociedad global se enfrenta a una situación signada por la ausencia de un acuerdo multilateral amplio, en el sentido de una convención o tratado integral y comprehensivo, para hacer frente a los principales riesgos y amenazas en el dominio cibernético; sin embargo, esa ausencia ha motivado la constitución de mecanismos alternativos de gobernanza para mejorar la situación en diferentes aspectos de esa cuestión.

A partir de las metas identificadas, este trabajo se estructura en tres partes, siendo la primera de ellas la presente nota introductoria. A continuación, en una fase de desarrollo, se proporcionarán inicialmente algunos conceptos relativos a la ciberseguridad, a los efectos de su mejor comprensión y a la correcta ponderación de su importancia en la agenda de la Seguridad Internacional actual. Luego, apelando al instrumental teórico de las relaciones internacionales, se hará foco en el grado y las características de la institucionalización de esta cuestión a nivel internacional. En este punto, se enfatizará en los mecanismos de gobernanza como una vía para superar las limitaciones existentes. En un

tercer momento, el foco de este escrito se centrará en la ciberguerra, cuestión central en el campo de la ciberseguridad contemporánea, debido a su peligrosidad e importancia. En tal sentido, se repasarán algunos mecanismos de gobernanza que pretenden regularla. Por último, se propondrán unas breves conclusiones.

Ciberseguridad contemporánea: algunas características

Luego de cinco décadas de desarrollo constante, a partir de su primera transmisión pública en 1969, internet alcanzó a comienzos del año 2020 a 4.5 mil millones de usuarios, casi el 60 % de la población mundial, y su influencia llegó a todos los aspectos de la interacción social. Hoy esa red constituye el basamento del ciberespacio considerado, en forma simplificada, como un "entorno virtual de información e interacciones entre personas".[2] Este entorno es global y dinámico, y está sustentado en infraestructuras y sistemas de información y telecomunicaciones.[3] Existe consenso en considerar al ciberespacio como un "común global", es decir, un dominio que no está bajo el control ni la jurisdicción de ningún Estado, pero su uso es materia de competencia por actores estatales y no estatales de todo el planeta.[4] Pero esa idea de común global, se limita a la infraestructura de internet, a sus aspectos técnicos, mientras se observan nítidas competencias y pujas de poder en las acciones que allí se despliegan.[5]

El ciberespacio tiene una dimensión de seguridad precisamente a causa de las competencias y pujas que allí se registran, protagonizadas por diferentes tipos de actores. Así, en líneas generales, puede entenderse que la ciberseguridad se enfoca en las amenazas y riesgos que surgen y se despliegan en el ciberespacio. Sin embargo, de manera más específica este concepto tiene contenidos y límites variables, de acuerdo con la fuente; de hecho, trabajos que exploraron esta cuestión comprobaron la existencia de medio centenar de definiciones diferentes sobre ciberseguridad.[6] Para superar esta diversidad, aquí empleamos la definición amplia e inclusiva que propone Naciones Unidas, a través de la Unión Internacional de Telecomunicaciones (UIT):[7]

2 Kissinger, Henry, *Orden mundial*, Barcelona, Debate, 2016.

3 Quintana, Yolanda, *Ciberguerra*, Madrid, Ediciones de la Catarata, 2016.

4 Stang, Gerald, "Global Commons. Between Cooperation and Competition", *Issue Brief* No. 17, European Union Institute for Security Studies, April, 2013.

5 Broeders, Dennis, "The Public Core of Internet: Towards an International Agenda for Internet Governance", *CyFy Journal* No. 3, 2016, pp. 24-30.

6 Maurer, Tim, & Morgus, Robert, *Compilation of Existing Cybersecurity and Information Security Related Definitions*, Switzerland, Federal Department of Foreign Affairs, 2014.

7 Unión Internacional de Telecomunicaciones, "Decisiones destacadas de Guadalajara", Actualidades de la UIT 9/2010, p. 20.

> La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.

La definición de ese organismo le otorga un lugar especial a la protección de los activos y los usuarios. *In extenso*, esta actividad centra su foco en la disponibilidad, integridad y confidencialidad de la información (la llamada "tríada CIA", por sus siglas en el idioma inglés) frente a eventuales agresiones o actividades maliciosas. Esas agresiones y actividades en el ciberespacio adoptan múltiples fisonomías y los actores que pueden ejecutarlas son extremadamente heterogéneos, tanto estatales como no estatales. Existen diferentes tipologías sobre los protagonistas de las cuestiones de ciberseguridad, de naturaleza no estatal. Empero, en todos los casos, las clasificaciones incluyen a organizaciones terroristas, inspiradas en móviles de naturaleza política, así como a grupos criminales movilizados por la obtención de ganancias económicas, a través de actividades ilegales. No pueden soslayarse los expertos en informática que emplean sus conocimientos para dañar los sistemas y robar la información que contienen, con fines de lucro (los mal llamados *hackers*[8]), como tampoco pueden dejar de mencionarse las sofisticadas entidades abocadas al ciberespionaje, también denominadas APT, por sus siglas en el idioma inglés de "amenazas persistentes avanzadas".

En el caso de los Estados-naciones protagonizan ese tipo de actividades a través de organismos civiles o militares, utilizando de alguna manera su poder cibernético, o ciberpoder, que puede ser entendido, en forma amplia, como "la habilidad de usar el ciberespacio para crear ventajas e influenciar eventos en todos los ambientes y a través de los instrumentos de poder".[9] De manera más ajustada, consiste en "la habilidad de obtener resultados deseados a través del uso de recursos de información interconectada, del dominio cibernético" e involucra formatos de poder blando y poder duro.[10]

Un criterio de amplio empleo para calificar las agresiones o actividades maliciosas en el ciberespacio, es aquel que las discrimina de acuerdo con su intensidad, dife-

8 En forma cotidiana, sin mayores precisiones semánticas, denominamos *hackers* a lo que la jerga informática considera *crackers*. Los primeros no utilizan su conocimiento experto en forma maliciosa; de hecho, lo emplean dentro del marco legal vigente. En muchos casos, los *hackers* comparten sus conocimientos y contribuyen a la mejora de la seguridad informática.

9 Hathaway, Melissa, & Klimburg, Alexander, "Preliminary Considerations on National Cyber Security". In Klimburg, Alexander (Ed.), *National Cyber Security Framework Manual*, Tallinn, NATO CCD COE, 2012, p. 28.

10 Nye, Joseph, *Cyber Power*, Belfer Center for Science and International Affairs, May 2010, p. 4.

renciando entre ciberincidentes y ciberataques. Los ciberincidentes son eventos de seguridad que comprometen la integridad, confiabilidad y disponibilidad de un activo de información.[11] Se entiende que estos eventos son de limitada gravedad y no siempre reflejan una voluntad de generar daño por parte del ejecutor. Los ciberataques, en cambio, apuntan a recolectar, interrumpir, denegar o destruir recursos de sistemas de información o información en sí misma. Pueden causar lesiones o muerte a personas, además de daños o destrucción total a objetos.[12] Debido a su intensidad y a sus efectos, los ciberataques pueden constituir una cuestión de Seguridad Nacional y por esa razón la Ciberseguridad Nacional consiste en la aplicación de medidas gubernamentales específicas para proteger a los ciudadanos de diversos ciberataques y ataques no cibernéticos relacionados, tanto locales como extranjeros. Esas medidas actúan sobre sistemas de tecnologías de la información y la comunicación públicos o privados, locales o externos, en cuestiones relevantes para la Seguridad Nacional.[13]

11 The Hague Centre for Strategic Studies, *Assessing Cyber Security. A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks*, The Hague, The Hague Centre for Strategic Studies, 2015.

12 *Ibidem*.

13 Hathaway, & Klimburg, *op. cit.*

Ciberespacio, desde la Teoría de las Relaciones Internacionales

El campo de la ciberseguridad refiere a las cuestiones de seguridad que afectan al ciberespacio y, debido al daño que pueden provocar las agresiones y actividades maliciosas en este dominio, se ha consolidado como una de las cuestiones más relevantes de la agenda de la Seguridad Internacional contemporánea. A pesar de este preocupante escenario, desde Naciones Unidas aún no ha sido posible redactar e implementar una Convención sobre Ciberseguridad, generándose una perniciosa situación de inexistencia de marco jurídico referencial, semejante a la que se observa en materia de terrorismo. Las principales potencias mundiales, que a la sazón ostentan los más altos niveles de ciberpoder nacional, oportunamente realizaron tímidos intentos en esta materia, que fracasaron.

Repasando esos antecedentes, a fines del siglo pasado, el gobierno de Rusia comenzó a desarrollar un abordaje de seguridad al dominio cibernético en el cual la amenaza era la información en sí misma; es decir, los contenidos que circulan en el ciberespacio. En esa línea, Moscú lideró en la Asamblea General de las Naciones Unidas la adopción de una resolución sobre "Desarrollo en el campo de la Información y Telecomunicaciones en el contexto de Seguridad Internacional" (A/Res/53/70).

La resolución impulsaba la sanción de normas multilaterales que garantizaran el control estatal de esa información, colisionando con la postura prevaleciente en Occidente, opuesta al control gubernamental del libre flujo de ese recurso intangible.[14]

Estos enfoques antagónicos cristalizaron en sendas posturas, vigentes hasta hoy. Por un lado, la mayoría de las naciones occidentales, incluyendo a Estados Unidos y los miembros de la Unión Europea, abordan la información que circula por el ciberespacio como un activo, sin referencias políticas o ideológicas. Estos actores entienden que un control de la información es contrario a los principios democráticos. Por otra parte, para actores como Rusia y China el concepto rector es "seguridad de la información", pasando la ciberseguridad a ser una parte de ella;[15] esta lectura se incluyó en un acuerdo suscripto en el año 2009 por los miembros de la Organización de Cooperación de Shanghái, en cuyo texto se justifica la adopción de medidas de censura y vigilancia digital.[16] Específicamente en el caso ruso, ya su Doctrina de Seguridad de la Información, aprobada en el año 2000, se refería a la protección de los intereses nacionales en la esfera informativa en un balance de intereses entre los individuos, la sociedad y el Estado.[17]

Desde aquellos momentos, y hasta nuestros días, no se registran intentos serios por parte de las principales potencias para articular entendimientos duraderos en esta materia. Apenas se puede mencionar el acuerdo firmado en 2015 por el mandatario estadounidense Barack Obama con su par chino Xi Jinping, por el cual el país asiático cesaría sus actividades de ciberespionaje sobre blancos de la contraparte. Aunque se entiende que el entendimiento nunca derivó en una modificación de la conducta china en este campo, fue dejado de lado con el inicio de la Administración Trump y el consecuente recrudecimiento de las fricciones bilaterales.[18]

Frente a esta innegable realidad y las posibilidades de un eficaz gerenciamiento de las cuestiones de ciberseguridad en el plano político global, las teorías de las relaciones internacionales presentan diferentes diagnósticos. En este sentido, la escuela realista subraya la naturaleza anárquica del ciberespacio, sosteniendo que esa cualidad lo transformará, inevitablemente,

14 Golden, Josh, "Dos enfoques incompatibles para gobernar el ciberespacio obstaculizan el consenso mundial", *Leiden Security & Global Affairs*, 16 de mayo de 2019.

15 Tsaruk, Oleksandr, & Korniiets, Maria, "Hybrid Nature of Modern Threats for Cybersecurity and Information Security", *Smart Cities and Regional Development Journal*, Vol. 4, No. 11, 2020, pp. 57-78.

16 Urgessa, Worku, "Multilateral Cybersecurity Governance: Divergent Conceptualizations and its Origin", *Computer Law & Security Review*, Vol. 26, 2020, pp. 1-8.

17 Gady, Franz-Stefan, & Austin, Greg, *Russia, the United States and Cyber Diplomacy*, New York, East-West Institute, 2010.

18 Alperovich, Dmitri, "The Case for Cyber-Realism. Geopolitical Problems Don't Have Technical Solutions", *Foreign Affairs*, January/February, 2022.

en un nuevo campo de batalla.[19] Además, esa anarquía facilitará que se extiendan a este plano rivalidades geopolíticas propias del mundo físico; en esta línea argumental, la conflictividad del ciberespacio sería más un síntoma que un fenómeno en sí.[20] Los realistas también sostienen que en el ciberespacio el Estado es el actor verdaderamente relevante y que un elemento clave en ese dominio, es el poder (planteo que remite al mencionado ciberpoder). El empleo de este poder sería más efectivo en modo ofensivo que defensivo, debido a la difícil atribución de los ciberataques, su bajo costo y su alta capacidad de daño.[21]

Finalmente, y a tono con lo anterior, el realismo explica la aparición de carreras armamentistas en el plano cibernético, por parte de los Estados con el poder necesario, como respuesta a la anarquía existente.[22] Implícitamente, se entiende, en esa apreciación realista, la existencia de armas cibernéticas, o ciberarmas, que pueden ser entendidas como "códigos de computadora que son usados, o diseñados para ser usados, con el objeto de amenazar o causar daño físico, funcional o mental a estructuras, sistemas o seres vivos".[23]

La idea de ciberarmas y carreras armamentistas en el plano cibernético retroalimentan la lógica realista. Por un lado, refuerzan el reconocimiento del Estado como actor predominante de esta arena, pues únicamente un puñado de ellos cuentan con los recursos (económicos, tecnológicos, humanos) necesarios para desarrollar ciberarmas de alto grado de sofisticación.[24] Por otro, ponen sobre la mesa la idea de un balance de poder entre las principales potencias del ciberespacio, quienes se restringirán y respetarán en ese dominio, como efecto colateral del aumento cuantitativo y una mayor letalidad de ese armamento.[25]

Las perspectivas liberales, a su turno, critican del realismo su excesivo estadocentrismo a la hora de estudiar el ciberespacio, soslayando la creciente relevancia de actores no estatales. Al mismo tiempo, valoran la cooperación para mitigar la peligrosidad de las amenazas en el dominio digital, incluyendo la cooperación entre las esferas pública y privada. También, tienen en cuenta a las instituciones multilaterales y su capacidad de satisfacer la fuerte demanda existente de normas de conducta compartidas.[26] En este punto, resulta conveniente introducir el concepto de "ciber-

19 Petallides, Constantine, "Cyber Terrorism and IR Theory: Realism, Liberalism and Constructivism in the New Security Threat", *Inquiries Journal/Student Pulse*, Vol. 4, No. 03, 2012.

20 Alperovich, *op. cit.*

21 Craig, Anthony, & Valeriano, Brandon, "Realism and Cyber Conflict: Security in the Digital Age", *E-International Relations*, February 3, 2018.

22 *Ibidem*.

23 Rid, Thomas, *Cyber War Will Not Take Place*. New York, Hurst & Co, 2013, p. 36.

24 *Ibidem*.

25 Valeriano, Brandon, & Maness, Ryan, "IR Theory and Cyber Security: Threat, Conflict and Ethics in an Emergent Domain". In Brown, Chris, & Eckersley, Robyn (Eds.), *The Oxford Handbook of IR Theory*, Oxford, Oxford University Press, 2017, pp. 259-272.

26 Valeriano, & Maness, *op. cit.*; Petallides, *op. cit.*

normas", entendidas como expectativas de conducta apropiada en el ciberespacio, que pretenden regular el desenvolvimiento de los actores y limitar los daños generados por actividades maliciosas.[27]

El liberalismo entiende que, aun cuando la carencia de una Convención sobre Ciberseguridad claramente afecta de forma negativa las posibilidades de cooperación en este campo, se han registrado importantes iniciativas por parte de diferentes organismos, de alcance regional o global. Estas instituciones han articulado esfuerzos con otros actores no estatales en un intento por configurar mecanismos de gobernanza global, pero solo han abordado algunos aspectos específicos de la ciberseguridad. En este punto, entendemos a la gobernanza global como la manera en que, en ausencia de una autoridad central, asuntos cuyos efectos alcanzan todo el planeta son manejados por un conjunto de actores de diferente tipo. Entre ellos, Estados, organismos multilaterales, ONG, entidades de la sociedad civil e, incluso, empresas privadas. Estos mecanismos no cuentan con estructuras formales ni registran un ejercicio de soberanía territorial.[28]

Considerando al ciberespacio en términos generales, los primeros abordajes sobre gobernanza se enfocaron en internet. En la Cumbre Mundial de la Sociedad de la Información, celebrada en Túnez en el año 2005, se entendió ese tipo de gobernanza en particular como:

> El desarrollo y aplicación, por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivos roles, de principios, normas, reglas, procesos de toma de decisiones y programas compartidos, que afectan a la evolución y el uso de Internet.[29]

A lo largo del tiempo, se registró una evolución del esquema de gobernanza planteado inicialmente en Túnez, que contemplaba tres tipos de participantes, a un modelo más complejo, de múltiples partes interesadas (*multistakeholder*): Estados, sector privado, sociedad civil, organismos internacionales, comunidades técnicas y mundo académico. No todos estos interesados tienen igual grado de influencia, razón por la cual se considera un modelo imperfecto.[30]

En el campo de la ciberseguridad, el concepto de gobernanza no se enfoca en la infraestructura de internet, que en definitiva es una cuestión técnica, sino en las actividades que se despliegan empleando

27 Ruhl, Christian, Hollis, Duncan, Hoffman, Wyatt, & Maurer, Tim, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, Working Paper, Washington, D. C., Carnegie Endowment for International Peace, 2020.

28 Badai i Dalmases, Francesc, *Orden y desorden en el siglo XXI*, Barcelona, Icaria, 2018.

29 World Summit on the Information Society, *Tunis Agenda for the Information Society*, Document WSIS-05/TUNIS/DOC/6(Rev.1)-E, November 18, 2005, Paragraph 33.

30 Dutton, William, *Multistakeholder Internet Governance?* Washington, D. C., The World Bank, 2016.

ese andamiaje. Como se anticipó a inicios de este trabajo, existe cierto consenso en que la infraestructura de internet sea considerada un bien público global, y en tal sentido permanezca al margen de pujas y rivalidades, al tiempo que las políticas de poder signan las acciones que en ella se llevan a cabo.[31]

Tal cual hemos explicado en un trabajo anterior, un claro ejemplo de gobernanza en ciberseguridad se encuentra en la referida UIT, comprometida con el desarrollo de eficaces estrategias nacionales en esta materia. A ese efecto, desarrolla guías e índices para el empleo de los gobiernos, que cuentan con la participación de heterogéneos actores: organismos multilaterales globales (Banco Mundial) y regionales (Organización del Tratado de Atlántico Norte, OTAN), empresas privadas (Deloitte, Microsoft) e instituciones académicas (Global Cyber Security Capacity Centre, Geneva Centre for Security Policy y Potomac Institute for Policy Studies).[32]

En la construcción de los mecanismos de gobernanza de la ciberseguridad, y en forma más amplia del ciberespacio en su conjunto, la diplomacia estaría llamada a ejercer un papel clave. Sobre todo, en materia de ciberseguridad, pues esta afecta —y amenaza— la gobernanza del ciberespacio en su conjunto. Precisamente, la llamada "ciberdiplomacia" alude a prácticas diplomáticas vinculadas con la gobernanza del ciberespacio, protagonizadas por funcionarios que deben entender de cuestiones cibernéticas y estar en capacidad de negociar con interlocutores de diferente tipo (las múltiples partes interesadas referidas en un párrafo anterior).[33] El enfoque europeo sobre la ciberdiplomacia identifica cinco objetivos, que se encuentran directamente vinculados con la ciberseguridad: Fortalecimiento de la resiliencia, Construcción de confianza, Prevención de conflictos, Protección de derechos humanos y libertades individuales, y Promoción del multilateralismo.[34]

Mecanismos de gobernanza en el campo de la ciberguerra

Como se indicó, un aspecto de la ciberseguridad en la cual se comprueba la vigencia de mecanismos de gobernanza es el que atañe a la ciberguerra. A partir de su aparición hace casi tres décadas,[35] este concepto ha sido objeto de controversias en cuanto a su significado y alcances. Al respecto, las perspectivas abarcan desde

31 Broeders, *op. cit.*

32 Anguita, Concepción y Bartolomé, Mariano: "El reto de la gobernanza global en ciberseguridad. La gestión de la Unión Europea y la Organización de Estados Americanos". En Sánchez Gutiérrez, Bianca y Pineda, Antonio (Coords.), *Comunicación política en el mundo digital: tendencias actuales en propaganda, ideología y sociedad*, Madrid, Dykinson, 2021, pp. 623-648.

33 Riordan, Shawn, "Por qué necesitamos diplomáticos en el ciberespacio", *EsGlobal*, 22 de abril de 2019.

34 EU Cyber Direct, *Cyber Diplomacy in the European Union*, Brussels, European Union, 2020.

35 Arquilla, John, & Ronfeldt, David, "Cyberwar is Coming!", *Comparative Strategy*, Vo. 12, No. 2, 1993, pp. 141-165.

lecturas según las cuales la ciberguerra es un concepto de escasa utilidad, debido a su casi nula probabilidad de ocurrencia,[36], hasta planteos que vaticinan que esa será la fisonomía de los futuros conflictos.[37] Está fuera de duda, en cambio, que el hecho bélico incluirá distintas formas de combate cibernéticas que se combinarán con acciones ejecutadas en los otros dominios.[38] Aunque los debates en torno a la naturaleza y las características de la ciberguerra y las formas de combate cibernéticas exceden el objetivo del presente trabajo, los esfuerzos de gobernanza asociados a estas cuestiones apuntan a evitar la ocurrencia de estos acontecimientos, como hipótesis de máxima, o al menos regularlos.

Con este panorama, resalta el aporte realizado desde el Centro de Excelencia en Ciberdefensa de la OTAN, instalado en Estonia tras el ciberataque sufrido por la nación báltica en 2007, ya mencionado a inicios de este trabajo. Desde esa institución, se realizaron importantes esfuerzos para tipificar las formas de combate cibernéticas y encuadrarlas dentro del Derecho Internacional Humanitario, o Derecho Internacional de los Conflictos Armados. Esos intentos adoptaron la forma de manuales colectivos elaborados por expertos, de carácter orientativo y no vinculante.[39] El resultado de estas iniciativas ha sido confirmar que el Derecho Internacional de los Conflictos Armados, es aplicable al ciberespacio y al caso de ciberataques. Empero, numerosos especialistas han señalado diversas cuestiones que aún permanecen sin aclarar, o generan dudas, en este campo.[40] Entre ellas, las diferencias de empleo de ciberataques en tiempos de paz o guerra; cuándo es considerado un "uso de la fuerza", de acuerdo con el Derecho Internacional; qué tipo de blancos son aceptables o cómo ajustar estas acciones a los principios del *ius in bello*. Tampoco queda claro cómo mensurar las capacidades de un Estado para realizar ciberataques, pues el concepto de capacidades cibernéticas "ofensivas" no presenta diferencias claras con el de ciberarmas, siendo que estas pueden emplearse en modalidades defensivas. Aquellas remiten, textualmente, a: "una capacidad diseñada para acceder a un sistema o red de computadoras para dañar entidades vivas o materiales".[41]

36 Rid, Thomas, *op. cit.*

37 Sanger, David, *The Perfect Weapon. War, Sabotage and Fear in the Cyber Age*. New York, Crown Publishing, 2018.

38 Stevens, Tim, "Cyberweapons: Power and the Governance of the Invisible", *International Politics*, Vol. 55, 2018, pp. 482-502. Bartolomé, Mariano, "Las ciberamenazas y su impacto en el campo de la Seguridad Internacional", *Revista de la Escuela Superior de Guerra*, núm. 602, 2019, pp. 151-163.

39 Schmitt, Michael (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013. También, Schmitt, Michael (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2017.

40 Hathaway, & Klimburg, *op. cit.*; Stevens, *op. cit.*

41 Smeets, Max, & Lin, Herbert, "Offensive Cyber Capabilities: to what Ends?". In Minarik, T., Jakschis, R., & Lindstrom, L. (Eds.), *10th International Conference on Cyber Conflicts: Maximizing Effects*. Tallinn, NATO CCD COE, 2018, p. 58.

Naciones Unidas ha aportado en este campo la constitución de sendos grupos, creados en 2004 y 2018, respectivamente, enmarcados en la Oficina de Asuntos de Desarme: el Grupo de Expertos Gubernamentales (GGE), integrado por técnicos de veinticinco naciones partes, y relacionado con organismos regionales;[42] y el Grupo de Trabajo de Final Abierto, precisamente abierto a todos los miembros de la ONU y también a ONG y entidades de la sociedad civil. Ambas instancias se enfocan en los rumbos que sigue la agenda global de ciberseguridad y la aplicación del Derecho Internacional de los Conflictos Armados al dominio cibernético.

El funcionamiento del GGE ya ha culminado y su informe final será presentado en la Asamblea General anual tras procesar diferentes insumos, entre ellos, los aportes de las organizaciones regionales.[43] No obstante, algunas de sus conclusiones parciales enfatizan en que no es clara la aplicación en el ciberespacio de las definiciones "ataque armado" o "uso de la fuerza", como tampoco la forma de medición de estos fenómenos ni quién tendrá esa potestad. De manera inevitable, esta falta de claridad se traslada al ejercicio de la "legítima defensa" por medios tradicionales frente a un ciberataque.[44]

La gobernanza de la ciberseguridad en materia de ciberguerra y formas de combate cibernéticas atiende también la gestión de crisis en este dominio, evitando su surgimiento y, en caso de acontecer, su escalada. Nuevamente, en este caso, el GGE desarrolla un interesante papel, impulsando la aplicación de Medidas de Fomento a la Confianza y la Seguridad (CSBM). En ese sentido, se adopta el modelo de la Organización para la Seguridad y la Cooperación en Europa (OSCE), estructurado en torno a tres ejes: postura, preparación y comunicación.[45] Por otra parte, también son destacables las iniciativas desarrolladas en este campo por un actor no estatal, Microsoft, promoviendo la adopción internacional de un conjunto de normas que permitan prevenir el surgimiento y escalada de conflictos cibernéticos, a partir de una afectación a la —ya mencionada— tríada CIA.[46]

42 Estos organismos son la Unión Africana (UA), la Unión Europea (UE), la Organización de Estados Americanos (OEA), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Asociación de Naciones del Sudeste Asiático (ASEAN).

43 United Nations Office for Disarmament Affairs, *Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. December, 2019.

44 United Nations Institute for Disarmament Research & Center for Strategic International Studies, *Report of the International Security Cyber Issues Workshop Series*, Geneve, UNIDIR, 2016.

45 Radicevic, Velimir, *The Role of OSCE Confidence Building Measures in Addressing Cyber/ICT Security Challenges to Critical Infrastructure*. OSCE, October 9, 2018.

46 Microsoft, *Five Principles for Shaping Cybersecurity Norms*, Microsoft Corporation, 2013.

Conclusiones

En la actualidad, el ciberespacio, entorno virtual de información e interacción, alcanza cada rincón de la sociedad y afecta prácticamente todos los campos de las relaciones humanas. Al tiempo que reporta bienestar y calidad de vida, ese plano se ha tornado en escenario para la aparición y despliegue de múltiples amenazas y riesgos, dando lugar al dinámico campo de la ciberseguridad. Una heterogénea variedad de actores protagoniza las cuestiones de ciberseguridad, incluyendo los Estados-naciones, a través de diferentes agencias o instituciones, empleando de alguna manera su ciberpoder. Se supone que un número reducido de actores estatales puede disponer de capacidades ofensivas en el ciberespacio; la mayor parte de ellos suelen llevar adelante medidas de gobierno orientadas a prevenir y remediar incidentes o ataques que pueden sufrir en el dominio cibernético bajo una concepción —explícita o implícita— de Ciberseguridad Nacional.

La importancia que este tema representa, en términos de la Seguridad Internacional contemporánea, ha motivado su abordaje y análisis desde la perspectiva teórica de las relaciones internacionales. En este punto, las dos corrientes teóricas más importantes presentan perspectivas diferentes: el realismo entiende al ciberespacio como un entorno anárquico, y consecuentemente altamente conflictivo, donde el principal recurso es el poder que ostentan los principales actores, a la sazón Estados; en la vereda opuesta, el liberalismo considera que el ciberespacio es un dominio donde despliegan sus acciones actores de diferente naturaleza, agregando que la anarquía existente puede mitigarse mediante la cooperación y el accionar multilateral.

La realidad sugiere que la situación actual del ciberespacio refleja aristas que responden a las dos corrientes teóricas mencionadas. Así, su importancia no se refleja en los niveles de institucionalización alcanzados, desde el momento en que no se ha conseguido un documento rector en la materia, en el seno de las Naciones Unidas. Empero, mecanismos de gobernanza han paliado parcialmente las peligrosas consecuencias que puede acarrear esa carencia. La cuestión de la ciberguerra permite confirmar esta apreciación: numerosas iniciativas han tratado de aportar una clara tipificación de sus diferentes manifestaciones dentro del Derecho Internacional Humanitario, o Derecho Internacional de los Conflictos Armados. Aquí sí las Naciones Unidas han jugado un papel destacado, propiciando la constitución de dos grupos de trabajo: uno de ellos vinculado a organismos regionales; el otro, abierto a la interacción con actores no estatales de diverso tipo.

Sin embargo, el éxito de los mecanismos de gobernanza de la ciberguerra es

sumamente discutible. Todavía hoy persisten numerosas dudas en torno de la aplicación del Derecho Internacional de los Conflictos Armados a la ciberguerra. Incluso, el mismo concepto de "ataque armado" en el entorno cibernético continúa siendo objeto de controversias. No queda claro que los mencionados mecanismos existentes puedan arrojar luz sobre estos asuntos y aumentar el grado de los consensos ya alcanzados, pero no se avizora otra alternativa con mayor grado de institucionalidad en el corto plazo.

Referencias

Alperovich, Dmitri, "The Case for Cyber-Realism. Geopolitical Problems Don't Have Technical Solutions", *Foreign Affairs*, January/February, 2022.

Anguita, Concepción y Bartolomé, Mariano: "El reto de la gobernanza global en ciberseguridad. La gestión de la Unión Europea y la Organización de Estados Americanos". En Sánchez Gutiérrez, Bianca y Pineda, Antonio (Coords.), *Comunicación política en el mundo digital: tendencias actuales en propaganda, ideología y sociedad*, Madrid, Dykinson, 2021, pp. 623-648.

Arquilla, John, & Ronfeldt, David, "Cyberwar is Coming!", *Comparative Strategy*, Vol. 12, No. 2, 1993, pp. 141-165.

Badai I Dalmases, Francesc, *Orden y desorden en el siglo* XXI, Barcelona, Icaria, 2018.

Bartolomé, Mariano, "Las ciberamenazas y su impacto en el campo de la Seguridad Internacional", *Revista de la Escuela Superior de Guerra*, núm. 602, 2019, pp. 151-163.

Broeders, Dennis, "The Public Core of Internet: Towards an International Agenda for Internet Governance", *CyFy Journal*, No. 3, 2016, pp. 24-30.

Craig, Anthony, & Valeriano, Brandon, "Realism and Cyber Conflict: Security in the Digital Age", *E-International Relations*, February 3, 2018.

Dutton, William, *Multistakeholder Internet Governance?* Washington, D. C., The World Bank, 2016.

EU Cyber Direct, *Cyber Diplomacy in the European Union*, Brussels, European Union, 2020.

Gady, Franz-Stefan, & Austin, Greg, *Russia, the United States and Cyber Diplomacy*, New York, East-West Institute, 2010.

Golden, Josh, "Dos enfoques incompatibles para gobernar el ciberespacio obstaculizan el consenso mundial", *Leiden Security & Global Affairs*, 16 de mayo de 2019.

Hathaway, Melissa, & Alexander Klimburg, "Preliminary Considerations on National Cyber Security". In Klimburg, Alexander (Ed.), *National Cyber Security Framework Manual*, Tallinn, NATO CCD COE, 2012.

Kissinger, Henry, *Orden mundial*, Barcelona, Debate, 2016.

Lindstrom, Gustav, "Meeting the Cyber Security Challenge", Geneva Centre for Security Policy, *Geneva Papers*, 7, 2012.

Maurer, Tim, & Morgus, Robert, *Compilation of Existing Cybersecurity and Information Secu-*

rity Related Definitions, Switzerland, Federal Department of Foreign Affairs, 2014.

Microsoft, *Five Principles for Shaping Cybersecurity Norms*, Microsoft Corporation, 2013.

Nye, Joseph, *Cyber Power*, Belfer Center for Science and International Affairs, May, 2010.

Petallides, Constantine, "Cyber Terrorism and IR Theory: Realism, Liberalism and Constructivism in the New Security Threat", *Inquiries Journal/Student Pulse*, Vol. 4, No. 03, 2012.

Quintana, Yolanda, *Ciberguerra*, Madrid, Ediciones de la Catarata, 2016.

Radicevic, Velimir, *The Role of OSCE Confidence Building Measures in Addressing Cyber/ICT Security Challenges to Critical Infrastructure*. OSCE, October 9, 2018.

Rid, Thomas, *Cyber War Will Not Take Place*. London, Hurst & Co, 2013.

Riordan, Shawn, "Por qué necesitamos diplomáticos en el ciberespacio", *EsGlobal*, 22 de abril de 2019.

Ruhl, Christian, Hollis, Duncan, Hoffman, Wyatt, & Maurer, Tim, *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*, Working Paper, Washington, D. C., Carnegie Endowment for International Peace, 2020.

Sanger, David, *The Perfect Weapon. War, Sabotage and Fear in the Cyber Age*. New York, Crown Publishing, 2018.

Schmitt, Michael (Ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013.

----- (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2017.

Smeets, Max, & Lin, Herbert, "Offensive Cyber Capabilities: to what Ends?" In Minarik, T., Jakschis, R., & Lindstrom, L. (Eds.), *10th International Conference on Cyber Conflicts: Maximizing Effects*. Tallinn, NATO CCD COE, 2018, pp. 55-72.

Stang, Gerald, "Global Commons. Between Cooperation and Competition", *Issue Brief* No. 17, European Union Institute for Security Studies, April, 2013.

Stevens, Tim, "Cyberweapons: Power and the Governance of the Invisible", *International Politics*, Vol. 55, 2018, pp. 482-502.

The Hague Centre for Strategic Studies, *Assessing Cyber Security. A Meta-Analysis of Threats, Trends, and Responses to Cyber Attacks*, The Hague, The Hague Centre for Strategic Studies, 2015.

Tsaruk, Oleksandr, & Korniiets, Maria, "Hybrid Nature of Modern Threats for Cybersecurity and Information Security", *Smart Cities and Regional Development Journal*, Vol. 4, No. 11, 2020, pp. 57-78.

United Nations Institute for Disarmament Research & Center for Strategic International Studies, *Report of the International Security Cyber Issues Workshop Series*, Geneve, UNIDIR, 2016.

United Nations Office for Disarmament Affairs, *Regional Consultations Series of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. December, 2019.

Unión Internacional de Telecomunicaciones, "Decisiones destacadas de Guadalajara", Actualidades de la UIT 9/2010, pp. 20-22.

Urgessa, Worku, "Multilateral Cybersecurity Governance: Divergent Conceptualizations and its Origin", *Computer Law & Security Review*, Vol. 26, 2020, pp. 1-8.

Valeriano, Brandon, & Maness, Ryan, "IR Theory and Cyber Security: Threat, Conflict and Ethics in an Emergent Domain". In Brown, Chris, & Eckersley, Robyn (Eds.), *The Oxford Handbook of IR Theory*, Oxford, Oxford University Press, 2017, pp. 259-272.

World Summit on the Information Society, *Tunis Agenda for the Information Society*, Document WSIS-05/TUNIS/DOC/6(Rev.1)-E, November 18, 2005.