ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

101/2016 3 de octubre de 2016

*Margarita Robles Carrillo* *

El concepto de arma cibernética en el marco internacional: una aproximación funcional



# El concepto de arma cibernética en el marco internacional: una aproximación funcional

## Resumen:

La definición de un concepto de arma cibernética es un presupuesto previo necesario para la efectiva aplicación del principio de prohibición del uso y de la amenaza de la fuerza en el ámbito internacional. En este trabajo se analiza, en primer lugar, como contexto general, el contraste entre el discurso político-institucional y la práctica internacional en relación con la efectividad de este principio en el entorno cibernético. En segundo término, se exponen las principales concepciones sobre la noción de arma cibernética elaboradas desde una perspectiva instrumental o material. Finalmente, se propone la adopción de un concepto funcional de arma cibernética capaz de distinguir esas acciones teniendo en cuenta la polivalencia de las actividades cibernéticas y de incorporar los distintos componentes subjetivo, material y teleológico que, combinados, permitirían identifican un uso de la fuerza armada en Derecho internacional.

*Abstract:*

*The definition of a concept of cyber weapon is necessary for the effective implementation of the principle of prohibition of the threat and use of force in the international arena. This paper examines, first, as a general context, the contrast between the political and institutional discourse and international practice in relation to the effectiveness of this principle in the cyber environment. Secondly, this work presents the main concepts of the notion of cyber weapon made from an instrumental or material perspective. Finally, the paper proposes the adoption of a functional concept of cyber weapon capable of distinguishing those actions taking into account the versatility of cyber activities and to incorporate the various subjective, material and teleological components that together allow identify a use of force armed in international law.*

## Palabras clave:

Arma cibernética, prohibición de la amenaza y del uso de la fuerza, Derecho internacional.

*Keywords:*

*Cyber Weapon, prohibition of the threat and use of force, International Law.*

## Introducción

La articulación de un concepto de arma cibernética constituye no sólo un desafío desde el punto de vista técnico, político, institucional y doctrinal sino, también y sobre todo, una prioridad en el marco de un modelo de seguridad internacional que se sustenta en el principio básico de prohibición del uso y de la amenaza de la fuerza armada. Es un principio clave del Derecho internacional contemporáneo consagrado en el artículo 2.4 de la Carta de Naciones Unidas que, además, prevé como una excepción al mismo, en su artículo 51, el ejercicio de la legítima defensa individual o colectiva en caso de "ataque armado contra un miembro de Naciones Unidas". El concepto de arma sirve, en consecuencia, tanto para determinar el alcance y contenido de la prohibición del artículo 2.4, como para justificar las excepciones al principio establecido en esa disposición de naturaleza imperativa. Entre ellas se encuentra no sólo la legítima defensa sino, también, la posibilidad de adopción de medidas coercitivas por parte del Consejo de Seguridad, de conformidad con el capítulo VII de la Carta, entre las cuales es lógico prever la posibilidad de realizar acciones cibernéticas[1].

La definición del principio de prohibición del uso y de la amenaza de la fuerza y del alcance de sus excepciones en términos operativos nunca ha estado exenta de polémica, como prueban la práctica internacional y la jurisprudencia, en particular, del Tribunal Internacional de Justicia. En las dos últimas décadas, la interpretación del alcance del artículo 51 de la Carta o la generación de doctrinas que quieren introducir nuevas excepciones a la prohibición del uso o amenaza de la fuerza han reactivado notablemente el debate en torno al mismo. Ese debate se ha visto, asimismo, impulsado por la irrupción y el preocupante aumento de las amenazas procedentes de los actores no estatales con la particularidad de que, sin ser ellos los destinatarios naturales de la prohibición recogida en el artículo 2.4 de la Carta, sí que pueden asumir la autoría del "ataque armado" al que se refiere su artículo 51. Esta disposición define como sujeto

[1] Las disposiciones contenidas en el Capítulo VII de la Carta no contienen una relación cerrada de medidas a disposición del Consejo de Seguridad. En particular, el artículo 41 indica que "podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas. Por su parte, el artículo 42 dispone que "podrá ejercer, por medio de fuerzas aéreas, navales o terrestres, la acción que sea necesaria para mantener o restablecer la paz y la seguridad internacionales. Tal acción podrá comprender demostraciones, bloqueos y otras operaciones ejecutadas por fuerzas aéreas, navales o terrestres de Miembros de las Naciones Unidas".

pasivo al "miembro de Naciones Unidas", pero no precisa la identidad del sujeto activo que, en consecuencia, puede ser un Estado o un actor no estatal.

En este contexto, marcado por un debate profundo, continuo y escasamente pacífico sobre el alcance, contenido y límites de la prohibición del uso y de la amenaza de la fuerza, se plantea la cuestión de su aplicación en el ciberespacio.

La aplicación de este principio en el ciberespacio es absolutamente lógica por dos motivos principales: en primer lugar, porque es una norma básica para la coexistencia social en cualquier sistema jurídico, que se manifiesta, en los derechos internos, atribuyendo al Estado el monopolio de la violencia legítima y, en Derecho internacional, mediante la regulación del uso legítimo de la fuerza como dispone la Carta de Naciones Unidas; y, en segundo término, aunque no en orden de importancia, naturalmente, porque es una norma de naturaleza imperativa en vigor que obliga al conjunto de los Estados, con independencia del medio o ámbito de actuación, ya sea el espacio virtual o el no virtual.

Pero, por otra parte, la traslación de este principio al ciberespacio plantea dos categorías principales de problemas: los técnicos-jurídicos, derivados de la dificultad de calificar una acción cibernética como uso o amenaza de uso de la fuerza armada: y, junto a ellos, los político-jurídicos, resultantes de las diferentes interpretaciones de que es objeto este principio, en ocasiones, con el propósito último de eludir su prohibición o de subvertir las condiciones jurídicamente establecidas para introducir excepciones a dicho principio[2].

En el marco de ese debate, el concepto de arma cibernética es esencial porque ha de servir para definir la existencia de un uso de la fuerza armada prohibido por el Derecho internacional y para determinar la existencia de un ataque armado capaz de justificar una excepción legítima a dicha prohibición. Pero no existe un concepto consensuado en el plano político, institucional, doctrinal o, incluso, técnico. No son pocos los motivos que explican ese disenso, pero buena parte de ellos trae causa de la contradictoria relación

[2] Pueden verse, al respecto, HURD, I, "Permissive Law on the International Use of Force", en *The Use of Armed Force: Are We Approaching Normative Collapse?, ASIL Proceedings*, 2015, 10; RUYS, T., "Divergent Views on The Chapter Norms on the Use of Force – A Transatlantic Divide?, en *The Use of Armed Force: Are We Aproaching Normative Collapse?, ASIL Proceedings,* 2015, 14; WOOD, M., *The Use of Force in 2015 With Particular Reference to Syria*, Hebrew University of Jerusalem Legal Studies Research Paper, Serie nº 16-05, 2015.

que se está produciendo desde hace tiempo entre el discurso jurídico-político y la práctica internacional.

## El discurso político-jurídico versus la práctica internacional

El debate global sobre los avances tecnológicos y sus repercusiones en materia de seguridad internacional se ha canalizado a través de la Asamblea General de Naciones Unidas que, desde hace tiempo, se está ocupando de esta cuestión. En ese marco confluyen las observaciones individuales presentadas por los Estados[3], las propuestas conjuntas que han liderado Rusia y China junto con otros países[4] y los sucesivos Informes de los Grupos de Expertos Gubernamentales[5].

El análisis de esos trabajos pone de manifiesto la progresiva formación de un consenso sobre dos principios básicos: la aplicación del Derecho internacional en vigor, en particular, las normas contenidos en la Carta de Naciones Unidas y la adopción progresiva de las normas específicas necesarias atendiendo a la singularidad del ciberespacio.

Este principio de acuerdo puede parecer un avance pero resulta ser, en mayor medida, una situación de impasse por un doble motivo: primero, porque se trata simplemente del compromiso de aplicar el derecho vigente creado para un mundo sólo físico, como no podía ser de otra manera porque son normas obligatorias para los Estados con

[3] En la Resolución 53/70 sobre "Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional", de 4 de enero de 1999, la AGNU invita a todos los Estados Miembros a que hagan llegar al Secretario General sus comentarios de los Estados sobre: "a) Evaluación general de los problemas de la seguridad de la información; b) Determinación de criterios básicos relacionados con la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de los sistemas de información y de telecomunicaciones y de los recursos de información; c) Conveniencia de elaborar principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información" (A/RES/53/70, 4 de enero de 1999, 2).

[4] Rusia y China han liderado dos propuestas conjuntas ante la AGNU. La primera se encuentra en una carta, fechada el 12 de septiembre de 2011, en la que China, Rusia, Tayikistán y Uzbekistán presentan una propuesta de resolución conteniendo un código internacional de conducta para la seguridad de la información (A/66/359, 14 de septiembre de 2011, 3-5). En 2015, incorporando a Kazajstán y Kirguistán, presentan la versión revisada del código de conducta (A/69/723, 13 de enero de 2015, 3-6).

[5] Tras el fracaso en 2004 del primer Grupo de Expertos Gubernamentales (GEG), incapaz de concluir un informe, y el acuerdo de mínimos alcanzado en 2010, se suceden los informes de los GEG de 2013 (A/68/98, 24 de junio de 2013) y de 2015 (A/70/174, 22 de julio de 2015) con avances significativos en determinados aspectos pero no precisamente en materia de uso y amenaza del uso de la fuerza a través del ciberespacio.

independencia de su ámbito de actuación; y, en segundo lugar, porque supone asumir que aún no se ha generado el consenso preciso para adoptar las normas específicas, que son reconocidas como necesarias, para adaptarse a las condiciones singulares que impone el ciberespacio.

En definitiva, el acuerdo se resume en aplicar las normas en vigor creadas para el mundo físico reconociendo que el cibernético necesita normas específicas que aún no han sido objeto de consenso. En términos generales y de técnica jurídica, nadie discute que las obligaciones asumidas por los Estados, en particular, dentro del modelo de seguridad colectiva de la Carta de Naciones Unidas, se extienden al ciberespacio. Pero, en términos prácticos, no todas esas obligaciones son fácilmente extrapolables a este otro ámbito genética y funcionalmente marcado por la impronta de su singularidad. Es el caso, en particular, de la prohibición del uso y de la amenaza de la fuerza. La cuestión es por qué no se está avanzando en esa línea cuando es evidente que la acción cibernética se está manifestando como una modalidad de uso de la fuerza y como un componente presente en las estrategias de seguridad y defensa de todos los Estados.

La realidad ofrece, a esos efectos, tres datos contundentes: 1) La práctica internacional muestra que se están realizando acciones en el ciberespacio susceptibles de ser calificadas como uso de la fuerza en distintas modalidades que van desde los conocidos ataques a Estonia hasta el aún oscuro caso Stuxnet, sin obviar situaciones como las de Georgia, Ucrania o Siria, que constituyen la expresión del uso de la acción cibernética en una situación de conflicto armado; 2) La mayoría de los países están desarrollando capacidades cibernéticas en el marco de sus estrategias de seguridad y defensa y la acción cibernética se incorpora en ellas como un instrumento político, defensivo y ofensivo, en mayor o menor medida, según los casos; 3) La conflictividad cibernética está creciendo exponencialmente a nivel interno e internacional sin que se haya reconocido institucionalmente un único supuesto de uso de la fuerza cibernética[6].

El Consejo de Seguridad de Naciones Unidas, que es el máximo responsable en materia de mantenimiento de la paz y la seguridad internacional, no ha querido o no ha tenido ocasión de pronunciarse calificando una acción cibernética como un uso de la fuerza,

[6] Una explicación más extensa y precisa de esos datos puede verse en ROBLES CARRILLO, M., "Amenaza y uso de la fuerza a través del ciberespacio: un cambio de paradigma", *Revista Latinoamericana de Derecho Internacional*, nº 4, 2016, 3-9 (http://www.revistaladi.com.ar/numero4-robles/).

una amenaza a la paz, un quebrantamiento de la paz o un acto de agresión[7]. Es obvio que entre sus miembros permanentes se encuentran los Estados que lideran el avance tecnológico que son, precisamente, también los que representan las cosmovisiones más opuestas sobre el ciberespacio[8], siendo ello un dato clave que explica la ausencia de pronunciamientos. Pero tampoco la Asamblea General avanza en una solución a estos problemas. En una sesión del Comité de Asuntos Exteriores de la Cámara de Representantes del Congreso estadounidense sobre ciberguerra, en septiembre de 2015, James a. Lewis afirmaba que, en el marco de los trabajos de Naciones Unidas, el punto principal de desacuerdo es el artículo 2.4 de la Carta que prohíbe el uso y la amenaza de la fuerza y el artículo 51 que establece el derecho a la legítima defensa como excepción al mismo[9].

La Cumbre del G-7 celebrada en Ise-Shima, Japón, los días 26 y 27 de mayo de 2016, ha conducido a la adopción de una declaración conjunta sobre los principios y acciones en el ciberespacio en la que se subraya directamente el problema del uso de la fuerza. Según los términos de la misma, "We affirm that under some circumstances, cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law. We also recognize that states may exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the United Nations Charter and in accordance with international law, including international humanitarian law, in response to an armed attack through cyberspace"[10]. El G-7 reconoce los avances en los trabajos del GEG y apoya, en

---

[7] Weissbrodt sostiene que "The Security Council has the full authority to label any CNO a threat to the peace, but they are unlikely to do so. Decisions to use force under Articles 39 and 42 are determined after extensive debates and deliberations, and during voting any decision to use force may be blocked through a veto made by any of the permanent members of the Security Council. (…) In light of Russia's and China's presence on the Council (cyber operations regularly emanate from their territory), this limitation may well prove the greatest obstacle to effective U.N. action in the face of those cyber operations which would in some fashion endanger international stability." (WEISSBRODT, D. "Cyber-conflict, Cyber-crime, and Cyber-Espionage", *Minnesota Journal of International Law*, vol. 22, 2013, 361).

[8] Sánchez de Rojas identifica tres cosmovisiones básicas y distintas de la ciberseguridad: la ciberliberal defensiva representada por la UE y los países europeos, la ciberliberal ofensiva abanderada por EEUU y la cibernacionalista-aislacionista de Rusia y China (SÁNCHEZ DE ROJAS DÍAZ, E. "Cooperación internacional en temas de ciberseguridad", en *Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario*, Madrid, Ministerio de Defensa, 2013, p. 262).

[9] *Cyber War: Definitions, Deterrence, And Foreign Policy*, Hearing Before The Committee On Foreign Affairs House of Representatives. First Session. September 30, 2015, p. 12. Online: http://foreignaffairs.house.gov/hearing/hearing-cyber-war-definitions-deterrence-and-foreign-policy.

[10] http://www.mofa.go.jp/files/000160279.pdf.

particular, "the continued development and implementation of cyber confidence building measures between states to promote trust and reduce the risk of conflict stemming from the use of ICTs"[11]. Esta propuesta, que cuenta con el apoyo de un buen número de Estados y que se está encauzando con medidas operativas en el marco de la OSCE, es una demostración clara del largo camino que queda para llegar a acuerdos mayores entre los Estados en esta materia.

Pero es que además, la aplicación de ese principio en el ciberespacio plantea dos órdenes de problemas. Por una parte, genera dificultades de naturaleza subjetiva por un doble motivo: porque ha aumentado la presencia y el protagonismo de los agentes no estatales y porque se ha incrementado hasta límites inimaginables su capacidad para actuar en el marco internacional en todos los ámbitos, incluido, el uso de la fuerza. Por otra parte, plantea obstáculos de naturaleza objetiva derivados de la singularidad del arma cibernética y sus diferencias con la cinética que se manifiestan, destacadamente, en tres extremos: la mayor accesibilidad y disponibilidad del medio cibernético; la variedad y diversidad de operativos; y la multifuncionalidad de las acciones cibernéticas.

Esta combinación de circunstancias demuestra la dificultad de extrapolar política y jurídicamente al espacio cibernético la prohibición contenida en el artículo 2.4 de la Carta, en buena medida, porque no se está consensuando un concepto de arma cibernética que permita definir la existencia de una vulneración de ese principio.

En mi opinión, el problema de fondo reside en que el discurso jurídico-político internacional sobre el uso de la fuerza en el ciberespacio es un discurso contaminado y es un discurso deliberadamente ambiguo.

Es, en primer lugar, un discurso contaminado porque cuando los Estados debaten sobre ese principio en el marco de Naciones Unidas están más centrados y preocupados por justificar y, en su caso, imponer y consolidar sus propias doctrinas sobre el uso de la fuerza que en analizar y resolver los problemas que plantea la aplicación de la prohibición del uso de la fuerza a través del ciberespacio. El debate se ha focalizado en las interpretaciones o en la defensa de las excepciones a la prohibición del uso de la fuerza como la legitima defensa anticipada o preventiva, la intervención por invitación o la aplicación de la doctrina *unable and unwalling*, entre otras. No es, como debería ser, un

[11] *Ibidem.*

debate sobre el uso de la fuerza en el ciberespacio, sino un debate sobre este principio en su conjunto en el que cada parte trata de defender su propia percepción sobre el mismo[12]. Y esto es, hasta cierto punto, comprensible aunque no lógico.

Es, en segundo lugar, un discurso deliberadamente ambiguo[13] porque la inexistencia de un verdadero debate sobre las particularidades que implica la aplicación de este principio en el ciberespacio, identificando problemas y ofreciendo soluciones, permite que los Estados sigan aprovechando la relativa indefinición en cuanto a su régimen jurídico para realizar acciones cibernéticas con un margen de discrecionalidad infinitamente mayor del que tendrían si el uso de la fuerza en todas sus dimensiones se hubiese reglamentado ya en clave cibernética.

La conclusión es que, en el plano político-institucional, no se están abordando los problemas técnico-jurídicos que plantea la aplicación del principio de prohibición del uso y de la amenaza de la fuerza y, entre ellos, uno primero consistente en establecer cuando una acción cibernética constituye un uso o una amenaza del uso de la fuerza armada[14]. Por ello es prioritario definir el concepto de arma cibernética. Así lo ha hecho la doctrina especializada asumiendo una perspectiva objetiva o material.

---

[12] Pueden verse, como ejemplo, las observaciones de Rusia (A/56/164/Add.1, de 3 de octubre de 2001), Estados Unidos (A/66/152, de 15 desde julio de 2011), China (A/68/98, de 2 de julio de 2007), Alemania (A/66/152, de 15 de julio de 2011 y A/68/156/Add.1, de 9 de septiembre de 2013) o Cuba (A/65/154 de 20 de julio de 2010).

[13] Pueden verse, como ejemplo, las propuestas conjuntas lideradas por Rusia y China (A/66/359 de 14 de septiembre de 2011 y A/69/723, de 13 de enero de 2015) cuando se refieren a la no realización de actividades a través de las TICs que se opongan a la tarea de mantener la paz y la seguridad internacional) o los informes de los GEG. En el informe 2015, el GEG "señala la importancia fundamental de los compromisos" de los Estados recogidos en la Carta y, entre ellos, la prohibición del uso y de la amenaza de la fuerza. Pero, al ofrecer sus opiniones, sobre la forma de aplicar el Derecho internacional a las TICs, sólo menciona expresamente en un apartado la soberanía, la igualdad soberana, la solución pacífica de controversias y la no intervención en los asuntos internos de los Estados, junto con el respeto de los derechos y libertades fundamentales. A continuación, en un párrafo distinto y con un tenor también diferente, el informe "subrayando las aspiraciones de la comunidad internacional de lograr el uso de las TICs con fines pacíficos para el bien común de la humanidad y recordando que la Carta se aplica en su totalidad, manifiesta que los Estados tienen el derecho inmanente de adoptar medidas compatibles con el derecho internacional como se reconoce en la Carta" (A/70/174 de 22 de juluo de 2015, 8 y 16).

[14] Puede verse SILVER, D.N.,"Computer Network Attack as a Use opf Force under Article 2(4) of the United Nations Charter", *International Law Studies*, vol. 76, 2002, 74.

## El concepto de arma cibernética: una perspectiva material

El objetivo es determinar el concepto de arma cibernética, esto es, cómo se define una acción cibernética capaz de constituir un uso de la fuerza prohibido por las normas de Derecho internacional[15]. No es una cuestión que tenga fácil respuesta por dos motivos principales: en primer lugar, porque supone plantearse si, cómo y cuándo las acciones y las herramientas cibernéticas pueden ser calificadas como "armas"; y, en segundo término, porque implica evaluar si la realización de esas acciones o la utilización de dichos dispositivos puede alcanzar el nivel de uso o de amenaza de la fuerza armada prohibido por la normativa internacional. Es verdad que, en sede doctrinal y en el marco político, se ha procedido a valorar como tales determinadas acciones cibernéticas. Pero es igualmente cierto que no existe un concepto jurídica o políticamente acordado, ni doctrinal o técnicamente establecido[16], y que ni siquiera se está operando respecto del ciberespacio con categorías conocidas y discutidas en el mundo físico como son los usos indirectos de la fuerza o los usos agravados cuando se produce un ataque armado o una agresión[17]. Hay diferentes aproximaciones doctrinales a esta cuestión desde planteamientos metodológicos distintos o, incluso, opuestos. Entre ellas cabría destacar las siguientes:

a) Una concepción autónoma de ciberarma que atiende materialmente al instrumento, más que a sus efectos o a la naturaleza del objetivo. Es el caso del Informe del *EastWest Institute Critical Terminology Foundations* que define el arma cibernética como el "software, firmware or hadware designed or applied to cause damage through the cyber domain"[18].

---

[15] El término "acción" se utiliza en este contexto de modo genérico para englobar cualesquiera actos, medidas, instrumentos, procedimientos o dispositivos susceptibles de ser catalogados como un uso de la fuerza.

[16] STINISSEN, J., MINÁRIK, T., PISSANIDIS, N. , VEENENDAAL, M. Y GLORIOSO, L., *A Study of Existing and Possible Rules of Engagement for Cyberspace*, Tallín, CCDCOE, 2015, 12.

[17] No sólo resulta controvertida la definición de ciberarma sino, incluso, el alcance y significado de las expresiones utilizadas para designar acciones cibernéticas como los conceptos de Computer Network Explotation (CNE), Computer Network Operation (CNO) y Computer Network Attack (CNA). Véanse, al respecto, LIBICKI, M. Cyberdeterrence and cyberwar, Santa Monica, Rand Corporation, 2009, 23-24; JOHNSON, P.A., "Is it Time for a Treaty on Information Warfare?", *International Law Studies*, vol. 76, 2002, 440-441.

[18] Por su parte, el ciberataque es "an offensive use of a cyber weapon intended to harm a designated target". Según el Informe, el término "harm" incluye "degrading, inhibiting – temporary or permanent". Se advierte, asimismo, que un ciberataque "is defined by the weapon type and not by the nature of the target" (GODWIN III, J.B., KULPIN, A., RAUSCHER, K.F. Y YASCHENKO, C., *Critical Terminology Foundations*

b) Una concepción finalista del arma cibernética que privilegia el resultado o los efectos del uso. Es la opción seguida en el Manual de Tallín que procede a la definición del arma cibernética como "cyber means of warfare that are by design, use, or intended use capable of causing either injury to, or death of, persons; or damage to, or destruction of, objects, that is, causing the consequences required for qualification of a cyber operation as an attack'"[19].

c) Una concepción analógica de ciberarma que asume su posible equivalencia con el armamento menos convencional, las armas tipo NBQ o incluso, la típica arma cinética. Esta propuesta es defendida por Simonet[20] y por Brown para quien, en realidad, hay que distinguir tres armas: el código, el sistema informático y el operador[21].

d) Las tesis negacionistas excluyen la posibilidad de calificar una acción cibernética como acción "armada" recurriendo a argumentos de distinto signo que van desde la ausencia de una práctica interestatal en ese sentido hasta el carácter más temporal que permanente de los daños o los efectos más disfuncionales que destructivos de las actividades cibernéticas[22].

e) La tesis relativista considera que el concepto de arma es, en gran medida, relativo porque se pueden utilizar muchos objetos como arma, incluso en el mundo físico, sin que

---

*2*, Nueva York, EastWest Institute, 2011, 56 y 44).

[19] Regla Nº 11, pp. 45-48. En esa línea, Boothby entiende que esta noción "would comprise any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects" (BOOTHBY, W.H., "Methods and Means of Cyber Warfare", *International Law Studies*, vol. 89, 2013, 389).

[20] Para Simonet, "des attaques informatiques pourraient relever de l'usage de la force selon la Charte, à condition toutefois que les effets de ces actes soient comparables, en termes de létalié et de destructions, à ceux d'attaques conventionnelles ou NBC (nucléaires, biologiques ou chimiques)" (SIMONET, L., "L'usage de la force dans le cyberspace et le droit international", *Revue défense nationale*, 2012, 53).

[21] Para la definición de ciberarma, según Brown, es útil establecer una analogía con el arma de fuego. Cuando un arma se dispara, la bala viaja a través del espacio y llega a un objetivo, dañándolo. El arma de fuego por sí misma no puede hacer daño porque su función es impulsar la bala a su destino. La bala sí mismo no puede hacer daño porque se convierte en mortal al ser impulsada a alta velocidad por la pistola. Por último, ni la pistola ni la bala son eficaces como arma a menos que un combatiente está presente para cargar la bala y disparar (BROWN, D., "A Proposal for An International Convention To Regulate the Use of Information Systems in Armed Conflict", *Harvard International Law Journal*, vol. 47, nº 1, 2006, 184-185).

[22] Entre los motivos de esa doctrina, Das explica que "unequivocal state practice characterizing cyber-attacks as uses of force is lacking. This is due to the Article 2(4) prohibition extending solely to state action. Very few states have definitively been identified as the initiator of cyber operations that constitute use of force". Pero, además, "the vast majority of cyber operations do not look to cause permanent damage to any system. Attacks generally look to inconvenience a user, denying him the ability to properly utilize the subject of attack" (DAS, P.R., "Linking Cyber Attacks And The Use Of Force In Public International Law: An Exercise In Interpretation", *Nalsar International Law Journal*, vol. 1, nº 1, 2015, 125 y 135).

sea ese su cometido natural o primigenio. Como exponente de esta teoría, Kolb considera que "on peut utiliser beaucoup d'objects comme armes, du moment qu'il en résulte une contrainte physique analogue à celle armée"[23]. El autor pone como ejemplo la propagación de un incendio o, en otro contexto, la contaminación medioambiental o radioactiva. En esta línea de argumentación, encaja la calificación del desplazamiento de refugiados hacia Europa como el "arma humana" utilizada por ISIS o DAESH.

En definitiva, no hay un concepto de ciberarma definido jurídicamente, aceptado institucionalmente o compartido doctrinalmente. Pero las diversas opciones expuestas no son necesariamente incompatibles o excluyentes entre sí y parecen, al menos, parcialmente coincidentes en la importancia acordada a dos extremos: el uso que se hace del dispositivo cibernético y la intencionalidad que subyace a ese uso. Ambos elementos favorecen la opción por una aproximación funcional, y no sólo material o instrumental, al concepto de arma cibernética.

## El concepto de arma cibernética: una perspectiva funcional

La adopción de un concepto funcional de arma cibernética se justifica, en principio, por dos motivos: la importancia generalmente otorgada a los elementos del uso y de la intencionalidad y la naturaleza polifuncional de la mayoría de las acciones cibernéticas.

El arma cibernética no es asimilable materialmente a un objeto, sino funcionalmente a una acción, pero no a una acción cualquiera sino a aquélla que se realiza con una determinada función y finalidad. Ello es debido a que las actividades cibernéticas son, generalmente, multi o polifuncionales en el sentido de que una misma acción, por ejemplo, una botnet puede ser utilizada con una finalidad delictiva, terrorista o bélica o ser un medio de espionaje o, incluso, de mero activismo social.

Una acción cibernética puede ser calificada como cibercriminalidad, ciberespionaje, ciberterrorismo o ciberguerra porque un mismo acto puede cumplir todas esas funcionalidades. La adscripción de ese acto dentro de esa tipología depende no sólo del acto mismo sino, también y sobre todo, de los sujetos, el autor y el destinatario, la intención y los efectos. Ni las calificaciones materiales construidas en el mundo físico

[23] KOLB, K., *Ius contra bellum. Le droit international relatif au maintien de la paix*, Bruselas, Bruylant. 2003, 183.

para definir un arma, ni la identificación de la autoría de los acciones son miméticamente extrapolables al entorno cibernético. Pero constituyen un punto básico de referencia.

Con carácter general, siguiendo la definición recogida en el *Diccionario de la Lengua de la Real Academia Española*, un arma se concibe como un instrumento, medio o máquina destinados a atacar o a defenderse siempre que, siguiendo la jurisprudencia, esa defensa haya de realizarse mediante un ataque. A partir de ahí, jurídicamente se ha operado estableciendo una distinción genérica entre los conceptos de "arma" y de "arma de guerra"[24] que responde a los paradigmas de un mundo físico donde se diferencia, conceptual y funcionalmente, entre actos criminales y acciones bélicas[25] y donde siempre ha resultado más simple atribuir la autoría de los mismos, respectivamente, a los individuos y a los Estados. Prueba de ello es que la legislación nacional remite a la normativa sobre defensa y a los acuerdos internacionales para la definición de la noción de "arma de guerra" y, además, penaliza la adquisición, tenencia o uso de ese tipo de armas por parte de los particulares[26]. Esta distinción no resulta operativa en el espacio cibernético por la naturaleza multifuncional de las acciones y dispositivos desarrollados en el mismo y porque, además, por su efecto igualador o reductor de las asimetrías[27], el ciberespacio capacita a muchos sujetos -y no sólo a los Estados- para acceder a un arma cibernética con una función bélica y no sólo criminal y para realizar acciones susceptibles de ser calificadas como acciones de guerra, ataques armados, agresiones o usos de la fuerza armada en el contexto internacional. No hay que olvidar, además, que la acción

[24] El Reglamento de Armas, aprobado por el Real Decreto 137/1993, de 29 de enero, dedica su sección 5ª, artículo 6, a las armas de guerra que tienen un régimen distinto al de las armas cuya adquisición, tenencia y uso está permitido a los particulares.

[25] Mele explica que "To reach a precise definition of the concept of cyber-weapon in the specific context of conflicts (warfare), it is necessary to separate it from the legal concept of malware, typically used for criminal purposes. It is easy to imagine how this complicates things since, as it happens for traditional weapons, a cyber-warfare case performed through malware and/or information tools, which are also used to commit mere criminal actions, might amount to a criminal offence" (MELE, S.,"Cyber-Weapons: Legal ansd Strategic Aspects", *Defense IQ*, 2013, 9).

[26] Véanse los artículos 563 a 570 del Código Penal español.

[27] Como advierte Gómez de Ágreda, el ciberespacio "vive en un estado permanente de agresión en el que todos los usuarios, sea cual sea su nivel, son susceptibles de recibir ataques con relativa independencia de su grado de protección". En su opinión, el efecto igualador que ejerce el ciberespacio sobre sus usuarios "amplía hasta el infinito el número de agresores potenciales" (GÓMEZ DE ÁGREDA, Á., "El ciberespacio como escenario de conflictos. Identificación de las amenazas", en *El ciberespacio. Nuevo escenario de confrontación*, Monografías del CESEDEN, nº 126, 2012, 180).

cibernética constituye una expresión casi extrema de la capacidad de doble uso, civil y militar, de muchos instrumentos y dispositivos[28].

Desde esos presupuestos, una acción cibernética podrá ser calificada como un arma cibernética cuando asume o cumple una función ofensiva o defensiva cuando, como tal, ha de materializarse en un ataque. La naturaleza criminal o bélica de esa acción no dependerá de la calificación como arma o como arma de guerra, ni tampoco del hecho de que la autoría corresponda a un individuo o a un Estado, sino que vendrá determinada por la combinación de los elementos que, en este otro contexto, permiten adscribir dicha acción dentro de una categoría: el subjetivo, el material y el teleológico[29]. En definitiva, una acción armada en el sentido del artículo 2.4 será aquella resultante de la concurrencia de los componentes subjetivo, material y teleológico en los términos definidos en dicha disposición.

a) Componente subjetivo

La acción armada prohibida por el artículo 2.4 de la Carta de Naciones Unidas se sitúa en un contexto exclusivamente interestatal, esto es, es aquella atribuible a un Estado y dirigida contra otro Estado. Ello excluiría una acción imputable a un agente no estatal. El problema estriba en que dentro del concepto de uso y de la amenaza de la fuerza se incluyen dos categorías específicas, el ataque armado al que hace referencia el artículo 51 de la Carta y la agresión incluida en el Estatuto de Roma y definida en la Conferencia de Kampala, que puede tener como autores a actores a no estatales.

Como consecuencia de ello, la acción cibernética será una acción armada en el sentido del artículo 2.4 cuando esté dirigida contra un Estado, entendiendo comprendido en ese concepto su territorio, población y su organización interna y exterior, incluidos sus nacionales en el extranjero. El autor habrá de ser un Estado si la acción se califica como uso o amenaza de la fuerza y podrá ser un Estado o un agente no estatal si se trata de una acción considerada ataque armado o agresión. Además del problema clave de la

[28] Puede verse OHLIN, J.D., “Remoteness and Reciprocal Risks”, *Cornell Legal Studies Research Paper*, No. 16-24, 2016, 18-22. Online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811271.

[29] Mele entiende que para la definición de ciberarma es preciso atender a tres elementos: el contexto, el objetivo y el instrumento (MELE, S.,“Cyber-Weapons: Legal ansd Strategic Aspects”, *Defense IQ*, 2013, 10).

atribución a un sujeto del acto cibernético[30], ese desajuste en la construcción subjetiva obliga a incorporar el componente objetivo o material en la definición de acción armada.

b) Componente material

Más allá de la presencia del correspondiente componente subjetivo, la acción cibernética será armada si puede ser catalogada como un uso de la fuerza, un ataque armado o una agresión. Hay consenso jurisprudencial, institucional y doctrinal en el sentido de que la agresión y el ataque armado constituyen uso de la fuerza, pero no a la inversa porque no todo uso de la fuerza encaja en las otras categorías[31]. No existe, sin embargo, una delimitación clara y definitivamente establecida entre ellas y resulta aún más compleja en el entorno cibernético.

Hay diversas propuestas doctrinales para proceder a esa delimitación conceptual: la teoría de la escala y los efectos, el recurso a los criterios teleológico y funcional o la introducción del ingrediente de la intencionalidad. Con carácter general, el daño y/o destrucción en las cosas y el daño y/o muerte en las personas parecen ser la clave para identificar la existencia de un uso de la fuerza y puede que, incluso, según parte de la doctrina, para distinguir entre esa modalidad y el ataque armado o la agresión. Katharina

---

[30] A diferencia de lo que ocurre con carácter general en el marco del Derecho internacional, donde la autoría determina la atribución que, a su vez, establece la responsabilidad internacional del Estado, en el mundo virtual, la situación es más compleja. El ciberespacio complica la determinación de la autoría porque, además de caracterizarse en términos generales por la presencia del anonimato y la opacidad, exige dos operaciones y presenta dos aspectos diferentes: la trazabilidad, de carácter técnico y la atribución de naturaleza jurídica. La trazabilidad constituye un problema principal en la determinación de la autoría de un Estado. Como explica Moore, "While it may seem fairly straightforward that a state is held responsible for the action of its agents, the difficulty lies in the subtle nature of cyber attacks. For instance, cyber attack technologies are not as readily detectable as chemical or nuclear weapons. Instead, "a nation [can] hide its cyber weapons on thumb drives or CDs anywhere in the country."Perhaps for this reason, to date, no cyber attack has been conclusively attributed to a state" (MOORE, S., "Cyber Attacks and the Beginnings of an International Cyber Treaty", *North Carolina Journal of International Law*, vol. XXXIX, 2013, 243).

[31] En el asunto Nicaragua, el Tribunal Internacional de Justicia apunta en esa dirección cuando afirma la necesidad de distinguir "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms", such as a "mere frontier incident", based on the "scale and effects" of the force involved" (Sentencia de 27 de junio de 1986, Rec. 1986, párr. 227-238). En el marco de la OTAN se reconoce que "A well-known difference between the above-mentioned provisions of the Charter is that the prohibition in Article 2 (4) is wider than the exception in Article 51, which only allows countermeasure including use of force when an armed attack occurs" (*NATO Legal Deskbook*, MC 362/1 de la OTAN, 233). Entre la doctrina, Schmitt sostiene que "all armed attacks are uses of force [within the meaning of Article 2], but not all uses of force qualify as armed attacks that are a prerequisite to an armed response" (SCHMITT, M.N., "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," en *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, National Academies Press, 2010, 163. Online: http://books.nap.edu/openbook.php?record_id=12997&page=R1).

Ziolkowski avanza en ese concepto considerando que "it can be assumed that malicious cyber activities can be considered use of [armed] force in the meaning of Article 2(4) of the UN Charter if they – indirectly – result in: 1) death or physical injury to living beings and/or the destruction of property; 2) massive, medium to long-term disruption of critical infrastructure systems of a State (if in its effect equal to the physical destruction of the respective systems"[32]. Pero no hay uniformidad a ese respecto en sede doctrinal y ninguna de las diversas opciones posibles ha recibido una confirmación de su operatividad en la práctica interestatal. El caso más complejo se manifiesta en la agresión, a pesar de haber sido definida después de la Conferencia de Kampala, porque, atendiendo a sus contenidos, no siempre resulta fácil discernir sus diferencias con los otros supuestos y porque la calificación de una acción como tal depende del Consejo de Seguridad si se trata de un acto atribuible a un Estado o también de la Corte Penal Internacional si es la acción de un individuo.

Pero es que, además, la calificación de una acción cibernética dentro de cada uno de los tipos en presencia va a depender, también, necesariamente del componente teleológico.

c) Componente teleológico

La definición de una acción cibernética como acción armada exige atender a su componente teleológico donde concurren dos elementos: la intención del autor y los efectos de la acción. Ninguno de ellos está exento de problemas.

La intencionalidad se ha utilizado doctrinalmente bien para determinar la existencia de un uso de la fuerza, bien para cualificarlo como un ataque armado o, en alguna medida, una agresión. Pero hay, al menos, tres problemas. En primer término, la intencionalidad, que es una categoría bien conocida en derecho interno, no es un componente del régimen de responsabilidad internacional de los Estados que se apoya en dos elementos objetivos: el material, la existencia de un hecho ilícito, y el subjetivo, la atribución de ese hecho a un Estado o a un sujeto internacional. En segundo lugar, aun excluyendo ese dato y en relación con los actos de los actores no estatales, si la intención es un criterio para determinar que se ha realizado una acción armada habría que demostrar que ha

[32] K. Ziolkowski, "Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt Criteria" for Use of Force", en C. Czosseck, R. Ottis, K. Ziolkowski (Eds.), *4th International Conference on Cyber Conflict*, Tallín, CCD COE, 2012, 173-174.

existido la intención de usar o amenazar con el uso de la fuerza, de realizar un ataque armado o de cometer una agresión, esto es, dilucidar la intención concreta del autor de la acción cibernética, primero, para definirla como armada y, después, para ubicarla en uno de esos supuestos cuya delimitación material no es conclusiva ni completamente cierta. Por último, en el caso de que no se produzca el efecto esperado con la acción armada cibernética, la intención podría tener o no consecuencias jurídicas porque las tiene en derecho interno respecto de los individuos, pero no en Derecho internacional respecto de los Estados.

A pesar de ello, la intención es un factor que cobra en el ciberespacio una entidad de la que carece en el mundo físico en el marco de las relaciones interestatales. En este contexto, las acciones y los instrumentos utilizados por los Estados pueden ser objeto de una calificación relativamente fácil comparada con la complejidad que presenta a esos efectos el espacio cibernético. En el primero, un acto bélico es diferenciable de un acto de espionaje, mientras que, en el entorno virtual, una misma acción puede cumplir ambas funcionalidades y su calificación dependerá de la intención del autor.

Por su parte, los efectos de la acción cibernética se manifiestan también como un elemento clave para determinar su naturaleza como acción armada. La presencia de daño y/o destrucción en las cosas o de daño y/o muerte en las personas puede llevar a dudar sobre su consideración concreta como uso de la fuerza, ataque armado o agresión, pero es indudablemente un supuesto de uso de la fuerza armada por tratarse de la categoría genérica que engloba a las demás cuando la autoría es atribuible a un Estado y sería un acto criminal si sólo admite esa consideración –y no la de ataque armado o agresión- en el caso de un agente no estatal.

Un problema adicional en lo concerniente a los efectos estriba en que, por su naturaleza, la acción cibernética puede tener consecuencias más disfuncionales o disruptivas que destructivas y más temporales que permanentes. Ello obliga a superar el criterio de la capacidad destructiva de la acción cómo único o principal baremo a la hora de determinar que se trata de una acción armada o a atemperarlo atendiendo a las circunstancias diferentes del entorno ciberespacial.

## Conclusiones

La articulación de un concepto de arma cibernética es necesario porque, desde el final de la Segunda Guerra Mundial, el modelo de seguridad creado para garantizar el mantenimiento de la paz y de la seguridad internacional se ha construido, principal aunque no exclusivamente, sobre la base del principio de prohibición del uso y de la amenaza del uso de la fuerza armada, tanto en su alcance y contenido, como en sus excepciones. Este principio de naturaleza imperativa recogido en el artículo 2.4 de la Carta de Naciones Unidas se aplica a las acciones de los Estados en el mundo físico y también en el virtual pero, en términos operativos, no basta con actuar por mero mimetismo y sin apreciar las marcadas diferencias que a esos efectos introduce el entorno virtual. La práctica internacional muestra que las acciones ciberespaciales forman parte integrante de las estrategias de seguridad y defensa de los Estados y que la conflictividad cibernética está creciendo exponencialmente tanto en el marco de situaciones de conflicto armado como fuera de ellas.

Un problema principal a la hora de extrapolar dicho principio al espacio cibernético, aunque no el único, es la construcción de un concepto de arma cibernética cuyo uso podría ser considerado una contravención del principio que prohíbe el uso y la amenaza de la fuerza armada. La definición de ese concepto desde una perspectiva objetiva o instrumental no sólo plantea problemas de orden teórico o práctico, sino que tampoco se ha traducido en un consenso doctrinal y menos aún político o normativo.

En mi opinión, el concepto de arma cibernética debería definirse desde una aproximación funcional por varios motivos: en primer lugar, por la naturaleza multi o polifuncional de las acciones cibernéticas y por la importancia que esa circunstancia imprime en el uso que se hace del medio o dispositivo cibernético y de la intencionalidad que subyace a ese uso; en segundo término, porque la calificación de una acción cibernética como acción armada en el sentido del Derecho internacional obliga a operar combinando los componentes subjetivo, material y teleológico porque va a depender no sólo de la acción en sí misma sino, también y muy particularmente, del autor, el destinatario, la intención

y los efectos; y, en tercer lugar, no en orden de importancia, porque el concepto de arma cibernética debe ser un concepto funcional dinámico, en lugar de instrumental o estático, y capacitado, además, para absorber los potenciales resultados del avance tecnológico futuro en esta materia que, aun siendo todavía desconocidos, no pueden ni han de ser inesperados.

[i]

*Margarita Robles Carrillo* *****
Profesora Titular Derecho Internacional Público y RR.II.
Universidad de Granada