Capítulo cuarto

De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio

Jacobo de Salas Claver

Resumen

Se ha creado oficialmente un nuevo ámbito de operación, el ciberespacial, transversal al resto de ámbitos tradicionales, y en el que ya se han producido acciones ofensivas reales. En este trabajo se pretenden exponer, de forma práctica y para los no juristas, algunas de las principales consideraciones jurídicas a tener en cuenta en el planeamiento y ejecución de acciones ofensivas en el ciberespacio en el marco de los conflictos armados.

Palabras clave

Ciberguerra, ciberataque, ciberdefensa, ciberderecho, derecho internacional humanitario, derecho de los conflictos armados, Tallin 2.0, Internet.

Abstract

A cyberdomain has been oficially established. It cross sections the other domains, and for real cyberattacks have already been executed within it. The aim of this work is to show, in practical terms and to non-laywers, some of the main legal issues to be taken into account for the planning and execution of cyberattacks within an armed conflict.

Keywords

Cyberwar, cyberattack, cyberdefense, cyberlaw, international humanitarian law, law of armed conflict, Tallin 2.0, internet.

Introducción

La causa: la sociedad del siglo XXI y la lex artis

Las actividades profesionales de una sociedad contemporánea no se pueden entender sin dos circunstancias de naturaleza mixta, fáctica y normativa, como son los protocolos o procedimientos de actuación profesional y la buena práctica profesional o *lex artis* respectivamente. En efecto, a estas alturas del siglo xxi, en toda actividad profesional humana se exige a quien la desarrolle que su actuación no se limite a cumplir con las normas positivas en vigor, sino que además dicha actividad profesional sea conforme a la *lex artis*, que siendo un concepto jurídico indeterminado, puede considerarse como el conjunto de prácticas profesionales generalmente aceptadas como adecuadas por la comunidad profesional para el desarrollo de la actividad profesional orientada a la consecución de un determinado propósito. Y, a su vez, una concreta actuación profesional estará amparada bajo la *lex artis* cuando el operador actúe conforme a los procedimientos y protocolos generalmente admitidos por la comunidad profesional como adecuados para la obtención del fin perseguido.

Podría pensarse que dichas circunstancias son exclusivamente propias de actividades civiles y, singular o tradicionalmente, de la medicina. Sin embargo, no podemos olvidar que el artículo 62 de las Reales Ordenanzas[1] dispone, con respecto a la toma de decisiones por el mando, que «en el ejercicio de su actividad será prudente en la toma de decisiones, fruto del análisis de la situación y la valoración de la información disponible, y las expresará en órdenes concretas, cuya ejecución debe dirigir, coordinar y controlar, sin que la insuficiencia de información, ni ninguna otra razón, pueda disculparle de permanecer inactivo en situaciones que requieran su intervención». Y en consecuencia, la reciente publicación *Doctrina para el empleo de las Fuerzas Armadas*[2] puede ser considerada como un ejemplo de esta situación contemporánea de establecimiento de *lex artis* para el uso de la fuerza militar. En efecto, en el prólogo de esta publicación el JEMAD afirma que esta doctrina «describe la forma de empleo de las Fuerzas Armadas y establece las normas fundamentales con las que estas operan» y, singularmente, que «... la doctrina establece y detalla los principios morales, legales y doctrinales, determina cómo ejecuta la acción conjunta, la combinada con nuestros aliados, y la integrada con los demás instrumentos de poder; describe el entorno y el espacio de las operaciones, añadiendo a los ámbitos físicos tradicionales, el ciberespacial y el formado por la información y las percepciones; indica

[1] Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas.

[2] ESTADO MAYOR DE LA DEFENSA. Publicación Doctrinal Conjunta PDC-01(A). *Doctrina para el empleo de las Fuerzas Armadas*. Madrid: Ministerio de Defensa, 2018, p. 5.

cómo sincronizar el planeamiento concurrente y la ejecución dinámica de operaciones en los niveles estratégico, operacional y táctico; y, por último, ayuda a reflexionar sobre el ejercicio del mando en operaciones».

El ámbito ciberespacial es nuevo y esencialmente propio del siglo xxi. Por este motivo, puede razonablemente pensarse que haya una cierta carencia de principios o procedimientos generalmente admisibles en el ámbito de las acciones ofensivas en el ciberespacio (AOC) derivada precisamente de la juventud de este ámbito de operación y de la correlativa lógica ausencia de tratados internacionales o de jurisprudencia relevante que guíe a los operadores, al mando, y a sus asesores legales. Y así llegamos a lo que es el propósito de este capítulo, que es intentar facilitar al lector una primera aproximación a las consideraciones jurídicas propias de las AOC.

Nótese, en todo caso, que este trabajo ni pretende abarcar todas las perspectivas posibles sobre la materia, pues expresamente se deja fuera del mismo a las consideraciones jurídicas propias del *ius ad bellum*, ni tampoco aspira a constituirse en la fuente interpretativa de la aplicación del *ius in bello* en el ámbito del ciberespacio, ni mucho menos pretende agotar sus múltiples perspectivas. Lo reciente del ámbito de operación, las distintas aproximaciones a los problemas de este por las diferentes tradiciones jurídicas o intereses nacionales de los distintos operadores y, en fin, la aplicación del principio de prudencia ante la incertidumbre, impiden poder facilitar respuestas simples a problemas complejos. No obstante estas limitaciones, este trabajo pretende facilitar una visión clara y coherente de las reglas de este nuevo *juego*, para que la valoración jurídica de las AOC sea razonablemente objetiva, coherente y defendible legalmente. Por último, este trabajo pretende facilitar al lector las referencias literales de algunas de estas reglas, pues difícilmente se puede juzgar, o aplicar en la actividad diaria, lo que se desconoce.

Las acciones ofensivas en el ciberespacio ya están aquí, y son relevantes

Del mismo modo que tras el ataque aéreo británico a la flota italiana fondeada en Tarento en la noche del 11 de noviembre de 1940 ya no se podía decir que el ataque japonés el 7 de diciembre de 1941 a Pearl Harbor fuera una sorpresa conceptual[3], en la actualidad las AOC ya no pueden considerarse como meras hipótesis de futuro. Según un informe del Cato Institute, entre los años 2000 y 2016 se han documentado 272 ciberoperaciones entre Estados rivales[4].

[3] O un «cisne negro», en los términos de Nassim Nicholas Taleb en su conocido libro homónimo (TALEB. Niassim Nicholas, «*The Black Swan*». New York: Random House, 2007).

[4] VALERIANO, Brandon, y JENSEN, Benjamin. «The Myth of the Cyber Offense». *Policy Analysis*. Number 862. Cato Institute, 2019, p. 4.

Las AOC son, por su objeto, relevantes y deben ser causa de severa preocupación. Las sociedades del siglo XXI dependen de los sistemas y tecnologías de la información para la gestión de sus instalaciones críticas, tales como centrales de energía (incluyendo plantas nucleares y presas), sistemas de tratamiento y distribución de agua potable, refinerías de petróleo y gas, sistema bancario y financiero, hospitales, centros de salud e instalaciones de almacenaje y distribución de medicamentos y sistemas ferroviario y aeronáutico. Estos sistemas y tecnologías de la información constituyen el enlace entre el mundo físico y el digital, y son altamente vulnerables a ataques maliciosos[5]. Solo tenemos que pensar qué ocurriría en una sociedad occidental de corte urbano si el sistema bancario de un país estuviera fuera de servicio durante un par de semanas (y además con incertidumbre sobre la fecha de restablecimiento); o el sistema eléctrico, con las repercusiones que ello tendría sobre la cadena de frío y los sistemas de transporte de alimentos.

De hecho, ya se ha considerado que se han producido AOC como parte de un conflicto armado[6]. Efectivamente, en el ámbito de la intervención rusa en la península de Crimea en 2014, el sistema eléctrico ucraniano fue atacado el 23 de diciembre de 2015, infiltrando *software* malicioso en los sistemas de tres compañías eléctricas, con el efecto de causar un apagón durante varias horas en una gran zona urbana. Posteriormente, los días 17 y 18 de diciembre de 2016, se produjo un nuevo apagón en parte de la ciudad de Kiev como consecuencia de que una estación de distribución eléctrica quedase fuera de servicio tras ser infectados sus sistemas con una versión del conocido virus Stuxnet. Se puede decir, entonces, que ya se ha producido una ciber versión del ataque de Tarento, por lo que ya no hay excusas admisibles ante la ciber versión del ataque a Pearl Harbor.

Ámbito del ciberespacio

La definición militar española para el ciberespacio se contiene en la Doctrina para el empleo de las Fuerzas Armadas, que describe el ámbito ciberespacial como «... el ámbito artificial compuesto por infraestructuras, redes, sistemas de información y telecomunicaciones y otros sistemas electrónicos, por su interacción a través de las líneas de comunicación sobre las que se propaga y el espectro electromagnético (EEM), así como por la información que es almacenada o transmitida a través de ellos. Es transversal a los demás ámbitos y no está sujeto a un determinado espacio geográfico.

[5] DROEGE, Cordula. «Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians». *International Review of the Red Cross*. Volume 94, Number 886, Ginebra, 2012, p. 538.

[6] EFRONY, Dan y SHANY, Yuval. «A Rule Book on the Shelf? Tallin Manual 2.0 on Cyber Operations and Subsequent State Practice». *Hebrew University of Jerusalem Legal Studies Research Paper* Series No. 18-22. Jerusalem: The Hebrew University of Jerusalmen Faculty of Law, 2018, p. 38.

Le caracteriza su extensión, el anonimato, la inmediatez y su fácil acceso. Finalmente, su carácter artificial y su rápida evolución generan continuas vulnerabilidades y oportunidades»[7]. Esta definición trae causa de la primera definición del ciberespacio en el ordenamiento patrio[8], que tuvo lugar en la Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas[9], y que definió el ciberespacio como el «dominio global y dinámico compuesto por infraestructuras de tecnología de la información –incluyendo Internet–, redes de telecomunicaciones y sistemas de información».

Sin embargo, lo cierto es que el concepto de ciberespacio no es objeto de consenso. Las Fuerzas Armadas de Estados Unidos definen el ciberespacio como «un ámbito global[10] dentro del entorno de la información consistente en redes interdependientes de infraestructuras de tecnologías de la información y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y controladores y procesadores empotrados»[11]. El *Manual de Tallin 2.0*, probablemente el documento doctrinal sobre operaciones en el ciberespacio de mayor consenso internacional, define el ciberespacio como «el entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos usando redes informáticas»[12].

En todo caso, más allá de discusiones doctrinales, lo auténticamente relevante de la definición no es tanto la misma como los elementos que se incluyen en lo definido o, por utilizar el vocabulario generalmente admitido, sus capas. En términos generales, el ciberespacio está formado por cuatro capas interdependientes: (i) la capa física o de *hardware*, (ii) la capa lógica o de *software*, (iii) la capa de contenidos, consistente en la información captada, almacenada o procesada, y (iv) la capa personal, consistente en las personas físicas o jurídicas que actúan en el ciberespacio. Y es en esas capas o contra

---

7 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, doc. cit., p. 81.

8 DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas,* pendiente de publicación.

9 *BOE* de 26 de febrero de 2013.

10 Los otros ámbitos globales para EE. UU. son el terrestre, marítimo, aéreo y el espacial: Headquarters, Department of the Army. *Field Manual 3-38 Cyber Electromagnetic Operations*. Washington, 2014, p. 1-5. Disponible en https://fas.org/irp/doddir/army/fm3-38.pdf. Sin embargo, nótese que para España los ámbitos de operación son el terrestre, marítimo, aeroespacial, cognitivo y ciberespacial. ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, doc. cit., p. 79. La OTAN también considera el ciberespacio como un ámbito de operación. Vid. el apartado 70 del NATO, Warsaw Summit Communiqué, 9 de julio de 2016. Disponible en https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

11 US JOINT CHIEFS OF STAFF. *Joint Publication 3-12: Cyberspace Operations*. 2018, p. GL-4. Disponible en https://fas.org/irp/doddir/dod/jp3_12.pdf.

12 VV. AA. *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, 2017, p. 564.

esas capas contra las que se pueden realizar AOC[13] o fuera de él, pues Israel no ha dudado en lanzar un ataque aéreo para destruir un edificio (y los objetos y personas que contenía) que ha descrito como el *ciber cuartel general de Hamas*[14] y desde el cual se había lanzado un cibertaque contra un objetivo civil no identificado en Israel. Consecuentemente, dado que los datos y los sistemas de información permean todas las áreas de actividad humana, la doctrina militar española considera que el ciberespacio da lugar a un ámbito mixto de operación que es «de especial interés para las operaciones por ser de frecuente y necesario empleo, por implicar una dificultad añadida por la coordinación de las acciones y por requerir procedimientos no solo específicos sino además conjuntos»[15]. Y así, se ha configurado el «area de operaciones de ciberdefensa (AOCD)» como «la parte del ciberespacio en que, de manera permanente o puntual, se ejecutan operaciones militares. Está formado de manera permanente por todas las redes y sistemas de información y telecomunicaciones empleadas por el Ministerio de Defensa y las de potenciales adversarios, y de manera eventual, por las de adversarios o terceros que estuvieran afectando, o pudieran afectar, a las operaciones, así como por las de aquellos otros cuya protección le sea encomendada a las Fuerzas Armadas»[16]. Este va a ser el campo de tiro de las actuales flechas que son los ratones de los ordenadores.

El problema de la atribución

La atribución es un problema que, en general, es anterior a una AOC en el ámbito de los conflictos armados, por corresponderse a la imputación de responsabilidad por una ciberoperación que no alcanza el nivel de uso de la fuerza o de ataque armado; o de realizarse dentro de un conflicto armado, por ser realizada por un Estado o por haberse realizado por un actor no estatal. Por ese motivo, la cuestión de la atribución no va a ser objeto de consideración en el presente trabajo; sin embargo, por la indudable relación de un *ciberataque* con una AOC en el ámbito de los conflictos armados, nos parece que al menos deben dejarse apuntados determinados elementos a

---

13 CORN, Gary P. «Cyber National Security: Navigating Grey Zones Challenges In and Through Cyberspace» pendiente de publicación en *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*. 2017 pp. 9 y 10. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3089071. Véase también DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual Derecho de las Operaciones Aéreas, pendiente de publicación.

14 SCALITER, Juan. «Guerra híbrida: detener "*hackers*" con misiles». Diario *La Razón*, 8 de mayo de 2019, p. 46 y 47. Vid. también CHESNEY, Robert. «Crossing a Cyber Rubicon? Overreactions to the IDF's Strike on the Hamas Cyber Facility». www.lawfareblog.com. 8 de mayo de 2019. Accesible en https://www.lawfareblog.com/crossing-cyber-rubicon-overreactions-idfs-strike-hamas-cyber-facility.

15 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, doc. cit., p. 79.

16 Ibídem, p. 84.

tener en consideración para la imputación de responsabilidad por quien ha sufrido un ataque cibernético.

El primero de ellos es que los potenciales adversarios pueden incardinarse en una de las tres siguientes categorías:

a) Estado/s o coalición de Estados u organización internacional. En esta categoría se incluyen las fuerzas armadas de un país, sus servicios de inteligencia o policiales, o la administración civil.

b) Actores no estatales, entre los cuales están las organizaciones terroristas, las milicias o guerrillas insurgentes y el crimen organizado.

c) Adversarios por delegación o proxies, que son los actores no estatales o Estados débiles empleados de forma encubierta por un tercer Estado adversario con la finalidad de alcanzar sus propios objetivos. De esta forma, el tercer Estado y su proxy forman en cierta manera un solo conjunto[17].

El segundo elemento a tener en consideración es que en ciberataques el anonimato es la regla, lo que implica que deberá realizarse una investigación *forense* (policial, judicial, informática y/o militar, según proceda en cada caso) para la determinación de quién es el autor material del ataque[18].

Y el tercer elemento a tener en consideración es en qué circunstancias los ataques realizados por actores no estatales o proxies pueden ser imputados a un Estado, lo que entra de lleno en la cuestión jurídica de la atribución de responsabilidad a un Estado por hechos ajenos[19]. La doctrina[20], en general, considera que las reglas que regulan esta cuestión se contienen en el proyecto de *Artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*[21] que ha elaborado la Comisión de Derecho Internacional de

---

17 Ibídem, p. 87.

18 Vid. DROEGE, Cordula. *Op. cit.,* p. 544. Véase también el capítulo «Back-Tracking and Anonymity in Ciberspace» de PIHELGAS, Mauno en ZIOLKOWSKI, Katharina (ed.) *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. *NATO CCD COE Publication*. Tallin 2013, pp. 31 y ss.

19 La responsabilidad de un Estado por sus propios actos en principio entra de lleno en el sentido común y, en todo caso, se determina en las reglas 14 y 15 del *Manual de Tallín 2.0.*

20 Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación; y el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo en RODRÍGUEZ, José Luis, y LÓPEZ, Joaquín (coords) *Derecho Internacional Humanitario*. Valencia: ed. Tirant lo Blanch y Cruz Roja Española (Centro de Estudios de Derecho Internacional Humanitario), 2017, p. 627. Véase también SCHMITT, Michael N. «Grey Zones in the International Law of Cyberspace». *The Yale Journal of International Law Online*. 2017. Disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180687

21 Disponible en http://portal.uned.es/pls/portal/PORTAL.wwsbr_imt_services.GenericView?p_docname=22634788.PDF&p_type=DOC&p_viewservice=VAHWSTH&p_searchstring=

la Asamblea General de las Naciones Unidas, cuyo artículo 8 establece que «se considerará hecho del Estado según el derecho internacional el comportamiento de una persona o de un grupo de personas si esa persona o grupo de personas actúa de hecho por instrucciones o bajo la dirección o control de ese Estado al observar ese comportamiento».

Siendo aparentemente claro que cuando una persona o grupo de personas actúe siguiendo «instrucciones» de un Estado, esas acciones se imputarán jurídicamente a dicho Estado, el segundo inciso de ese artículo 8 puede ser interpretado de dos formas distintas, en función de si se considera que se puedan imputar a un Estado las acciones realizadas por una persona o grupo de personas bajo su control *efectivo* o, alternativamente, basta que ese control sea *genérico* para realizar tal imputación[22] y, consecuentemente, se puedan exigir las responsabilidades procedentes.

A su vez, el *Manual de Tallin 2.0* parte del precedente de los *Artículos sobre la responsabilidad del Estado por hechos internacionalmente ilícitos*[23] y, consecuentemente, tiene un enfoque similar, pero algo más amplio, en su regla 17, según la cual «las ciberoperaciones ejecutadas por un actor no estatal se imputan a un Estado cuando: (a) se realizan siguiendo sus instrucciones o bajo su dirección o control, o (b) el Estado reconoce y adopta la operación como propia».

Como puede verse, por tanto, la cuestión de la atribución tiene una perspectiva fáctica, que es la de la prueba de que unos determinados actos cibernéticos han sido realizados por una determinada persona, física o jurídica, y una perspectiva jurídica, que es la de la acreditación de que esa persona sigue las instrucciones de un Estado o actúa bajo su dirección o control.

Marco legal del empleo de las Fuerzas Armadas

Si aceptamos que hoy en día la máxima latina de *inter armas silent leges*[24] ya no está en vigor, y los procesos de Nuremberg y Tokio y el Tribunal Penal Internacional están ahí para recordarlo[25], debemos tener presente –siquiera de forma somera– que el hecho de que una acción ofensiva de las Fuerzas Armadas se realice en el ámbito del ciberespacio no exime a aquella del marco legal de empleo de la fuerza por las Fuerzas Armadas.

---

22 Michael N. Schmitt, uno de los principales autores en la materia, considera que el control debe ser «efectivo» y no meramente «genérico» basándose en la sentencias Nicaragua y Genocidio en Bosnia del Tribunal Internacional de Justicia. SCHMITT, Michael N. «Gray Zones...» *op. cit*., pp. 9 y 10. En similar sentido se pronuncian los comentarios 5, 6 y 7 de la regla 17 del *Manual de Tallin 2.0*.

23 VV. AA. *Tallin Manual 2.0... op. cit.*, p. 95.

24 En tiempo de guerra la ley calla.

25 Ciertamente nunca se ha derogado la aplicación de la máxima latina *Vae victis*, Ay de los vencidos.

En efecto, el artículo 20 de la Ley Orgánica de Defensa Nacional[26] dispone que mediante ley se establecerán las reglas esenciales que definen el comportamiento de los militares, y que el Gobierno por Real Decreto desarrollará dichas reglas en las Reales Ordenanzas. El complemento legal de la Ley Orgánica de Defensa Nacional es la Ley Orgánica de Derechos y Deberes de los miembros de las Fuerzas Armadas[27], que regula en su artículo 6 las reglas esenciales que definen el comportamiento del militar. Entre estas, a los efectos de este trabajo, destacaremos las siguientes reglas:

> Quinta. Ajustará su conducta al respeto de las personas, al bien común y al derecho internacional aplicable en conflictos armados. La dignidad y los derechos inviolables de la persona son valores que tienen obligación de respetar y derecho a exigir. En ningún caso los militares estarán sometidos, ni someterán a otros, a medidas que supongan menoscabo de la dignidad personal o limitación indebida de sus derechos.
>
> Sexta. En el empleo legítimo de la fuerza, hará un uso gradual y proporcionado de la misma, de acuerdo con las reglas de enfrentamiento establecidas para las operaciones en las que participe.
>
> Duodécima. Si las órdenes entrañan la ejecución de actos constitutivos de delito, en particular contra la Constitución y contra las personas y bienes protegidos en caso de conflicto armado, el militar no estará obligado a obedecerlas y deberá comunicarlo al mando superior inmediato de quien dio la orden por el conducto más rápido y eficaz. En todo caso asumirá la grave responsabilidad de su acción u omisión.

Y, finalmente, las Reales Ordenanzas de las Fuerzas Armadas[28] disponen:

> Artículo 84. Uso legítimo de la fuerza. En el empleo legítimo de la fuerza, el militar hará un uso gradual y proporcionado de la misma, de acuerdo con las reglas de enfrentamiento establecidas para las operaciones en las que participe.
>
> Artículo 85. Principio de humanidad. Su conducta en el transcurso de cualquier conflicto u operación militar deberá ajustarse a las normas que resulten aplicables de los tratados internacionales en los que España fuera parte, relativos al derecho internacional humanitario.
>
> Artículo 106. Deberes en relación con el derecho internacional humanitario. El militar conocerá y difundirá, así como aplicará en el transcurso de cualquier conflicto armado u operación militar, los convenios internacionales ratificados por España relativos al alivio de la suerte de heridos,

[26] Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

[27] Ley Orgánica 9/2011, de 27 de julio, de Derechos y Deberes de los Miembros de las Fuerzas Armadas.

[28] Real Decreto 96/2009, de 6 de febrero, por el que se aprueban las Reales Ordenanzas para las Fuerzas Armadas.

> enfermos o náufragos de las fuerzas armadas, al trato a los prisioneros y a la protección de las personas civiles, así como los relativos a la protección de bienes culturales y a la prohibición o restricciones al empleo de ciertas armas.
>
> Artículo 111. Principio de distinción. En el transcurso de cualquier operación tendrá en cuenta el principio de distinción entre personas civiles y combatientes y entre bienes de carácter civil y objetivos militares para proteger a la población civil y evitar en lo posible las pérdidas ocasionales de vidas, sufrimientos físicos y daños materiales que pudieran afectarle.
>
> Artículo 113. Protección de bienes culturales. No atacará ni hará objeto de represalias o de actos de hostilidad a bienes culturales o lugares de culto claramente reconocidos, que constituyen el patrimonio cultural y espiritual de los pueblos y a los que se haya otorgado protección en virtud de acuerdos especiales. Evitará la utilización de dichos bienes culturales o de instalaciones que se encuentren próximas a ellos para propósitos que puedan exponerlos a la destrucción o al deterioro.
>
> Artículo 114. Medios y métodos de combate. No utilizará medios o métodos de combate prohibidos por el derecho internacional humanitario que puedan causar males superfluos o sufrimientos innecesarios, así como aquellos que estén dirigidos a causar o puedan ocasionar extensos, graves y duraderos perjuicios al medio ambiente, comprometiendo la salud o la supervivencia de la población.

España, como hemos visto, ha asumido legalmente las reglas propias del derecho internacional humanitario para su actuación en el ámbito de los conflictos armados, y en la actualidad, con todas las salvedades que se quieran poner, es una cuestión prácticamente pacífica internacionalmente que las reglas propias del derecho internacional humanitario se aplican a las AOC[29]. En todo caso, sería un error considerar a las reglas legales nacionales o propias del derecho internacional humanitario como meras limitaciones jurídicas a la acción ciberofensiva. Como bien reconoce la doctrina española, «la legitimidad en el uso de la fuerza consiste en actuar conforme a las leyes, los mandatos, los compromisos suscritos por España y al código moral de las Fuerzas Armadas españolas»[30]. Y no solo ello, en una sociedad audiovisual y ya 4.0, «tan importante es que se opere legítimamente como que sea percibido así por la opinión pública propia, la de las naciones que participan en las operaciones, la comunidad internacional, y la población local de la

[29] Véase el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo, en RODRÍGUEZ, José Luis, y LÓPEZ, Joaquín (coord.). *Derecho Internacional Humanitario*. Valencia: Ed. Tirant lo Blanch y Cruz Roja Española (Centro de Estudios de Derecho Internacional Humanitario), 2017, p. 622.

[30] ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A). Doctrina para el empleo de las Fuerzas Armadas*, *op. cit.*, p. 73.

zona donde se desarrolla la operación»[31]. Vietnam es claramente una lección aprendida.

El Mando Conjunto de Ciberdefensa

La Directiva de Defensa Nacional de 2012 declaraba que «España debe estar preparada para hacer frente a los riesgos de un mundo en el que la interconexión, la calidad y velocidad con que fluye la información, la gestión telemática de las transacciones, la libertad de movimientos y de intercambios comerciales, cuyos beneficios son tan evidentes para la sociedad, no configuren un escenario en el que jueguen con ventaja grupos terroristas y de la delincuencia organizada con capacidad para dañar gravemente la paz social, la seguridad ciudadana, la estabilidad política y la prosperidad general», y además reconocía que los ataques cibernéticos son «hipótesis nada alejadas de la realidad ya presente»[32]. A su vez, la *Estrategia de Seguridad Nacional de 2017* asumió expresamente que una de las tendencias actuales en los conflictos armados era el aumento de «capacidades en otros dominios como el ciberespacio», por lo que establecía como una de las líneas de acción en el ámbito de la ciberseguridad el «reforzar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta e investigación frente a las ciberamenazas»[33].

Y entre esos marcos conceptuales llegamos a la determinación de quién va a teclear o a manejar el ratón en las acciones ciberofensivas; o, dicho de otra forma, quién en el ámbito de las Fuerzas Armadas va a ejecutar la AOC por parte de España en un conflicto armado. Podremos encontrar la respuesta después de la *Directiva de Defensa Nacional de 2012*, que quizás estaba muy influenciada por una visión multilateral de la seguridad, y antes de la *Estrategia de Seguridad Nacional de 2017*, que quizás tuviera una visión más nacional de las responsabilidades de defensa. En ese período se dictó la Orden Ministerial 10/2013[34] de creación del Mando Conjunto de Ciberdefensa, dependiente del Jefe del Estado Mayor de la Defensa, encuadrándolo orgánicamente en el Estado Mayor de la Defensa como parte de la estructura operativa de las Fuerzas Armadas[35]. A este Mando Conjunto se le asigna el planeamiento y ejecución de las acciones relativas a ciberdefensa militar

[31] Ibídem, p. 74.

[32] Directiva de Defensa Nacional 1/2012, disponible en http://www.defensa.gob.es/Galerias/defensadocs/directiva-defensa-nacional-2012.pdf. Fecha de la consulta 8 de abril de 2019.

[33] *Estrategia de Seguridad Nacional 2017*, disponible en http://www.defensa.gob.es/Galerias/defensadocs/Estrategia_Seguriad_Nacional_2017.pdf. Fecha de la consulta 8 de abril de 2017.

[34] Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

[35] Artículos 4, 9 y 15 del Real Decreto 872/2014, por el que se establece la organización básica de las Fuerzas Armadas.

y, específicamente, le encomienda en su artículo 5.5 a «ejercer la respuesta oportuna, legítima y proporcionada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional». Es decir, la unidad de *arqueros cibernéticos* de las Fuerzas Armadas es el Mando Conjunto de Ciberdefensa.

Pero no todo el monte es orégano. Caveat sobre Tallin 2.0

Habíamos dejado indicado previamente[36] que, en la actualidad, con todas las salvedades que se quieran poner, es una cuestión prácticamente pacífica[37] internacionalmente que las reglas propias del DIH se aplican a las AOC. Habíamos dejado también indicado previamente que el *Manual de Tallin 2.0* probablemente sea el documento doctrinal[38] sobre acciones en el ciberespacio de mayor consenso internacional[39]. Y del mismo modo el general Auditor Domínguez Bascoy sostiene con respecto a la aplicación del DIH en el ámbito del ciberespacio que «la comunidad internacional no ha sido, sin embargo, capaz de alcanzar un consenso sobre la manera precisa en que han de aplicarse a aquellas muchos de los principios y normas internacionales»[40], igualmente debe reconocerse que las reglas contenidas en el *Manual de Tallín 2.0* han sido también objeto de crítica doctrinal y que, en ocasiones, la práctica de las operaciones de los Estados en el ciberespacio no ha sido plenamente conforme con sus reglas[41]. Esta situación ha sido cáusticamente resumida por Efrony y Shany diciendo: «Por lo tanto, aunque las reglas de Tallín han sido criticadas por no avanzar lo suficiente en la limitación de la habilidad para conducir ciberoperaciones en el ciberespacio, estamos viendo a algunos Estados protestando por lo opuesto, esto es, que [esas reglas] se deberían limitar aún más, y otros van incluso más allá»[42]. En realidad, es probable que estas discrepancias entre Estados sobre el *Manual de Tallin 2.0* no sean sino un reflejo de las discrepancias más

---

36 Véase el apartado El problema de la atribución de este capítulo *ut supra*.

37 Nótese sin embargo que dos Estados tan poderosos como Rusia o China no tienen una posición oficial acerca de la aplicabilidad del derecho internacional humanitario al ámbito cibernético. Cfr. DROEGE, Cordula, *op. cit.,* p. 537.

38 Que sea un documento doctrinal no le priva de valor jurídico. Otro documento doctrinal como es el Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar, y que por tanto es conceptualmente parecido a *Tallin 2.0*, es de notoria aplicación diaria en los estados mayores navales cuanto menos como argumento de autoridad o fuente de motivación jurídica.

39 Véase el apartado Ámbito del ciberespacio de este capítulo *ut supra*.

40 Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación, y en el mismo sentido el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo, *op. cit.,* p. 622.

41 Véase EFRONY, Dan, y SHANY, Yuval, *op. cit.,* pp. 3 a 8 y 58 a 59.

42 Ibídem, p. 58.

generales que aquellos tienen sobre la aplicación del derecho internacional a las acciones de los Estados en el ciberespacio, donde las diferencias no son tanto jurídicas como estratégicas, políticas o ideológicas[43].

La consecuencia práctica para el operador legal en la materia es que deberá tener en cuenta que el *Manual de Tallín 2.0*, en definitiva, es un tratado doctrinal y no una norma de fuerza legal. Por consiguiente, el análisis jurídico que se haga de una AOC en el ámbito de los conflictos armados podrá tener en cuenta las reglas de *Tallin 2.0*, pero no exclusivamente.

Acciones ofensivas en el ciberespacio y sus clases

«Ciberoperaciones»

En los ámbitos terrestre, marítimo y aéreoespacial las acciones o las operaciones son perceptibles por los sentidos. Cuando una persona ve a una compañía de Leopards campo a través, o a unos F-18 volando, o una fragata navegando, puede deducir a simple vista que hay una acción o una operación en curso, pero eso no pasa en el dominio cibernético. Por eso, un primer paso para el análisis de una AOC es la determinación primero de qué es el sustantivo antes de la de qué es el adjetivo.

En España el general Auditor Domínguez Bascoy ha definido como «ciberoperación» como «aquella actividad en la que se emplean capacidades cibernéticas en o a través del ciberespacio»[44]. Se trata de una definición similar a la adoptada en 2018 por EE. UU. en su *Publicación Conjunta 3-12* del Presidente de la Junta de Jefes de Estado Mayor, conforme a la cual una ciberoperación es el «empleo de capacidades cibernéticas en las que el propósito primario es alcanzar objetivos en o a través del ciberespacio»[45], que a su vez asume la definición que al respecto había adoptado su Ejército de Tierra[46].

---

[43] La Asamblea General de Naciones Unidas tiene convocado un Grupo de Expertos Gubernamentales dentro del Primer Comité de la misma sobre «Los avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional» y que es probablemente el único foro intergubernamental general sobre la materia. El trabajo de ese grupo encalló en 2017 por las diferencias que los Estados tienen sobre la bondad –o no – del flujo libre de información en Internet y la difusión de los derechos fundamentales. Véase al respecto HENRIKSEN, Anders. «The end of the road for the UN GGE process: The future regulation of cyberespace». *Journal of Cybersecurity*. Volume 5, Issue 1, 2019, accedido en https://academic.oup.com/cybersecurity/article/5/1/tyy009/5298865 el 24 de mayo de 2019.

[44] Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación.

[45] US JOINT CHIEFS OF STAFF. Joint Publication 3-12 «Cyberspace Operations». *Op. cit*., p. I-1.

[46] HEADQUARTERS. Department of the Army. Field Manual *FM 3-38, Cyber Electromagnetic Activities*. *Op. cit.,* pp. 1-3.

En resumen, podemos concluir que el concepto de «ciberoperación» está compuesto por (1) las capacidades del actor, (2) por el medio en el que se ejecutan tales capacidades, y (3) por el objetivo que se busca alcanzar.

Qué son las acciones ofensivas en el ciberespacio

La doctrina estadounidense distingue entre operaciones ciberofensivas (lo que aquí denominamos AOC) y ciberataques[47]. Resumidamente, considera que las operaciones ciberofensivas (AOC) son misiones cuyo objeto es la proyección de poder en y a través del ciberespacio extranjero a través de acciones de apoyo de un mando combatiente o de un objetivo nacional. Tal proyección de poder puede limitarse a afectar las capacidades en el ciberespacio del objetivo o crear efectos en el ciberespacio que desencadenen sucesivos efectos en los dominios reales (terrestre, aéreoespacial o marítimo) y que afecten a sistemas de armas, comunicaciones, nodos logísticos, u objetivos de alto valor.

Esas operaciones ciberofensivas (AOC) se ejecutan, según la doctrina estadounidense, a través de «ataques en el ciberespacio»[48], que son las específicas acciones que crean efectos de negación (degradación, disrupción o destrucción del objetivo) en el ciberespacio o manipulación de datos y que suponen efectos adversos en los dominios reales, y se considera que son equivalentes a un ataque cinético (*fire*).

España, por su parte, ha definido en la Orden Ministerial 10/2013 el concepto de «ciberataque» como la «acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan»[49]. Esta definición, por su menor abstracción que la estadounidense, es probablemente más útil para los operadores en el ámbito de los conflictos armados.

Uso de la fuerza vs ataque armado: necesidad del análisis de impacto del nivel de la acción ofensiva en el ciberespacio

Hemos visto en el apartado anterior que, doctrinalmente, puede distinguirse entre una AOC y un ciberataque o ataque en el ciberespacio. Recordemos, igualmente, que la Carta de las Naciones Unidas prohíbe a los Estados recu-

---

47 US JOINT CHIEFS OF STAFF. *Op. cit.,* pp. II-5 y II-7. HEADQUARTERS, DEPARTMENT OF THE ARMY. *Op. cit.*, pp. 3-2 y 3-3.

48 Véanse las fuentes de la nota a pie de página anterior.

49 Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

rrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, a la vez que reconoce el derecho a la legítima defensa en caso de ataque armado (como hecho distinto del mero «uso de la fuerza»[50]). Esa distinción en las AOC entre (a) acción/operación que alcanza el nivel de uso de la fuerza, y (b) acción/operación que alcanza el nivel de ataque armado, que a su vez desencadena el derecho a la legítima defensa (y que se diferencian entre ellas por el impacto que producen), debe ser cuidadosamente analizada por los operadores. En efecto, mientras que un ataque armado legitima el recurso del agredido a la legítima defensa, el *mero* uso de la fuerza no lo hace, concediendo a la víctima únicamente otro tipo de respuesta *menor* como las contramedidas[51] (acciones u omisiones que un Estado realiza contra otro y que serían ilícitas salvo por la circunstancia de que se adoptan en repuesta al acto ilícito del otro Estado y al objeto de que desista de tal acto ilícito). Consecuentemente, el *Manual de Tallin 2.0* recoge tal criterio en su capítulo 14.

Reglas del *Manual de Tallin 2.0* sobre el uso de la fuerza (capítulo 14):

- Regla 68 – Prohibición del uso de la fuerza. Es ilícita una ciberoperación que constituya una amenaza o uso de la fuerza contra la integridad territorial o independencia política de cualquier Estado, o que de cualquier otra forma sea incompatible con los propósitos de las Naciones Unidas.
- Regla 69 – Definición de uso de la fuerza. Una ciberoperación constituye uso de la fuerza cuando en su escala y efectos son comparables con operaciones no cibernéticas que alcancen el nivel de uso de la fuerza.
- Regla 70 – Definición de amenaza de uso de la fuerza. Una ciberoperación, o la amenaza de una ciberoperación, constituye una amenaza ilícita de uso de la fuerza cuando la acción con la que se amenaza, si se ejecuta, fuera un uso ilícito de la fuerza.
- Regla 71 – Legítima defensa contra ataque armado. Un Estado que sea el objetivo de una ciberoperación que alcanza el nivel de ataque armado puede ejercer su derecho inherente a la legítima defensa. Que una ciberoperación constituya un ataque armado depende de su escala y efectos.
- Regla 72 – Necesidad y proporcionalidad. El uso de la fuerza en el desarrollo de una ciberoperación ejecutada por un Estado en el ejercicio de su derecho a la legítima defensa debe ser necesaria y proporcionada.
- Regla 73 – Inminencia e inmediatez. El derecho al uso de la fuerza en legítima defensa surge si un ataque armado cibernético ocurre o es inminente. Además, se requiere que sea inmediato.

[50] Sentencia Nicaragua de la Corte Internacional de Justicia de 27 de junio de 1986.

[51] Véanse las reglas 20 y siguientes del *Manual de Tallín 2.0.*

A su vez, en los comentarios[52] a la regla 69 (definición de uso de la fuerza), se indica que los factores que los Estados consideran para determinar si una «ciberoperación» alcanza el nivel de uso de la fuerza son, resumidamente y entre otros, los siguientes:

a) Gravedad (*severity*): sujeto a una regla *de minimis*, la causación de daños físicos a personas o cosas cualificará la ciberoperación como uso de la fuerza.

b) Inmediatez (*immediacy*): cuanto antes se manifiesten los efectos de la ciberoperación más probable es que se considere como uso de la fuerza.

c) Causación (*directness*): cuanto más directo sea el nexo causal entre el acto (la ciberoperación) y sus consecuencias, más probable es que se considere como uso de la fuerza.

d) Intrusión (*invasiveness*): cuanto la ciberoperación se haya dirigido a la penetración en sistemas protegidos del objetivo, más probable es que se considere como uso de la fuerza.

e) Cuantificabilidad de efectos (measurabilty of effects): cuanto más cuantificables sean los efectos de una ciberoperación, más probable es que se considere como uso de la fuerza.

f) Carácter militar (*military character*): La vinculación entre una ciberoperación y operaciones militares aumenta la probabilidad de que se considere aquella como uso de la fuerza.

g) Implicación estatal (*State involvement*): cuanto más clara sea la vinculación entre un Estado como actor y una ciberoperación, más probable es que se considere como uso de la fuerza.

h) Presunción de legalidad (*presumptive legality*): en derecho internacional público, lo que no está prohibido por tratados internacionales o la costumbre internacional se considera que está permitido (por ejemplo, el derecho internacional público no prohíbe el espionaje). Será menos probable que las ciberoperaciones que estén cubiertas por una presunción de legalidad se consideren como uso de la fuerza.

Por otra parte, en los comentarios[53] a la regla 71 (legítima defensa contra ataque armado), se indica que no es lo mismo el uso de la fuerza que el ataque armado, en concordancia con la sentencia Nicaragua[54] de la Corte Internacional de Justicia. La diferencia entre uso de la fuerza y el ataque armado es que la escala y efectos de este es superior a aquel, lo que necesariamente implica un análisis caso por caso de cada AOC. Un ejemplo pue-

52 VV. AA. *Tallin Manual 2.0... Op. cit.,* pp. 334 a 337.

53 Ibídem, pp. 339 a 348.

54 Sentencia Nicaragua de la Corte Internacional de Justicia de 27 de junio de 1986.

de ser el del virus Stuxnet, que fue utilizado por una potencia para tomar el control de centrifugadoras usadas para el enriquecimiento de uranio por parte de Irán, de forma que las mismas se autodestruyeran. Los autores del *Manual de Tallin 2.0* han considerado que el ataque Stuxnet ha alcanzado el nivel de uso de la fuerza y, para parte de ellos, que incluso ha llegado al nivel de ataque armado[55].

Parece razonablemente claro que un ciberataque que, al menos, cause daños físicos a personas u objetos puede ser considerado como uso de la fuerza[56]. Se ha considerado a su vez, con razonable criterio, que una AOC alcanza el nivel de ataque armado cuando sus efectos directos e indirectos sean equivalentes a los que se habrían producido por un ataque armado convencional[57]. Sin embargo, lo cierto es que la ausencia de una regla clara acerca de cuándo el uso de la fuerza alcance el nivel de ataque armado hace que las AOC en tiempo de paz entren de lleno en la *zona gris*[58], ámbito que se trata brillantemente en el capítulo «El conflicto en las sombras: aspectos generales y elementos jurídicos de las operaciones en la zona gris» de esta publicación y del que es autor el teniente coronel auditor Mario Lanz Raggio.

Tipos de ciberataques

Una AOC se basa, lógicamente, en una vulnerabilidad detectada en el sistema del objetivo, lo que en términos de los dominios tradicionales se consideraría el punto débil. Cómo se ataca a esa vulnerabilidad puede ser analizada desde distintos ángulos, tal y como ha expuesto H. LIN[59]:

- Acceso. En función del acceso, el ciberataque puede ser por acceso remoto, típicamente a través de Internet, o por acceso cercano, a través de la colocación local de un determinado *hardware* o *software*.
- Capacidad. La capacidad se refiere a las cosas que se pueden hacer aprovechando el acceso ganado al sistema objetivo.
- Efectos. Los efectos que el ciberataque produce en el objetivo, que pueden ser desde el mero acceso a la información contenida en el sistema

55 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 342.

56 SCHMITT, Michael N. *Grey Zones... Op. cit*, p. 14.

57 LIN, Herbert S. «Offensive Cyber Operations and the Use of Force». *Journal of National Security Law & Policy*. Vol. 4-63, 13 agosto 2010, p. 73.

58 SCHMITT, Michael N. *Grey Zones... Op. cit*., p. 15.

59 LIN, Herbert S. «Offensive Cyber Operations and the Use of Force». *Journal of National Security Law & Policy*. Vol. 4-63, 13 agosto 2010, pp. 66 y siguientes. Coincide con las ciberoperaciones ofensivas tipo el T. Col. Vito Smyth, USAF, en su trabajo SMYTH, Vito. «The Best Defense is a Good Offense: Conducting Offensive Cyberoperations and the Law of Armed Conflict». Air War Collage, Air University, p. 9. Disponible en https://apps.dtic.mil/dtic/tr/fulltext/u2/1019221.pdf el 10 de abril de 2019.

objetivo, pasando por su manipulación, sustracción, o falsificación, hasta la destrucción del propio sistema.

De esta forma, los ciberataques tipo pueden consistir en

- La destrucción de datos en un sistema, o la misma destrucción del sistema.
- La suplantación de un miembro del sistema, generando información o mensajes falsos.
- La modificación de datos contenidos en una base de datos.
- La degradación o denegación de servicio de un sistema.

La estructura conceptual de un ciberataque: The Cyber Kill Chain

Difícilmente podrá realizarse una valoración jurídica de una AOC sin comprender sus fases, elementos o componentes. Para ello, vamos a utilizar el modelo Cyber Kill Chain. El término Kill Chain se ha referido tradicionalmente a la composición de los elementos que conforman un ataque militar, generalmente referidos como (i) identificación del objetivo, (ii) asignación de fuerzas para el ataque, (iii) orden de ataque y (iv) destrucción del objetivo. Una descripción más precisa del término es la del acrónimo F2T2EA, que se refiere a: *Find* (encuentra un objetivo), *Fix* (determina su situación exacta), *Track* (sigue los movimientos del objetivo), *Target* (escoge el arma apropiada para el ataque), *Engage* (ataque propiamente dicho sobre el objetivo), y *Assess* (evalúa el efecto del ataque).

Sobre el modelo F2T2EA, la empresa Lookheed Martin[60] *ha patentado* el concepto Cyber Kill Chain, para explicar el orden de las fases en que se articula un ciberataque[61]:

1) Reconocimiento: fase de recopilación de información sobre el objetivo, generalmente proveniente de fuentes abiertas.

   Ejemplo de esta fase es la recopilación de información desde ICANN, la aplicación de WHOIS o, en general, páginas web o publicaciones diversas.

[60] Véase https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, accedido el 15 de abril de 2019.

[61] Véase DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación. Para una visión detallada del asunto véase también el capítulo «Technical Methods, Techniques, Tools and Effects of Cyber Operations» de MAYBAUM, Markus en ZIOLKOWSKI, Katharina (ed.). *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. Tallin: NATO CCD COE Publication, 2013, pp. 103 y ss.

2) Creación del arma: fase de diseño y fabricación del instrumento (*malware*) que se va a emplear para obtener los efectos pretendidos por el ciberataque.

   Ejemplo de esta fase es el diseño o selección del programa o aplicación (*malware*) que se va a preparar y probar de forma individualizada para el ciberataque, lo que a su vez tendrá en cuenta si el objetivo no está protegido, está poco protegido, o está muy protegido.

3) Lanzamiento: fase de envío del *malware* al objetivo, lo que se puede hacer por correo-e, por dispositivos de memoria, por acceso no autorizado a la red, etc.

   Ejemplo de esta fase es el envío de un correo-e que lleve adjunto el programa o aplicación utilizado para el ataque para que sea abierto e instalado por el destinatario del correo-e.

4) Explotación: fase de explotación de una vulnerabilidad en el objetivo para la introducción del *malware* en aquel.

   Ejemplo de esta fase es que el atacante tenga la capacidad de alterar el flujo de control de trabajo del sistema objetivo sin tener las credenciales de este que le autoricen para ello. Es el equivalente medieval a conquistar, al menos, la puerta de una ciudad amurallada.

5) Instalación: fase de instalación del instrumento en el objetivo de forma que aquel se pueda ejecutar en este.

   Ejemplo de esta fase es la instalación de una *puerta trasera* al sistema objetivo de forma que el atacante pueda acceder repetidamente al mismo sin autorización.

6) Mando y control: fase en la que el atacante toma el control remotamente el objetivo.

   Ejemplo de esta fase es la capacidad de la que disfruta el atacante de acceder telemáticamente por una *puerta trasera* al sistema objetivo para realizar las acciones sobre el objetivo o, en su caso, para implantar un instrumento que no necesite control *on-line*, como una *bomba lógica* que se active por el mero transcurso del tiempo o por una acción tomada por el controlador del sistema objetivo.

7) Acciones sobre el objetivo: fase en la que el atacante ejecuta las concretas acciones sobre el objetivo con el propósito de alcanzar los efectos pretendidos.

   Ejemplos de esta fase son (i) cambiar el nombre de archivos, (ii) cambiar las versiones y/o fechas de archivos, (iii) modificar tablas y gráficos en archivos, (iv) eliminación de archivos, (v) inserción de archivos con información falsa, (vi) modificación de privilegios de usuario (para

asignar dichos privilegios al atacante o para quitárselos a alguien del objetivo), (vii) cambio de contraseñas, (viii) desinstalación de *software*.

El análisis jurídico de la AOC tendrá entonces en cuenta las concretas medidas y decisiones que por acción y omisión haya realizado el atacante con respecto a cada una de las fases descritas.

Ciberlimitaciones derivadas de los principios generales del derecho internacional humanitario

Decíamos en el Marco legal del empleo de las Fuerzas Armadas de este capítulo que hoy en día, con todas las salvedades que se quieran poner, es una cuestión prácticamente pacífica internacionalmente que las reglas propias del DIH se aplican a las AOC. Como dice la regla 80 del *Manual de Tallín 2.0*: «Las ciberoperaciones ejecutadas en el contexto de un conflicto armado están sujetas a la ley de los conflictos armados». A su vez, debe tenerse presente que pueden ejecutarse AOC *out of the blue* que, por causar daños físicos a personas y objetos de naturaleza o efectos equivalentes a los que se habrían producido por un ataque armado convencional, puedan ser consideradas como ataque armado en sí mismas[62]. Tal hecho implica, por un lado, que esas AOC estén sujetas *per se* a las reglas del derecho internacional humanitario[63] y que, por otro lado, generen el derecho a la autodefensa bajo la Carta de Naciones Unidas como consecuencia de haberse producido una situación de conflicto armado, nacional o internacional, precisamente como consecuencia del ciberataque. En todo caso, no puede ignorarse que, en ausencia de hostilidades abiertas, la práctica parece mostrar que la calificación jurídica del ciberataque por la víctima vendrá determinada por una multiplicidad de factores añadidos (correlación de fuerzas agresor-agredido, situación nacional o internacional, alianzas internacionales, dependencias económicas, etc.), lo que conduce de nuevo a la zona gris[64].

A continuación, expondremos, sin pretender agotar este campo, que es tan amplio como la realidad misma, las principales limitaciones que, con carácter general, se derivan de los principios generales del derecho internacional humanitario.

El principio de necesidad militar

Una regla básica del DIH es que las operaciones militares se dirigirán únicamente[65] contra objetivos militares (artículo 48 del Protocolo I Adicional a los

62 Vid. Apartado Uso de la fuerza vs ataque armado: necesidad de análisis de impacto del nivel de la acción ofensiva en el ciberespacio de este trabajo.

63 Y desde luego a las reglas del *ius ad bellum*, materia ajena por otra parte al objeto de este trabajo.

64 SCHMITT, Michael N. *Grey Zones... Op. cit.,* p. 15.

65 ESTADO MAYOR DEL EJÉRCITO. «*OR7-004 Orientaciones – El Derecho de los Conflictos Armados*». Tomo I, 1996, pp. 2-3.

Convenios de Ginebra de 1949). La necesidad militar requiere que los objetivos legítimos sean únicamente aquellos que realicen una contribución directa al esfuerzo bélico del enemigo, o que su destrucción o daño produzca una ventaja militar al atacante por su naturaleza, localización, propósito o uso[66].

De ello se deriva que el atacante debe realizar todo lo que razonablemente pueda para verificar que el objetivo sea un objetivo militar y, eligiendo en todo caso los medios que minimicen los daños colaterales, cancelar o suspender el ataque cuando sea aparente que el objetivo no sea objetivo militar o que se incumplirá el «principio de proporcionalidad»[67] (sobre el que tratará el apartado homónimo de este capítulo). Consecuentemente, el *Manual de Tallin 2.0* recoge en su cuerpo el principio de necesidad militar.

Reglas del *Manual de Tallin 2.0* sobre el principio de necesidad militar:

> Regla 114 – Cuidado constante. Durante las hostilidades que impliquen ciberoperaciones, se tendrá un cuidado constante de preservar a la población civil, a civiles individuales, y a objetos civiles.
>
> Regla 115 – Verificación de objetivos. Aquellos que planeen o decidan un ciberataque harán todo lo que sea factible para verificar que los objetivos a ser atacados no sean personas u objetos civiles y no estén sujetos a especial protección.
>
> Regla 116 – Elección de medios o métodos. Aquellos que planeen o decidan un ciberataque tomarán todas las precauciones que sean factibles en la elección de medios o métodos bélicos empleados en el ataque, con la intención de evitar, y en cualquier caso minimizar, los daños incidentales a civiles, la pérdida de vidas civiles, y el daño o destrucción de objetos civiles.

De hecho, puede razonablemente pensarse que la cuestión del principio de la necesidad militar en el ciberespacio y de que, en consecuencia, se tomen todas las medidas adecuadas para limitar los daños incidentales a civiles, puede tener un cierto paralelismo con una de las razones últimas de la prohibición de las armas biológicas, en el sentido de evitar los efectos derivados de la expansión incontrolada del arma, sea esta un virus biológico o informático (*malware*).

El principio de distinción

El principio de distinción está intrínsecamente unido al de necesidad militar en tanto en cuanto se basa también en la diferenciación entre objetivo mi-

[66] SMYTH, VITO. *Op. cit.,* p. 11.

[67] SCHMITT, Michael N., «Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum», Harvard National Security Journal, Vol. 8, 2017, p. 276.

litar y objetivo civil, si bien aquel pretende dar una regla de respuesta más específica a la cuestión de qué objetos civiles, por la ventaja militar que proporcionan al enemigo, son susceptibles de ser atacados. Aquí las reglas de partida, en cuanto a los objetos, son las de

- El artículo 52.3 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «En caso de duda acerca de si un bien que normalmente se dedica a fines civiles, tal como un lugar de culto, una casa u otra vivienda o una escuela, se utiliza para contribuir eficazmente a la acción militar, se presumirá que no se utiliza con tal fin».
- Los apartados 2 y 3 del artículo 54 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «2. Se prohíbe atacar, destruir, sustraer o inutilizar los bienes indispensables para la supervivencia de la población civil, tales como los artículos alimenticios y las zonas agrícolas que los producen, las cosechas, el ganado, las instalaciones y reservas de agua potable y las obras de riego, con la intención deliberada de privar de esos bienes, por su valor como medios para asegurar la subsistencia, a la población civil o a la parte adversa, sea cual fuere el motivo, ya sea para hacer padecer hambre a las personas civiles, para provocar su desplazamiento, o con cualquier otro propósito»; y «3. Las prohibiciones establecidas en el párrafo 2 no se aplicarán a los bienes en él mencionados cuando una Parte adversa: a) utilice tales bienes exclusivamente como medio de subsistencia para los miembros de sus Fuerzas Armadas; o b) los utilice en apoyo directo de una acción militar, a condición, no obstante, de que en ningún caso se tomen contra tales bienes medidas cuyo resultado previsible sea dejar tan desprovista de víveres o agua a la población civil que esta se vea reducida a padecer hambre u obligada a desplazarse» .

El principio de distinción se refiere entonces a la acreditación de que haya un claro nexo entre el objeto en principio civil y las capacidades militares del enemigo para que pueda ser considerado objetivo militar y, en consecuencia, ser atacado.

El principio de distinción es una de las cuestiones más candentes en la actualidad en el ámbito del derecho internacional humanitario. En efecto, se ha reconocido que las AOC podrían ser particularmente útiles para tomar como objetivo determinados objetos civiles, por cuanto permiten a los beligerantes dirigirse contra objetivos que previamente estarían, en una perspectiva *tradicional*, más fuera de su alcance, como el sistema financiero o de sanidad, en tanto en cuanto se considere que contribuyen al esfuerzo bélico del enemigo, de forma que incluso la ciberguerra podría conducir a disponer de una mayor lista de objetivos legítimos comparada con los conflictos armados tradicionales[68]. Se trata de una consecuencia lógica de la regla de que un

[68] DROEGE, Cordula. *Op. cit*., p. 561.

objeto no puede ser civil y militar al mismo tiempo y, en consecuencia, de que redes básicas (de comunicaciones, de transporte, etc.) para la sociedad civil, en tanto en cuanto sean marginalmente usadas por las fuerzas armadas, se convierten en objetivos militares. Se produce, así, un riesgo cierto de guerra total que afecte directamente a la población por cuanto todo sea, en definitiva, objetivo militar. Como dice DROEGE[69]:

> «Las consecuencias humanitarias de esta situación son de la mayor relevancia para la protección de la población civil. En un mundo en que la mayor parte de las infraestructuras civiles, comunicaciones civiles, finanzas, economía y comercio se basan en la infraestructura cibernética internacional, la tentación es demasiado fuerte para los beligerantes para destruir estas infraestructuras. No hay necesidad de demostrar que una red bancaria se usa para acciones militares, o que una red eléctrica tiene uso dual. El dejar fuera de funcionamiento los cables principales, nodos, *routers* o satélites en los que estos sistemas se basan casi siempre será justificable por el hecho de que esos *routers* se usan para transmitir información militar y por tanto cualifican como objetivos militares».

Sin embargo, por otra parte, no podemos desconocer que los ciberataques pueden ser, por sí mismos preferibles a los ataques bélicos tradicionales[70]. Podemos considerar así una situación en la que uno de los beligerantes quiere cortar las vías de suministros por vía marítima del enemigo. Una opción sería bombardear el puerto de origen de los suministros, con el riesgo que ello supone de pérdida de vidas humanas de las personas que vivan cerca del puerto. Otra opción sería un ciberataque que, simplemente, deje inoperativo la infraestructura del puerto; esta opción alcanzaría el mismo objetivo que la bélica tradicional, pero sin riesgo de pérdidas de vidas humanas[71].

Otra consecuencia del principio de distinción, bien señalada por el general auditor Domínguez Bascoy es que las partes beligerantes, por principio, eviten el uso de ciberarmas indiscriminadas por naturaleza, como un *malware* que se replique sin control y cuyos efectos dañinos no se puedan limitar[72].

Reglas del *Manual de Tallin 2.0* sobre el principio de distinción en cuanto a los objetos:

---

69 Ibídem, p. 564.

70 Situación que reconoce el *Manual de derecho de la guerra* del Departamento de Defensa de EE. UU. Vid. Office of General Counsel – Department of Defence. «Department of Defence – Law of War Manual». Department of Defence, June 2015, updated December 2016, p. 1023.

71 Ejemplo considerado por SCHIMITT, Michael N. *Peacetime Cyber Responses... Op. cit*., p 277.

72 Véase el capítulo de DOMINGUEZ, Jerónimo. «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio». *Op. cit.*, p. 641.

Regla 93 – Distinción. El principio de distinción se aplica a los ciberataques.

Regla 99 – Prohibición de ataque de objetos civiles. Los objetos civiles son serán objeto de ciberataques. La ciberinfraestructura[73] puede ser objeto de ataque si cualifica como objetivo militar.

Regla 100 – Objetos civiles y objetivos militares. Los objetos civiles son todos los objetos que no son objetivos militares. Los objetivos militares son aquellos objetos que, por su naturaleza, localización, propósito o uso, realizan una contribución efectiva a la acción militar y cuya destrucción total o parcial, captura o neutralización, en las circunstancias que se den en el momento, ofrecen una ventaja militar relevante. La ciberinfraestructura puede cualificar como objetivo militar.

Regla 101 – Objetos usados para propósitos civiles y militares. La ciberinfraestructura usada para fines civiles y militares es un objetivo militar.

Regla 102 – Duda sobre el estatus de objetos. En caso de duda acerca de si un objeto y su ciberinfraestructura asociada que normalmente se dedica a fines civiles está siendo usada para realizar una contribución efectiva a la acción militar, la determinación de que así está siendo usada solo se puede realizar tras una cuidadosa valoración.

El principio de proporcionalidad

Otra regla básica del DIH es que las operaciones militares tengan por objetivo a combatientes, eximiéndose de los ataques a la población civil, y que sean proporcionadas en el sentido de que, cuando sea inevitable causar daños a población o bienes civiles, los daños que se causen a los mismos no sean excesivos en relación con el resultado global esperado[74]. Aquí las reglas de partida son:

- El art. 51. del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual se prohíben los «ataques indiscriminados» y se considera indiscriminado el ataque «cuando sea de prever que causarán incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, o ambas cosas, que serían excesivos en relación con la ventaja militar concreta y directa prevista»; y

[73] La nota 2 de la regla 99 remite al glosario para la definición de ciberinfraestructura, con la siguiente redacción: «Los dispositivos de comunicaciones, almacenamiento y computación sobre los que sistemas de información se construyen y operan».

[74] ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit., pp. 4-3 y 2-5.

- El art. 57 del Protocolo I Adicional a los Convenios de Ginebra de 1949), según el cual «... quienes preparen o decidan un ataque deberán: [...] ii) tomar todas las medidas factibles en la elección de los medios y métodos de ataque para evitar o, al menos, reducir todo lo posible el número de muertos y de heridos que pudieran causar incidentalmente entre la población civil, así como los daños a los bienes de carácter civil; iii) abstenerse de decidir un ataque cuando sea de prever que causará incidentalmente muertos o heridos en la población civil, daños a bienes de carácter civil, que serían excesivos con la ventaja militar concreta y directa prevista...».

La cuestión de la proporcionalidad es una de las más complicadas en las AOC que tengan como objetivo ciberinfraestructura civil que cualifique como objetivo militar, y para la que probablemente no haya respuestas fáciles o universalmente válidas. En efecto, consideramos un ciberataque tipo *Denial of Service* contra un objetivo militar, ataque que interfiere negativamente con servicios de correo-e civiles. El efecto reflejo negativo sobre el servicio de correo-e civil no se toma en consideración para el análisis de si la ventaja militar obtenida es excesiva con respecto al daño causado. Sin embargo, la pérdida de funcionalidad del servicio de correo-e civil sí es un daño colateral con respecto a la regla de proporcionalidad[75]. Del mismo modo, parece lógico que en la regla de proporcionalidad se tome en cuenta no solo el daño primario, sino también el daño consecuencial[76]. Consideremos así un ciberataque sobre un sistema dual civil-militar de comunicaciones de emergencia, que resulte en que se quede sin servicio: en la medida en que la falta de servicio de comunicaciones de emergencia resulte en que se perjudique la atención a personas heridas, tal perjuicio deberá ser tenido en cuenta a la hora del juicio de proporcionalidad[77]. Por este motivo, parece que el principal factor de *defensa* de las ciberinfraestructuras frente a los ciberataques será precisamente el principio de proporcionalidad[78].

La cuestión, en todo caso, es ciertamente complicada. Un reciente análisis[79] sobre AOC reales concluyó que las que tuvieron lugar con ocasión del conflicto armado de Ucrania (ya fuera en cuanto afectación del sistema eléctrico o de uso del virús NotPetya –virus que encriptaba el contenido de los ordenadores y requería el pago de un rescate en bitcoins para desencriptar–) no habían respetado los principios de distinción y proporcionalidad, destacando

75 SCHIMITT, Michael N. *Peacetime Cyber Responses... Op. cit.,* p. 277.

76 En idéntico sentido DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual *Derecho de las operaciones aéreas*, pendiente de publicación, y en el mismo sentido el capítulo «Aplicación del derecho internacional humanitario a las operaciones en el ciberespacio» de DOMINGUEZ, Jerónimo. *Op. cit.,* p. 643.

77 SCHIMITT, Michael N. *Peacetime Cyber Responses... Op. cit.,* p. 278.

78 DROEGE, Cordula. *Op. cit.,* p. 566.

79 EFRONY, Dan y SHANY, Yuval. *Op. cit.,* p. 57.

señaladamente para ello que no se había limitado el ataque (con el virús NotPetya) a direcciones IP de Ucrania, lo que permitió que el ataque se extendiera a ordenadores de todo el mundo.

Reglas del *Manual de Tallin 2.0* sobre el principio de proporcionalidad:

> Regla 113 – Proporcionalidad. Se prohíbe un ciberataque del que pueda esperarse que cause una pérdida incidental de vida humana, daños a civiles, daños a objetos civiles, o a una combinación de todos estos, que fuera excesiva en relación con la concreta y directa ventaja militar esperada.
>
> Regla 117 – Precauciones con respecto a la proporcionalidad. Aquellos que planean o deciden ataques se abstendrán de decidir el lanzamiento de cualquier ciberataque del que se pueda esperar que cause daño incidental de vidas civiles, lesiones a civiles, daño a objetos civiles, o una combinación de estos, que sea excesivo con respecto a la concreta y directa ventaja militar esperada.

Probablemente la palabra clave de la regla 113 sea «excesiva». El comentario 8[80] de esta regla recuerda que el concepto «excesivo» no está definido en derecho internacional, y que a estos efectos lo relevante no es la cantidad de daño causado a civiles y sus propiedades, sino si el daño que puede esperar es excesivo con respecto a la ventaja militar prevista teniendo en cuenta las circunstancias presentes en el momento, lo que conduce a un análisis caso por caso. Merece la pena destacar igualmente que el comentario 5 de esta regla indica que las inconveniencias, irritación, estrés o daño que pueda causar una ciberoperación no suponen un «daño incidental» para tener en cuenta.

Protección de personas civiles

Otra regla básica del derecho internacional humanitario es que las operaciones militares tengan por objetivo a combatientes, exonerándose de los ataques a la población civil[81]. Aquí las reglas de partida son:

- El art. 48 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «a fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus ataques únicamente contra objetivos militares».

80 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 473.

81 ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit. pp. 1-10 y 3-2.

- El art. 50 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «1. Es persona civil cualquiera que no pertenezca a una de las categorías de personas a que se refieren el artículo 4, A. 1), 2), 3), y 6), del III Convenio, y el artículo 43 del presente Protocolo [resumidamente, miembros de las Fuerzas Armadas, de milicias, de movimientos de resistencia organizada, o población civil que toma las armas]. En caso de duda acerca de la condición de una persona, se la considerará como civil. 2. La población civil comprende a todas las personas civiles. 3. La presencia entre población civil de personas cuya condición no responda a la definición de persona civil no priva a esa población de su calidad de civil».
- El art. 51 del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «1. La población civil y las personas civiles gozarán de protección general contra los peligros procedentes de operaciones militares. Para hacer efectiva esta protección, además de las otras normas aplicables de derecho internacional, se observarán en todas las circunstancias las normas siguientes. 2. No serán objeto de ataque la población civil como tal ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil. 3. Las personas civiles gozarán de la protección que confiere esta Sección, salvo si participan directamente en las hostilidades y mientras dure tal participación...».

Los ciberataques tienen, en cuanto al factor subjetivo del objetivo, dos peculiares características: por un lado, el objetivo habitual no será tanto una persona como un objeto, y por otro lado, que por las especiales características de los operadores en el ámbito informático, no es descartable la intervención de personas ajenas a las fuerzas armadas en acciones militares cibernéticas[82], lo que requiere analizar en qué momento esas personas pierden su protección bajo el derecho internacional humanitario.

Reglas del *Manual de Tallin 2.0* relativas a ataques contra personas:

> Regla 94 – Prohibición de atacar civiles. La población civil, como tal, así como civiles individualmente considerados, no serán objeto de ciberataque.
>
> Regla 95 – Duda sobre el estatus de las personas. En caso de duda acerca de si una persona es civil, esa persona será considerada como civil.

[82] Se trata de hecho de una cuestión expresamente reconocida en el *Law of War Manual* del Departamento de Defensa de EE. UU., que recoge en su apartado 16.5.5 la posibilidad de que «personal civil participe en ciberoperaciones, incluyendo acciones que puedan constituir una participación directa en las hostilidades», con la lógica consecuencia de que «civiles que tomen una participación directa en las hostilidades pierden la protección contra ser objeto de ataque»: Office of General Counsel – Department of Defence, *Law of War Manual*, doc. cit., pp. 1024 y 1025.

> Regla 96 – Personas como objetos que pueden ser legalmente atacadas. Las siguientes personas pueden ser objeto de ciberataques: (a) miembros de las Fuerzas Armadas; (b) miembros de grupos armados organizados; (c) civiles, si y por el tiempo que tomen directamente parte en las hostilidades, y (d) en un conflicto armado internacional, los participantes de un levantamiento en masa.
>
> Regla 97 – Civiles participando directamente en las hostilidades. Los civiles disfrutan de protección contra ataque excepto y mientras participen directamente en las hostilidades.

Se debe tener especialmente en cuenta que, no obstante la aparente claridad de las normas del *Manual de Tallín 2.0*, existen visiones contrapuestas acerca de cuándo un miembro de un grupo armado organizado puede ser objeto de ciberataque. Hay una visión según la cual la participación reiterada en las actividades de ese grupo armado organizado legitima su ataque en cualquier momento, y hay otra visión[83] según la cual ese miembro solo puede ser atacado si desarrolla una «función continua de combate»[84].

Del mismo modo, y con respecto a cuándo se considera que un civil toma participación directa en las hostilidades, los comentarios a la regla 97 del *Manual de Tallín 2.0* remiten a la *Guía para interpretar la noción de participación directa en las Hostilidades según el derecho interncional humanitario* del Comité Internacional de la Cruz Roja[85]. Esta guía toma en consideración tres elementos para responder a esa pregunta:

1) Umbral de daño. El acto del participante debe tener o pretender efectos adversos sobre las capacidades u operaciones militares del enemigo, o causar la muerte, o daños corporales o la destrucción de personas o cosas protegidas. Ese acto puede ser por acción (por ejemplo, una ciberoperación que afecte negativamente a los sistemas de mando y control) o por omisión (por ejemplo, mantener ciberdefensas pasivas sobre activos militares cibernéticos).
2) Causalidad directa. Debe existir un nexo causal directo entre la acción/omisión en cuestión y el daño pretendido o producido.
3) Nexo beligerante. La acción/omisión debe estar directamente relacionada con las hostilidades.

Nótese, finalmente, que a diferencia de lo que ocurre con respecto a los miembros de grupos armados organizados, un civil que tome participación

---

83 Basada en MELZER, Nils. *Guía para interpretar la noción de participación directa en las hostilidades según el derecho internacional humanitario*. Ginebra: Comité Internacional de la Cruz Roja, 2009, p. 35.

84 Véase el comentario 4 en VV. AA. *Tallin Manual... Op. cit*. p. 426.

85 MELZER, Nils, op. cit., pp. 46 y siguientes.

directa en las hostilidades solo puede ser objeto de un ciberataque mientras esté realizando dicha participación directa[86].

Prohibición de la perfidia

Otra regla básica del derecho internacional humanitario es la de la prohibición de la perfidia o *traición*[87]. Aquí la regla de partida es:

- El art. 37. del Protocolo I Adicional a los Convenios de Ginebra de 1949, según el cual «1. Queda prohibido matar, herir o capturar a un adversario valiéndose de medios pérfidos. Constituirán perfidia los actos que, apelando a la buena fe de un adversario con intención de traicionarla, den a entender a éste que tiene derecho a protección, o que está obligado a concederla, de conformidad con las normas de derecho internacional aplicables en los conflictos armados. Son ejemplos de perfidia los actos siguientes:

  a) Simular la intención de negociar bajo bandera de parlamento o de rendición;

  b) Simular una incapacitación por heridas o enfermedad;

  c) Simular el estatuto de persona civil, no combatiente; y

  d) Simular que se posee un estatuto de protección, mediante el uso de signos, emblemas o uniformes de las Naciones Unidas o de Estados neutrales o de otros Estados que no sean Partes en el conflicto.

  2. No están prohibidas las estratagemas. Son estratagemas los actos que tienen por objeto inducir a error a un adversario o hacerle cometer imprudencias, pero que no infringen ninguna norma de derecho internacional aplicable en los conflictos armados, ni son pérfidos ya que no apelan a la buena fe de un adversario con respecto a la protección prevista en ese derecho. Son ejemplos de estratagemas los actos siguientes: el camuflaje, las añagazas, las operaciones simuladas y las informaciones falsas».

Si hay un ámbito de los conflictos modernos en los que se presenten oportunidades para la perfidia y las estratagemas son las AOC. Un claro ejemplo de estratagema podría ser la alteración de la base de datos del enemigo, a resultas del cual se envíen mensajes a su cuartel general de supuestas unidades subordinadas o viceversa. Del mismo modo, según como se implemente una AOC, se podría incurrir en perfidia. Un ejemplo podría basarse en los códigos y señales establecidos por la Unión

[86] Véase el comentario 8 en VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 431.

[87] ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit., p. 3-11.

Internacional de Telecomunicaciones, la Organización Internacional de Aviación Civil y la Organización Marítima Internacional para su uso por unidades y transportes sanitarios para su identificación como tales. Si una AOC afecta a los sistemas de radar o señales de un beligerante de forma que identifique como transportes sanitarios a objetos que no lo son, se trataría aparentemente de un claro caso de perfidia[88]. Por este motivo, parece clara la conveniencia de un cuidadoso análisis jurídico previo a una AOC[89].

Reglas del *Manual de Tallin 2.0* sobre perfidia y estratagemas:

> Regla 122 – Perfidia. En la conducción de hostilidades que impliquen ciberoperaciones, está prohibido matar o lesionar a un adversario a través de la perfidia. Actos que invitan la confianza de un adversario en creer que él o ella tienen derecho a, o están obligados a conceder, protección bajo el derecho de los conflictos armados, con la intención de traicionar esa confianza, constituyen perfidia.
>
> Regla 123 – Estratagemas. Se permiten las ciberoperaciones que cualifiquen como estrategemas.

Interesantemente, el comentario 2 a la regla 123 del *Manual de Tallín 2.0* facilita diversos ejemplos de ciberestratagemas que, en cuanto tales, son legítimas bajo el derecho de los conflictos armados[90]:

1) La creación de sistemas informáticos simulados, que aparenten fuerzas inexistentes.
2) La transmisión de información falsa que cause a un oponente creer equivocadamente que una operación va a empezar o está en marcha.
3) La utilización de falsos identificadores o sistemas informáticos (*honeynets* o *honeypots*).
4) Ciberataques simulados que no violen la prohibición de ciberataques cuyo objetivo primario sea causar el terror entre la población civil.
5) Emisión de órdenes falsas supuestamente emitidas por los mandos enemigos.
6) Actividades de guerra psicológica.
7) Transmisión de información falsa cuyo propósito es que sea interceptada.
8) Uso de códigos, señales y contraseñas enemigas.

---

88 SMYTH, Vito. *Op. cit.,* p. 16.

89 Véase el apartado Cibertargeting & ROE de este capítulo..

90 Véase el comentario 2 en VV. AA. *Tallin Manual 2.0... Op. cit.* p. 495.

Medios y métodos

Abundando en lo establecido en el apartado Marco legal del empleo de las Fuerzas Armadas de este capítulo, es doctrina oficial[91] de las Fuerzas Armadas españolas[92] que «El empleo y actuación de las FAS deben ajustarse a principios de legalidad y legitimidad, establecidos en la Constitución Española, en la legislación nacional vigente y en los acuerdos internacionales suscritos por España, en especial la Carta de las Naciones Unidas». Consecuentemente, debe evitarse la causación de sufrimientos innecesarios y de males superfluos, o el empleo de medios y métodos que causen o se prevea que puedan causar daños extensos, duraderos y graves al medio ambiente natural, o recurrir al hambre como método de guerra contra la prohibición civil[93]. Aquí las reglas de partida están contenidas en la costumbre internacional y en los diversos tratados internacionales que componen el derecho internacional humanitario[94].

Probablemente la principal limitación legal en cuanto a los métodos a usar en las AOC es la prohibición de los ataques indiscriminados establecida en el artículo 51 del Protocolo I Adicional a los Convenios de Ginebra de 1949. La mejor doctrina[95] ha descrito como supuestos de ciberataques indiscriminados, y por tanto prohibidos, (i) lanzar un ciberataque sin intentar siquiera dirigirlo a una particular ciberinfraestructura militar que cualifique como objetivo militar, (ii) utilizar *malware* diseñado para su uso contra una red militar cerrada en una red militar que, sin embargo, esté conectada a una red civil, y (iii) atacar ciberinfraestructura usada para fines civiles y militares cuando fuera posible inutilizar o destruir únicamente la parte militar de esa infraestructura. Otro claro ejemplo de ciberataque indiscriminado sería la utilización de virus informáticos que se autorreplicaran y se expandieran sin control una vez lanzados[96].

---

91 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A) «Doctrina para el empleo de las Fuerzas Armadas»*, doc. cit., p. 44.

92 Y no solo de las Fuerzas Armadas españolas. El *Law of War Manual del Departamento de Defensa de EE. UU.* establece en su apartado 16.2.2 que «Si no se aplica ninguna regla específica, los principios de la ley de la guerra forman la guía general de conducta durante la guerra, incluyendo la conducta durante ciberoperaciones. Por ejemplo, bajo el principio de humanidad, se debe evitar en las ciberoperaciones el sufrimiento, lesión o destrucción innecesaria para alcanzar un propósito militar legítimo». OFFICE OF GENERAL COUNSEL – DEPARTMENT OF DEFENCE, *Law of War Manual*, doc. cit., p. 1014.

93 ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El derecho de los conflictos armados*, doc. cit., pp. 2-4, 2-5, 3-2 y 3-3.

94 Sin ánimo de ser exhaustivo, los artículo 22 y 23 del Reglamento Relativo a las Leyes y Costumbres de la Guerra Terrestre (H.IV.R), arts. 35, 37, 40, 51, 54 y 57 del Protocolo I Adicional a los Convenios de Ginebra de 1949, etc.

95 SCHMITT, Michael N. *Peacetime Cyber Responses… Op. cit.*, p. 275.

96 DROEGE, Cordula. *Op. cit.,* p. 570.

La conclusión, por tanto, y como ya habíamos dejado apuntado anteriormente[97], es que parece clara la conveniencia de un cuidadoso análisis jurídico previo a una AOC. Al respecto, el *Manual de Tallin 2.0* establece diversas reglas sobre medios y métodos.

Reglas del *Manual de Tallin 2.0* sobre medios y métodos:

> Regla 114 – Cuidado constante. Durante las hostilidades que impliquen ciberoperaciones, se tomará un cuidado constante en preservar a la población civil, a las personas civiles y a los bienes civiles.
>
> Regla 115 – Verificación de objetivos. Quienes preparen o decidan un ciberataque harán todo lo que sea factible para verificar que los objetivos a ser atacados no sean ni civiles ni objetos civiles y que no estén sujetos a especial protección.
>
> Regla 116 – Elección de medios y métodos. Quienes preparen o decidan un ciberataque tomarán todas las precauciones factibles en la elección de medios o métodos empleados en tal ataque, con el propósito de evitar, y en cualquier evento reducir, lesiones incidentales a civiles, la pérdida de vidas humanas, y el daño o destrucción a objetos civiles.
>
> Regla 117 – Precauciones con respecto a la proporcionalidad. Quienes preparen o decidan ataques se abstendrán de decidir cualquier ciberataque del que se pueda esperar la pérdida incidental de vidas civiles, lesiones a civiles, daños a objetos civiles, o una combinación de todo ello, que sea excesivo en relación con la concreta y directa ventaja militar prevista.
>
> Regla 118 – Elección de objetivos. Para los Estados que sean Parte del Protocolo Adicional I, cuando se pueda elegir entre varios objetivos militares para obtener una ventaja militar equivalente, se optará por el objetivo cuyo ciberataque se prevea que cause el menor peligro para vidas civiles y objetos civiles.
>
> Regla 119 – Cancelación o suspensión de un ataque. Quienes preparen o decidan un ciberataque cancelarán o suspenderán el ataque si se advierte que a) el objetivo no es militar o está sujeto a protección especial, b) es de prever que el ataque cause, directa o indirectamente, perdida incidental de vidas civiles, lesiones a civiles, daños a objetos civiles, o una combinación de todo ello, que sea excesivo en relación con la concreta y directa ventaja militar prevista.
>
> Regla 120 – Advertencias. Se dará aviso anticipado y eficaz de un ciberataque que pueda afectar a la población civil, salvo que las circunstancias no lo permitan.

[97] Véase el apartado Protección de personas civiles de este capítulo.

> Regla 121 – Precauciones contra los efectos de un ciberataque. Las partes en un conflicto armado tomarán, hasta donde sea factible, las precauciones necesarias para proteger de los peligros resultantes de ciberataques a la población civil, a personas civiles y a objetos civiles que se encuentren bajo su control.

Un ejemplo de la aplicación de la regla 116 es la que ilustra la nota 6 de la misma[98], que consiste en una operación de inserción de *malware* en un sistema militar cerrado a través de un dispositivo de memoria de una persona que trabaje en ese sistema militar cerrado. El ciberatacante debe valorar la posibilidad de que ese dispositivo de memoria también se introduzca en ordenadores conectados a una red civil y que, por tanto, cause daños colaterales. En tal caso, podría ser posible utilizar un *malware* distinto que minimice la posibilidad de daños colaterales.

Nótese, por otra parte, que las obligaciones contenidas en las anteriores reglas se refieren respectivamente tanto a atacantes como a atacados, refiriéndose las reglas 114 a 120 al atacante y la 121 al atacado[99]. Ello supone que los Estados deben adoptar las medidas defensivas oportunas frente a eventuales ciberataques, lo que abarca desde la separación de las ciberredes militares de las civiles hasta segregar los sistemas de las infraestructuras críticas de internet, pasando por tomar medidas por anticipado para asegurar la rápida reparación de los sistemas que caigan como consecuencia de ciberataques, etc.[100].

Aspectos singulares del cibertargeting

Cibertargeting & ROE

El *targeting* es el proceso por el que se eligen determinados blancos sobre las que se aplican ciertas reglas de enfrentamiento[101] (ROE) habida cuenta de la trascendencia de aquellos[102]. En España este proceso en la actualidad

98 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 480.

99 Véase el comentario 3 de la regla 121 en VV. AA. *Tallin Manual 2.0... Op. cit*., p. 488.

100 Una exhaustiva visión de la resilencia frente a las ciberamenazas se puede encontrar en el capítulo 3 de esta publicación, a cargo de la Dra. De Tomas Morales, al que nos remitimos íntegramente.

101 Las reglas de enfrentamiento se pueden definir como «normas de carácter operativo ajustadas a derecho que proporcionan a los comandantes de todos los escalones de mando y a los miembros de las unidades, guía y respaldo para el empleo de la fuerza determinando las circunstancias, condiciones, grado y forma en las que se puede, o no, aplicar»: Estado Mayor de la Defensa, *Publicación Doctrinal Conjunta PDC-01(A) «Doctrina para el empleo de las Fuerzas Armadas»*, doc cit., p. 96.

102 ALIA, Miguel, en el capítulo «El targeting» en PÉREZ DE FRANCISCO, Eugenio (coord.). *Manual de Derecho Operativo*. Madrid: Marcial Pons Ediciones Jurídicas y Sociales S. A., 2015, p. 291.

se halla ciertamente juridificado[103], y por eso se sostiene en la mejor doctrina que la función del asesor jurídico «en esta actividad es muy importante, porque debe velar por el cumplimiento de la legalidad sobre ataques. Ello implica la aplicación práctica del derecho de los conflictos armados y el dominio de las normas procedimentales sobre el *targeting*»[104].

La doctrina estadounidense[105] considera que hay tres aspectos singulares en el *targeting* aplicado a las AOC: en primer lugar, que las cibercapacidades propias pueden ser una opción viable para atacar determinados objetivos; en segundo lugar, que una AOC puede ser la opción preferible en algunos casos habida cuenta de que puede ofrecer una baja probabilidad de detección y/o no causar daños físicos; y en tercer lugar, que los efectos que produzca la AOC pueden superar –de forma intencionada o no– los previstos, con lo que ello implica de potencial respuesta por la parte atacada. Recordemos, en este sentido, que decíamos que el ciberespacio está formado por cuatro capas interdependientes: (i) la capa física o de *hardware*, (ii) la capa lógica o de *software*, (iii) la capa de contenidos, consistente en la información captada, almacenada o procesada, y (iv) la capa personal, consistente en las personas físicas o jurídicas que actúan en el ciberespacio, y que es en esas capas o contra esas capas contra las que se pueden realizar operaciones en el ciberespacio[106]. Pues bien, precisamente esa correlación es lo que hace que se necesite una potente capacidad de mando y control para, en el ámbito del *targeting*, identificar, correlacionar, coordinar y resolver los conflictos que se planteen entre las cuatro capas del ciberespacio como consecuencia de la AOC[107]. Y precisamente por la complejidad de la ejecución de las operaciones, puede considerarse[108] igualmente que las ROE sean el producto de la consideración conjunta del marco jurídico de las operaciones, de las instrucciones políticas dadas para su desarrollo, y de las consideraciones operativas[109].

Una vez que hemos visto en el capítulo anterior las ciberlimitaciones que se derivan de los principios generales del derecho internacional humanitario,

---

103 Los parámetros legales del *targeting* se van a referir a la misión, al blanco, a las fuerzas propias, a los resultados y al armamento, incluyendo daños colaterales, lo que requiere una potente visión de conjunto. Vid. ALIA, Miguel. *Op. cit.,* pp. 296 y 297.

104 ALIA, Miguel. *Op. cit.,* p. 295.

105 Vid. US JOINT CHIEFS OF STAFF, doc. cit., p. IV-8, y HEADQUARTERS. Department of the Army, doc. cit., p. 3-12.

106 CORN, Gary P. *Op. cit.,* p. 9. Véase también DOMÍNGUEZ, Jerónimo, en el capítulo 8 del manual «Derecho de las Operaciones Aéreas», pendiente de publicación.

107 Vid. JOINT CHIEFS OF STAFF, doc. cit., p. IV-9.

108 ALIA, Miguel. *Op. cit.*, p. 249.

109 Para una visión de los problemas que surgen para el establecimiento de ciberROE por las diferencias entre los ámbitos físicos tradicionales y el cibernético véase KEHLER, C. Robert; LIN, Herbert and SULMEYER, Michael. «Rules of engagement for cyberspace operations: a view from the USA». *Journal of Cybersecurity*, 3(1), 2017, pp. 69-80.

a continuación, trataremos determinados aspectos singulares del *cibertargeting* referidos a los objetivos de las AOC, dando aquí por reproducidas las reglas 114 y siguientes del *Manual de Tallín 2.0* que hemos citado en el apartado Medios y métodos de este capítulo.

Objetos civiles como objetivo

Recordemos que solo pueden ser atacados los objetos que sean militares o que, no siéndolo, por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida[110]. Ya hemos tratado previamente esta cuestión en el apartado relativo al principio de distinción, pero ahora merece la pena profundizar en la cuestión de la contribución eficaz a la acción militar como circunstancia legitimadora de un ciberataque.

Esa contribución eficaz a la acción militar puede ser directa, como sería el caso de una fábrica civil de armas, como caso prototípico de objetivo militar legítimo[111], o indirecta, en cuyo caso se entra de lleno en una zona de incertidumbre en lo relativo a si tal contribución indirecta convierte al objeto en objetivo militar legítimo. Un ejemplo de contribución eficaz indirecta sería el de los sistemas informáticos de una determinada industria de un Estado que a su vez depende de los ingresos o impuestos derivados de esa industria para mantener su capacidad bélica. Pensemos, por ejemplo, en un hipotético Estado centroeuropeo cuya principal industria en términos de generación de ingresos, impuestos y PIB sea su sector bancario y financiero. La inutilización o destrucción de los sistemas informáticos de su sistema bancario y financiero a través de un ciberataque deberían producir un impacto adverso relevante en la capacidad bélica de dicho Estado. No parece haber ahora mismo consenso acerca de si la contribución eficaz indirecta convierte al objeto en objetivo legítimo o no. Por un lado, los EE. UU. parecen considerar oficialmente que sí[112], mientras que en el ámbito del Comité Internacional de la Cruz Roja parece sostenerse la opinión contraria. La directora de la Unidad de Derecho Operativo tiene escrito que «El daño a la economía civil del enemigo, y a las capacidades de investigación y desarrollo en cuanto tales, nunca está permitido bajo el derecho internacional humanitario, con independencia de la ventaja militar prevista, y con independencia de la duración del conflicto. En otro caso, no habría límites a la actividad bélica pues virtualmente toda la economía de un país se puede considerar que contribuya a

110 Cfr. art. 52.2 del Protocolo I Adicional a los Convenios de Ginebra de 1949.

111 SCHMITT, Michael N. *Peacetime Cyber Responses… Op. cit.,* p. 269.

112 Vid. OFFICE OF GENERAL COUNSEL – DEPARTMENT OF DEFENCE. *Law of War Manual*, doc cit., p. 219.

la acción bélica»[113]. La mayoría de los expertos que redactaron el *Manual de Tallin 2.0* parecen alinearse con esta segunda visión por cuanto consideran que la contribución indirecta no convierte al objeto en objetivo legítimo por tener una vinculación excesivamente remota con el esfuerzo bélico[114]. Como puede verse, el color gris es de generosa aplicación en los ciberataques, y probablemente la opinión de cada pintor dependa precisamente de sus niveles de cibercapacidad, ya sean ofensivos o defensivos.

Colaboradores civiles como objetivo. Personal de empresas que participen en cooperación público-privada (public-private partnership)

Ya hemos hablado en el apartado Protección de personas civiles sobre el régimen de protección de los civiles bajo el derecho internacional humanitario frente a ciberataques. Hay también una singular zona de incertidumbre en esta cuestión derivada de las especiales características del ciberespacio, que hacen que sea no solo posible, sino incluso probable, que personal civil tome parte en acciones en el ciberespacio, ya sea como parte de la administración civil de un Estado[115] (piénsese por ejemplo en el personal de la National Security Agency de EE. UU. o del Centro Criptológico Nacional de España), ya sea como empleados de empresas privadas ligadas contractualmente con un Estado para la prestación de servicios (piénsese por ejemplo en personal de ISDEFE o de Indra en España).

La solución a esta cuestión en el *Law of War Manual* del Departamento de Defensa de EE. UU. es reconocer la posibilidad de que personal civil autorizado (y que por tanto está legitimado para tener la condición de prisionero de guerra) participe en ciberoperaciones, incluyendo acciones que puedan constituir una participación directa en las hostilidades, con la lógica consecuencia de que «civiles que tomen una participación directa en las hostilidades pierden la protección contra ser objeto de ataque»[116].

En el *Manual de Tallín 2.0* los expertos, al analizar la regla 96 (personas como objetos que pueden ser legalmente atacadas) distinguen tres casos relativos a personal civil que forme parte de ciberoperaciones[117]:

a) Contratista individual (trabajador autónomo en España) de un Estado. Solo puede ser atacado mientras participe directamente en las hostilidades.

---

113 DROEGE, Cordula. *Op. cit.,* p. 568.

114 VV. AA. *Tallin Manual 2.0...,* p. 441.

115 LIBICKI, Martin C. *Cyberdeterrence and Cyberwar*. Rand Corporation, 2009, p. 155.

116 Vid. OFFICE OF GENERAL COUNSEL – DEPARTMENT OF DEFENCE. *Law of War Manual,* doc. cit., pp. 1024 y 1025.

117 VV. AA. *Tallin Manual 2.0...*, p. 427.

b) Empleado de empresa contratada por un Estado. Puede ser atacado en cualquier momento por considerarse que forma parte de un grupo armado organizado o por analogía con tal consideración.

c) Funcionarios o empleados civiles. Puede ser atacado en cualquier momento si se considerase que forman parte de un grupo armado organizado, lo que parecería deducirse del tipo de organización en el que estuvieran encuadrados (típicamente, seguridad o inteligencia; por ejemplo, en España, el CNI). En caso contrario, solo pueden ser atacados mientras participen directamente en las hostilidades.

Ciertamente, en el caso estrictamente español, no parece tener mucho sentido hacer de peor condición a un empleado por cuenta ajena que a un empleado por cuenta propia, por lo que probablemente esta sea una cuestión incierta tanto a nivel nacional como internacional.

El dato en sí mismo como objetivo.

¿Es el dato, en sí mismo, un objeto, y por tanto, es *sujeto* de la regulación del derecho internacional humanitario? Esta pregunta no es baladí; pensemos en una AOC que elimine de forma irrecuperable el contenido de una base de datos cuyo contenido sea muy relevante para un Estado, como por ejemplo la base de datos de las autoridades tributarias. Si los datos no son un «objeto», entonces esa AOC no cualificará siquiera como ataque.

La respuesta a la pregunta no es unívoca, y probablemente dependa de la tradición jurídica de cada Estado. La mayoría de los expertos que redactaron el *Manual de Tallin 2.0* han sostenido que los datos como tales no son un «objeto» dado que, en su opinión, un «dato» es intangible y no se corresponde con el significado ordinario de la palabra «objeto», y además tampoco se corresponde con la explicación dada al término por los *Comentarios a los Protocolos Adicionales* hecho por el Comité Internacional de la Cruz Roja en 1987. A su vez, la minoría de los expertos ha mantenido la opinión contraria argumentando que, en caso contrario, serían *legales* ataques altamente disruptivos sobre población civil, como sería en el caso de la eliminación de las bases de datos de pensionistas[118]. Michael N. Schmitt, probablemente el principal tratadista estadounidense sobre la materia, reconoce que ambas opiniones tienen al menos parte de razón, pero parece inclinarse conceptualmente a favor de la posición de la minoría, y propone que se reconozca en el futuro que ciertas funciones civiles esenciales que se basen en el tratamiento de datos merezcan una especial protección bajo el derecho internacional humanitario[119].

118 VV. AA. *Tallin Manual 2.0*..., p. 437.

119 SCHMITT, Michael N. *Peacetime Cyber Responses*... *Op. cit.,* p. 270.

Desde el punto de vista español, la cuestión de si un dato es un «objeto» probablemente pueda ser respondida afirmativamente. Pensemos en primer lugar que el diccionario de la Real Academia Española define como «objeto», en su primera acepción: «Todo lo que pueda ser materia de conocimiento o sensibilidad de parte del sujeto, incluso este mismo», y solo en su sexta acepción, «cosa»[120]. Además, España tiene una regla especial de interpretación de las normas en su Código Civil, cuyo artículo 3 dispone que «Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquéllas». Dado que los Convenios de Ginebra son del año 1949, y que el Protocolo Adicional I a los mismos es del año 1977, años en los que la informática y cibernética no estaban tan desarrolladas como ahora mismo, y que su espíritu y finalidad son la protección de civiles y combatientes según su estatus, parece razonable interpretar que se pueda reconocer a los datos como «objetos» habida cuenta de la realidad social actual y del espíritu y finalidad de las normas del derecho internacional humanitario. En este mismo sentido, el Código Penal tipifica en el artículo 264 del Código Penal el borrado, alteración, supresión de «datos informáticos», artículo que está dentro del capítulo IV («De los daños») del título XIII («Delitos contra el patrimonio y contra el orden socioeconómico») del libro II («Delitos y sus penas»), lo que parece hacer equivalente los datos a objetos materiales.

En todo caso, lo cierto es que no se puede considerar la cuestión del dato como objeto, o no, desde una perspectiva exclusivamente nacional. Por eso, corresponderá a los Estados determinar convencional o consuetudinariamente si los datos son objetos a los efectos de *targeting* en el contexto de un conflicto armado[121].

Productos sanitarios y objetivos militares

Parece claro que una operación consistente en manipular medicamentos para que estos en vez de curar tengan efectos letales sería obviamente ilegal[122] pero ¿qué ocurre si en lugar de la manipulación de medicamentos lo que se hace es manipular telemáticamente productos sanitarios, para matar o lesionar a combatientes (por ejemplo, un comandante que tenga un marcapasos)? Para analizar la cuestión debemos tener en cuenta en primer lugar la diferencia que hay entre «productos sanitarios» y «medicinas».

---

120 *Diccionario de la Real Academia Española de la Lengua*. www.dle.rae.es, accedido el 26 de abril de 2019.

121 McCORMACK, Tim. «International Humanitarian Law and the Targeting of Data». *International Law Studies*. Volume 94. Stockton Center for the Study of International Law, US Naval War College, 2018, p. 239.

122 Cfr. Artículo 23 del Reglamento relativo a las Leyes y Costumbre de las Guerra Terrestre; artículo 8.2.b) del Estatuto de Roma de la Corte Penal Internacional.

Las medicinas son sustancias medicinales con propiedades preventivas, de diagnosis, tratamiento, paliativas o de curación de enfermedades. Un marcapasos no puede incluirse en esta categoría ya que no es una sustancia medicinal. Esto se fundamenta por la Ley 29/2006, de 26 de julio, de Uso Racional de Medicamentos y Productos Sanitarios. Esta Ley claramente distingue entre medicamentos y productos sanitarios en su artículo 8. Considera medicamento de uso humano a «toda sustancia o combinación de sustancias que se presente como poseedora de propiedades para el tratamiento o prevención de enfermedades en seres humanos o que pueda usarse en seres humanos o administrarse a seres humanos con el fin de restaurar, corregir o modificar las funciones fisiológicas ejerciendo una acción farmacológica, inmunológica o metabólica, o de establecer un diagnóstico médico», y considera producto sanitario a «cualquier instrumento, dispositivo, equipo, programa informático, material u otro artículo, utilizado solo o en combinación, incluidos los programas informáticos destinados por su fabricante a finalidades específicas de diagnóstico y/o terapia y que intervengan en su buen funcionamiento, destinado por el fabricante a ser utilizado en seres humanos con fines de 1.º diagnóstico, prevención, control, tratamiento o alivio de una enfermedad, 2.º diagnóstico, control, tratamiento, alivio o compensación de una lesión o de una deficiencia, 3.º investigación, sustitución o modificación de la anatomía o de un proceso fisiológico, 4.º regulación de la concepción, y que no ejerza la acción principal que se desee obtener en el interior o en la superficie del cuerpo humano por medios farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales medios». Esta distinción entre medicamento y producto sanitario también se recoge en el Real Decreto 1591/2009, de 16 de octubre, que regula los productos sanitarios y, específicamente, por el Real Decreto 1616/2009, de 26 de octubre, por el que se regulan los productos sanitarios activos, que trasponen los reglamentos comunitarios en la materia. Habida cuenta entonces de la distinción legal entre medicamentos y productos sanitarios, no está clara que la protección a los medicamentos sea extensible a los productos sanitarios.

El comentario 3 de la regla 132 del *Manual de Tallin 2.0*[123] señala que «los datos personales médicos requeridos para el tratamiento de pacientes están igualmente protegidos contra su modificación, borrado, o cualquier otra acción por medios cibernéticos que afectase negativamente a su cuidado, con independencia de que esa acción constituya un ciberataque». Parecería, entonces, que la manipulación de los datos de los productos sanitarios se encuentra prohibida, con independencia de que pueda ser discutible considerar que un marcapasos implantado en un paciente (el comandante, en nuestro ejemplo) sea «parte integral» de una «unidad médica». A su vez, curiosa-

[123] La regla 132 establece que los ordenadores, redes informáticas y datos que formen parte integral de las operaciones o gestión de unidades y transportes médicos deben ser respetados y protegidos, y en particular no pueden ser objeto de ataque. Vid. VV. AA. *Tallin Manual 2.0*..., p. 515.

mente, el comentario 9 de la regla 122[124] del *Manual de Tallin 2.0*, relativo a la perfidia, indica que mientras una parte (mayoritaria) de los expertos consideran que el uso de un *malware* utilizado para alterar el marcapasos del comandante sería un acto de perfidia, dado que ese *malware* se habría hecho pasar como generado por una fuente médica legítima para ser aceptado por el marcapasos, otra parte de los expertos han considerado que tal acción no sería un acto de perfidia dado que el *abuso de la confianza* propio de la perfidia presupone que la confianza la otorga una persona y no una máquina[125].

En nuestra opinión, el *Manual de Tallin 2.0* no *regula* adecuadamente el impacto del uso de productos sanitarios desde la perspectiva del derecho internacional humanitario. Habida cuenta de la diferencia legal existente entre medicamentos y productos sanitarios, habría sido deseable su equiparación en *Tallin 2.0* a los efectos del derecho internacional humanitario por los fines últimos de este, pues tanto los medicamentos como los productos sanitarios tienen como objetivo último el cuidado de la persona frente a enfermedades. De nuevo, será deseable que los Estados determinen convencional o consuetudinariamente el tratamiento de los productos sanitarios en el ámbito de las AOC.

El mando y su responsabilidad

El mando es «la autoridad conferida formal y legalmente a una persona en función del puesto y de la responsabilidad que le corresponde, y se materializa en la capacidad para tomar decisiones e impartir órdenes, instrucciones y directrices. Mando, autoridad, jefe o comandante son denominaciones comúnmente empleadas para identificar a esta persona»[126]. Específicamente, y en el ámbito de este trabajo, se sostiene por el US Cyber Comand que el propósito de tal Mando es «alcanzar la superioridad en el ciberespacio a través de la captura y mantenimiento de la iniciativa táctica y operaciones en el ciberespacio, culminando en una ventaja estratégica sobre los adversarios»[127].

Pero con el mando viene la responsabilidad. Conforme al derecho internacional humanitario, el mando debe conocer las leyes y usos de la guerra, tiene el deber de instruir a sus subordinados, y tiene el deber de prevenir y reprimir las infracciones que comentan por acción u omisión sus subordi-

124 Véase el apartado Prohibición de la perfidia de este capítulo.

125 VV. AA. *Tallin Manual 2.0... Op. cit.,* p. 493.

126 ESTADO MAYOR DE LA DEFENSA. *Publicación Doctrinal Conjunta PDC-01(A) «Doctrina para el empleo de las Fuerzas Armadas»,* doc. cit., p. 157.

127 US CYBER COMMAND. «Achieve and Maintain Cyberspace Superiority». *US Cyber Command.* 2018, p. 7. Accesible en https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010.

nados[128], y el incumplimiento de estos deberes se sanciona en España en el Código Penal con severas penas (artículos 608 y siguientes). Y este deber no puede ni debe darse por supuesto puesto que un combatiente adquiere el estatus de combatiente legítimo cuando, entre otras circunstancias, opera bajo un mando responsable (artículo 43 del Protocolo I Adicional a los Convenios de Ginebra de 1949).

Lógicamente, el *Manual de Tallin 2.0* también recoge la cuestión de la responsabilidad del mando en ciberoperaciones. Su regla 85 (responsabilidad penal de los mandos y superiores) dispone que los mandos son penalmente responsables por ordenar ciberoperaciones que constituyan crímenes de guerra, y que son igualmente responsables si sabían o, teniendo en cuenta las circunstancias del momento, deberían haber sabido, que sus subordinados estaban cometiendo, iban a cometer, o habían cometido, crímenes de guerra y dejaron de tomar todas las medidas razonables y disponibles para prevenir su perpetración o para castigar a los responables[129]. Y es que, obviamente, no hay motivo lógico o legal alguno para excluir de la regulación de los crímenes de guerra a las AOC.

Y en este sentido, enlazando con lo que previamente hemos dicho en el apartado Cibertargeting & ROE de este capítulo sobre la importancia del asesor jurídico, es doctrina formal estadounidense con respecto a la responsabilidad del mando en ciberoperaciones considerar que «es esencial que los mandos, planificadores y operadores consulten con los asesores legales durante la planificación y ejecución de ciberoperaciones»[130], y concordantemente se ha establecido específicamente la necesidad de la incorporación del asesor legal para asesorar al mando en el ámbito de las operaciones ciberelectromagnéticas al objeto de garantizar que las mismas cumplan con las leyes[131].

Esa responsabilidad del mando, y la necesidad de su asesoramiento integral, se potencian aún más por la propia naturaleza del ámbito ciberespacial, que requiere de una capacidad de respuesta inmediata[132]. No es sorprendente, por tanto, que la administración Trump haya dictado a finales de 2018 un National Security Presidental Memoranda – NSPM 13 conforme al cual se delegan al Mando de Ciberdefensa determinadas facultades de decisión antes reservadas al Presidente[133].

---

128 ESTADO MAYOR DEL EJÉRCITO. *OR7-004 Orientaciones – El Derecho de los Conflictos Armados*, doc. cit., pp. 2-1 y 2-2.

129 VV. AA. *Tallin Manual 2.0...,* pp. 396 y siguientes.

130 US JOINT CHIEFS OF STAFF, doc. cit., p. III-11.

131 HEADQUARTERS. Department of the Army, doc. cit., pp. 2-7 y 2-8.

132 Recuérdese a efectos comparativos la autoridad *renegade* española prevista en el artículo 16.d de la Ley Orgánica 5/2005 de la Defensa Nacional.

133 FREEDBERG, Sydney Jr. «Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff», 17 de septiembre de 2018, disponible en https://breakingdefense.com/tag/nspm-13/,

En resumen, y por las circunstancias que hemos citado, por un lado y de *lege ferenda*, sería aconsejable la creación formal de una autoridad *renegade de nivel bajo* para el ámbito de la ciberdefensa española, y por otro lado y de *lege data*, como se da en el caso del Mando Conjunto de Ciberdefensa, un mando inteligente, en un ámbito tan complejo y dinámico como el del ciberespacio, y en el que las repercusiones de las ciberoperaciones pueden ser mucho más amplias de lo inicialmente pretendido, no puede tener lejos de si a su asesor legal.

Conclusiones

Las AOC están aquí y han venido para quedarse. Y no hay diferencia jurídica entre una operación ofensiva *on line* u *off line* en el ámbito de los conflictos armados. Ambas están sujetas al derecho internacional humanitario, adaptándose simplemente las reglas de este al ámbito ciberespacial.

En realidad, las consideraciones jurídicas aplicables a las AOC que se han recogido en este trabajo no son sino extrapolaciones lógicas (nunca mejor dicho) al ámbito ciberespacial de las reglas generales contenidas en el derecho internacional humanitario. De esta forma, del mismo modo que se publicó el *Manual de San Remo sobre el derecho internacional aplicable a los conflictos armados en el mar*, adaptando dicho derecho a la guerra naval, o del mismo modo que se publicó el *Manual de Harvard sobre el derecho internacional aplicable a la guerra aérea y de misiles*, adaptando el referido derecho a la guerra aérea, ahora se ha publicado el *Manual de Tallín 2.0 sobre el derecho internacional aplicable a las ciberoperaciones*, para adaptar el reiterado derecho al ámbito ciberespacial. No hay nada nuevo bajo el sol, en definitiva.

Por eso, en realidad no hay diferencia real entre las reglas bélicas que se aplican a una sección española de arqueros en el bosque con respecto a las que se aplican a los operadores del Mando de Ciberdefensa ante sus pantallas y teclados. Cambian los instrumentos de combate, pero no la *lex artis*, ni tampoco las normas aplicables, y jamás su inquebrantable voluntad de vencer.

accedido el 27 de febrero de 2019. Vid. también CHESNEY, Robert. «CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed Over the Past Year», 9 de mayo de 2019, disponible en https://www.lawfareblog.com/cybercoms-out-network-operations-what-has-and-has-not-changed-over-past-year, accedido el 9 de mayo de 2019.