LA POSSIBILITAT DE LEGÍTIMA DEFENSA CONTRA ATACS CIBERNÈTICS ESTATALS I NO ESTATALS

TREBALL FINAL DE GRAU

Pol Peracaula Domínguez

Tutora: Dra. Mirentxu Jordana Santiago

Universitat de Girona · Facultat de Dret · Grau en Dret · Curs Acadèmic 2022-2023

Convocatòria Maig/Juny

Many though that the horrors of the Second World War—the camps, the cruelty, the exterminations, the Holocaust—could never happen again. And yet they have in Cambodia, in Bosnia and Herzegovina, in Rwanda. Our time has shown us that man's capacity for evil knows no limits.

Kofi A. Annan

ÍNDEX

LLISTAT D'ABREVIATURES

AGNU ..... Assemblea General de les Nacions Unides
CDI ..... Comissió de Dret Internacional
CNA ..... *Computer Network Attack*
CSNU ..... Consell de Seguretat de les Nacions Unides
DIP ..... Dret Internacional Públic
DoD ..... *Department of Defense*
ICJ ..... *International Court of Justice*
IDI ..... Institut de Dret Internacional
ILA ..... *International Law Association*
NCI ..... *National Critical Infrastructure*
OTAN ..... Organització del Tractat de l'Atlàntic Nord
OUP ..... *Oxford University Press*
TIJ ..... Tribunal Internacional de Justícia
US ..... *United States of America*

INTRODUCCIÓ

Sens dubte, els avenços tecnològics estan marcant el desenvolupament de la nostra societat i la nostra dependència sobre ells creix exponencialment. A conseqüència d'aquest fet, nombroses normes, tant internes com internacionals, s'estan quedant obsoletes i incapaces de donar resposta a les noves qüestions relatives al ciberespai. En aquest senti, avui dia el Dret Internacional s'enfronta a problemes que haguessin sigut inimaginables en el moment en què es van adoptar per primera vegada les seves normes, en especial, la prohibició de l'amenaça i l'ús de la força, així com, l'excepció de legítima defensa. No obstant això, la comunitat internacional no ha estat aliena als nous reptes sorgits envers la tecnologia, ni en concret, a la cibertecnologia.

Aleshores, l'objectiu principal és esbrinar si les activitats cibernètiques portades a terme per actors Estatals i no estatals poden vulnerar el principi de prohibició de l'ús de la força, i en particular, si poden constituir un atac armat i donar lloc a la legítima defensa per part de l'Estat víctima d'acord amb l'article 51 de la Carta de les Nacions Unides. Es tracta d'un treball de Dret Internacional Públic, de manera que aquest estudi no s'ocupa del dret intern, del dret internacional privat o del dret penal internacional. Així mateix, tampoc tractarem, tot i ser qüestions que es planteja el Dret Internacional Públic, les activitats cibernètiques relacionades amb la ciberguerra, la ciberresponsabilitat, el dret internacional de les telecomunicacions, els drets humans, el dret diplomàtic, el dret del mar, etc.

Tanmateix, el problema principal que es presenta és que no existeix una regulació específica pel cas de les activitats cibernètiques, degut a la seva ràpida aparició i desenvolupament i, principalment, per la manca de consens entre els Estats. Per tant, és essencial determinar en quina mesura es poden adoptar els principis i les normes existents del Dret Internacional per fer front a les noves amenaces cibernètiques.

En el Capítol 1, per tal d'arribar a l'objectiu últim d'aquest treball: descobrir si els Estats estan legitimats a utilitzar el seu dret a legítima defensa davant d'activitats cibernètiques; és indispensable veure, en primer lloc, si aquestes poden vulnerar el principi de prohibició de l'ús de la força. No serà necessari, en canvi, l'anàlisi de la prohibició de l'amenaça. En aquest sentit, és necessari explicar encara que sigui sistemàticament l'origen de la prohibició. Seguit de l'anàlisi del seu àmbit i significat, és a dir, on es troba regulada, a qui es dirigeix la prohibició i com s'interpreta. Aquest capítol és fonamental per saber quines operacions estan prohibides per la comunitat internacional i si les cibernètiques podrien formar part d'aquest grup o no.

En segon lloc, en el Capítol 1, s'analitzarà l'excepció per excel·lència de la prohibició de l'ús de la força: la legítima defensa. Per això, analitzarem on es troba regulada, les seves característiques

i consideracions generals a tenir en compte. Així com, els requisits que s'exigeixen per poder tenir dret a ella.

Al Capítol 2, s'aplicarà l'analitzat en els anteriors al camp de les activitats i operacions cibernètiques. En primer lloc, per tal de contextualitzar, serà necessari explicar mínimament que és el ciberespai, les activitats en aquest que ens interessen pel nostre estudi i la terminologia que s'usarà. A partir d'aquí, analitzarem, per tant, quines operacions cibernètiques poden constituir un ús de la força, quines un atac armat i com s'haurien de portar a terme els requisits de la legítima defensa davant d'atacs cibernètics. Així com, si seria possible una legítima defensa anticipada o preventiva donat la importància que tindria aquestes possibilitats pels Estats; doncs, tant el llançament com els efectes d'un atac cibernètic poden produir-se en un tancar i obrir d'ulls sense donar l'oportunitat a l'Estat per repel·lir-lo. També, serà molt important en aquest apartat analitzar si els actors no estatals poden portar a terme atacs armats, donada la capacitat cibernètica que s'està veient que tenen aquests grups en els últims anys.

De manera que, podem veure que la investigació es dividirà en 2 capítols, el qual el seu primer proporciona el marc per desenvolupar el segon.

Llavors, per aconseguir l'objectiu d'aquest treball s'ha utilitzat la següent metodologia:

Primerament, s'han consultat diversos instruments del Dret Internacional, com els convenis i la costum, per saber quin és l'actual marc legal aplicable a les activitats cibernètiques. En aquesta direcció, també s'han consultat la jurisprudència del Tribunal Internacional de Justícia en relació a l'ús de la força i la legítima defensa.

Per altra banda, la pràctica estatal i la posició expressada pels governs en fòrums internacionals també serà important, ja que ens proporcionaran possibles indicadors d'una *opinio iuris*. A més, aquest treball no es limita a verificar la *lex lata*, sinó que analitza les sentències, opinions consultives i documents institucionals que expressen el que ha de ser el Dret Internacional i, per tant, també propostes de *lege ferenda*. En aquest sentit, les monografies i articles doctrinals juguen un paper molt rellevant.

Finalment, m'agradaria destacar que a banda de l'estructura i metodologia del treball que ens permetrà aconseguir l'objectiu, el propòsit d'aquest treball és també proporcionar al lector, en especial, aquell no familiaritzat en aquest àmbit, un resum acurat de no més de 50 pàgines que li proporcioni un coneixement bàsic, però suficient, sobre la problemàtica, les direccions que semblen emprendre les seves solucions i la meva valoració personal.

CAPÍTOL 1

EL PRINCIPI DE LA PROHIBICIÓ DE L'ÚS DE LA FORÇA I L'EXCEPCIÓ DE LA LEGÍTIMA DEFENSA EN EL DRET INTERNACIONAL

A. Origen del principi de l'ús de la força

Fins a finals del segle XIX, l'ús de la guerra per part dels Estats es considerava una prerrogativa derivada de la sobirania de l'Estat[1]. La guerra era un atribut d'aquest.

No serà fins a l'última fase del Dret Internacional clàssic que la comunitat internacional començarà a demostrar interès en el manteniment de la pau[2]. A les Conferències de La Haia de 1899 i 1907 no s'aconsegueix una prohibició general de la guerra, sinó només prohibir-la pel cobrament de deutes. Dels esforços per limitar el *ius ad bellum*, neix el *ius in bello*. S'imposen límits per tal d'humanitzar la guerra, però no es prohibeix recorre a ella.

Després de la Primera Guerra Mundial, la necessitat es fa més evident i motiva el Pacte de la Societat de Nacions (1919). La guerra es contempla com a últim recurs, estableix una moratòria pel seu exercici, i interpreta restrictivament el concepte de guerra (disputa armada entre 2 Estats prèvia declaració de guerra)[3]. S'aconsegueix una renúncia parcial al *ius ad bellum*.

No serà fins al Pacte Briand-Kellog de 1928 que es prendrà el pas decisiu a l'actual prohibició, donat que aquest suposarà un rebuig a la guerra com a instrument de política internacional[4], es condemna per fi recorrer a la guerra. No obstant això, el Tractat es referia únicament a la "guerra" formalment declarada i no a qualsevol ús de la força. I tampoc disposava d'un mecanisme de reacció capaç d'imposar sancions davant de les violacions de les seves disposicions[5].

La Carta de les Nacions Unides, formula per primera vegada una prohibició general de l'ús de la força. Suposa un abans i un després, convertint-se actualment en la principal font de principis de dret consuetudinari internacional respecte a l'ús de la força en relacions internacionals, i l'article 2(4) expressa un principi fonamental en aquest camp. Tot i això, aquest no està exempt d'un

[1] Fernández, A. F., Ortega, J. M., Forcada, I., Sánchez, Á., Ballesteros, V. i Martínez, M. (2022). *Curso de Derecho Internacional Público* (2ª ed.). Tirant lo Blanch, p.429. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788411472296

[2] Pastor, J. A. (2013). *Curso de Derecho Internacional Público y Organizaciones Internacionales* (17ª ed.). Tecnos, p.620.

[3] *Ibid.*

[4] Fernández, A. F., *et altr*. (2022). *Op. cit.*, p.430.

[5] Pastor, J. A. (2013). *Op. cit.*, p.621.

nombre important de problemes tècnics i legals que han sigut objecte de debat tots aquests anys i que seran revisats a continuació.

B. Àmbit i significat del principi de la prohibició de l'ús de la força

El principi de prohibició d'ús de la força és una de les pedres angulars del Dret Internacional, segons el Tribunal Internacional de Justícia (TIJ)[6], i com a element essencial de la societat internacional actual[7]. Per explicar i entendre correctament aquest principi en el Dret Internacional contemporani, hem de distingir els seus dos fonaments jurídics o la seva doble naturalesa universalment acceptada[8] -tant per la doctrina, la pràctica internacional, així com pel TIJ[9]-: l'article 2(4) de la Carta, com a norma convencional; i com a norma consuetudinària. No obstant això, resulta difícil assenyalar una data concreta en la qual la prohibició d'ús de la força es transforma en norma de Dret Internacional consuetudinària[10]. Autors com Brownlie, consideren que aquesta es va consolidar per la pràctica portada a terme entre els anys 1920 i 1945[11].

Per tant, la prohibició d'ús de la força és actualment tant una norma convencional com de dret consuetudinari internacional, i ambdues normes, són idèntiques en el seu contingut a dia d'avui. No obstant això, sembla difícil pensar que es mantingui una correlació exacta entre les dues indefinidament[12]. La diferència entre ambdues normes podria ser al·legada atenent al seu àmbit d'aplicació personal[13]. Però, tot i que la norma consuetudinària permetria en teoria una certa flexibilitat pel que fa a l'abast personal de la prohibició, aquesta es dirigeix principalment als Estats[14]. Segons Dörr, a la pràctica es pot observar una certa extensió a les Organitzacions Internacionals que dirigeixen operacions militars, les quals es solen declarar vinculades a les

[6] Sentència del Tribunal Internacional de Justícia (TIJ), 19 de desembre de 2005, assumpte relatiu a les activitats armades en territori del Congo (República Democràtica del Congo v. Uganda), p.223, para. 148.
[7] Cervell, M. J. (2018). The Use of Force against International Terrorrism: Everything Changes, Nothing Remains Still. *Paix et Sécurité Internationales*, 6, 47-65, p.65. http://dx.doi.org/10.25267/Paix sécur_int.2018.i6.03
[8] Dörr, O. (2019). Use of force, Prohibition of. *The Max Planck Encyclopedia of Public International Law*, p.3. http://opil.ouplaw.com; també Dutra, M. (2017). Uso de la Fuerza: ¿Conflicto entre la prohibición de su uso y la validez de la legítima defensa preventiva en el contexto de la lucha contra el terrorismo organizado?. *Política y Estrategia*, p.45-87. https://doi.org/10.26797/rpye.v0i129.71
[9] Sentència del Tribunal Internacional de Justícia (TIJ), 27 de juny de 1986, assumpte relatiu a les activitats militars i paramilitars contra Nicaragua (Nicaragua v. Estats Units d'Amèrica), p.99 i 100, para. 188 i 190.
[10] Fuentes, X. (2014). La prohibición de la amenaza y del uso de la fuerza por el derecho internacional. *Araucaria, 16*(32), 255-267, p.257. https://revistascientificas.us.es/index.php/araucaria/article/view/779
[11] Brownlie, I. (1963). *International Law and the Use of Force by States*. Oxford University Press, p.332.
[12] Dinstein, Y. (2005). *War, Aggression and Self-Defence* (4ª ed.). Cambridge: Cambridge University Press, p. 97.
[13] Dörr, O. (2019). *Op. cit*., p.4, para. 10.
[14] *Ibid*., p.8, para. 27.

normes consuetudinàries sobre l'ús de la força, per exemple l'Organització del Tractat de l'Atlàntic Nord (OTAN) a l'article 1 del seu Tractat constitutiu.

A més, en la redacció de la Convenció de Viena del Dret dels Tractats de 1969, la Comissió de Dret Internacional (CDI) ja apuntava en el seu comentari a l'actual article 53 del Tractat, que la prohibició de l'ús de la força constituïa en si mateixa un exemple de norma de Dret Internacional de caràcter *ius cogens*[15]. Més endavant aquesta postura va ser acceptada pel TIJ[16]. Tanmateix, bona part de la doctrina també la consideren actualment com una norma *ius cogens*. Autors com Green, expliquen els motius analitzant tots els components que ha de complir una norma per tenir tal consideració, d'acord amb l'article 53 de la Convenció[17]. Mentre que l'acceptació com a norma imperativa és majoritàriament universal, segons una minoria d'autors, com per exemple Linderfalk, s'oposen a la noció de normes *ius cogens per se*[18]. I uns altres, no neguen l'existència de la categoria de normes *ius cogens*, ni tampoc la consideració d'aquesta a la prohibició de l'ús de la força, però únicament en les formes més greus, això és l'agressió[19]. La prespectiva que s'accepterà al llarg d'aquest estudi és la darrera, doncs resulta difícil atribuir aquesta consideració a totes les formes d'ús de la força prohibides per aquest principi, d'acord amb una concepció amplia del mateix com veurem.

1. La prohibició només s'aplica a "relacions internacionals"

Per definició, el Dret Internacional general no s'ocupa dels assumptes interns dels Estats, sinó que formen part del camp del Dret intern[20]. A més, de la mateixa definició de l'article 2(4) de la Carta, en utilitzar l'expressió "en les seves relacions internacionals" ja denota la intenció d'aplicar-la exclusivament a conflictes interestatals. Igualment, l'aplicabilitat d'aquest principi únicament a les relacions internacionals, ha sigut afirmada pels *travaux preparatoires* i en diferents resolucions de l'Assemblea General de les Nacions Unides (AGNU), que com veurem

[15] Green, J. A. (2011). Questioning the Peremptory Status of The Prohibition of the Use of Force. *Michigan Journal of International Law, 32*(2), 215-257, p.222. https://repository.law.umich.edu/mjil/vol32/iss2/1
[16] Sentència TIJ (Nicaragua v. Estats Units d'Amèrica), *op. cit*., p. 100, para. 190.
[17] Green, J. A. *Op. cit*., p. 219-225.
[18] *Ibid*., p. 224.
[19] Rafighdoust, H. (2018). *The right of self-defense against cyber attacks by states and non-state actors.* [Tesi doctoral, Universitat Autònoma de Barcelona]. Tesis Doctorals en Xarxa (TDX), p.28. http://hdl.handle.net/10803/666857; també Green, J. A. *Op. cit*., p. 215-257.
[20] Hernández, A. (2000). Uso de la fuerza en el derecho internacional: aplicación en conflictos internos. *Agenda internacional, 7*(15), 161-181, p.175. https://revistas.pucp.edu.pe/index.php/agendainternacional/article/view/7272

a continuació, mai van tenir la intenció d'estendre el principi ni a conflictes interns dels Estats ni a actors no estatals[21].

Un exemple, com dèiem, és la resolució 2625 (XXV) que al parlar del principi de prohibició de l'ús de la força menciona que "Tot Estat té el deure d'abstenir-se de recórrer a l'amenaça o l'ús de la força per violar les fronteres internacionals existents d'un altre Estat o com a mitjà de resolució de conflictes internacionals [...]"[22]. Amb la resolució 3314 (XXIX) també podem arribar a aquesta conclusió, donat que el numeral tercer dedicat a mencionar en *numerus apertus* els actes que es poden considerar com agressió, fa referència constantment a l'ús de la força en territori d'un altre Estat[23].

En aquesta línia, la necessitat de l'element territorial, va ser clarament emfatitzat pel TIJ en l'Opinió Consultiva respecte de la Construcció d'un Mur en territori ocupat de Palestina[24]. El Tribunal sostenia que el concepte d'atac armat, en el marc de l'art. 51 de la Carta, només s'aplicava als atacs procedents de l'exterior del territori d'un Estat i imputables a un altre. Autors com Dörr, afirmen que el mateix s'aplica a la norma general sobre l'ús de la força[25].

Tot això, ens porta a la conclusió òbvia que en aplicar-se a relacions internacionals, la norma no prohibeix l'ús de la força en l'àmbit intern (dins el seu territori i contra els seus propis ciutadans o residents estrangers), el que no significa al seu torn que aquesta utilització de la força en l'àmbit domèstic pugui violar altres normes *ius cogens* previstes per l'ordenament internacional[26].

El principi tampoc procedeix envers els individus o grups no Estatals: no són membres de les Nacions Unides i, per tant, no se'ls hi pot aplicar la norma convencional[27]. Com ja hem dit anteriorment, tampoc són destinataris de la norma consuetudinària. De la pràctica dels Estats tampoc pot demostrar-se que s'accepti una ampliació de la norma per vincular-la als actors privats tant per les seves operacions armades, com per protegir-los contra les operacions dels Estats[28]. Fins i tot, resten lliures de la prohibició, encara que posseeixin la força financera, militar i organitzativa que els hi permeti la comissió d'actes armats amb escala i efectes similars als d'una

[21] Rafighdoust, H. (2018). *Op. cit.*, p.37.
[22] Resolució AGNU 2625 (XXV) "Declaració sobre els principis de dret internacional referents a les relacions d'amistat i la cooperació entre els estats de conformitat amb la Carta de les Nacions Unides", 24 d'octubre de 1970, p.132, para. 3 i 7.
[23] Resolució AGNU 3314 (XXIX) "Definició d'agressió", 14 de desembre de 1974, p.15, art.3.
[24] Advisory Opinion ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, I. C.J. Reports 2004, p.194, para. 139.
[25] Dörr, O. (2019). *Op. cit.*, p.7, para. 22.
[26] Rafighdoust, H. (2018). *Op. cit.*, p.30.
[27] Dörr, O. (2019). *Op. cit.*, p.8, para. 25.
[28] *Ibid.*

operació interestatal[29]. Com diu Franck, la guerra a petita escala o com moltes s'han pogut iniciar, adopten la forma d'operacions de *hit-and-run* en zones rurals o urbanes per bandes armades, moltes vegades sense uniforme[30]. El que s'intensifica amb la guerra moderna, la cibernètica. Una altra qüestió és que aquests actes puguin atribuir-se a un Estat segons els criteris assentats per la jurisprudència del TIJ. Es tracta de la denominada forma indirecta d'ús de la força que analitzarem en un apartat posterior.

a) El consentiment com a eximent de la responsabilitat internacional

Un aspecte a tractar en aquest apartat, però sense aprofundir, és el consentiment de la intervenció militar d'un altre Estat. L'ús de la força per un Estat suposa la violació d'una obligació internacional i, per tant, la comissió d'un fet il·lícit internacional[31]. Com posteriorment explicarem, la legítima defensa regulada a l'article 51 de la Carta, estaria admesa com a excepció d'aquesta norma. No obstant, la Comissió de Dret Internacional a l'article 20 del Projecte sobre responsabilitat internacional dels Estats (2001), també contempla el "consentiment" entre les circumstàncies que fan desaparèixer la il·licitud[32]. En tot cas, aquest principi bàsic de dret internacional exclou la il·licitud de l'acte en relació amb l'Estat que el consenteix, sempre que el consentiment sigui vàlid i en la mesura que el comportament romangui dins els límits del consentiment atorgat[33]. Perquè aquest sigui vàlid, haurà de ser lliure, haver-se manifestat clarament i prestar-se per una persona autoritzada per fer-ho en nom de l'Estat[34].

Avui en dia, l'aparició d'actors no estatals a escala internacional, com en accions de terrorisme, han portat a la comunitat internacional a acceptar cada vegada més la justificació de la intervenció armada en altres Estats[35]. Però, una altra qüestió molt diferent és justificar també l'ús de la força sense consentiment previ en territori d'altres Estats que es mostrin incapaços o no vulguin frenar a grups que operin des del seu territori. És el que es coneix com la doctrina *unwiling or unable to*

[29] *Ibid*., p.9, para. 29.
[30] Franck, T. M. (1970). Who Killed Article 2(4)? Changing Norms Governing the Use of Force by States. *The American Journal of International Law*, *64*(5), 809-837, p.813. https://doi.org/10.2307/2198919
[31] Cervell, M. J. (2018). Un caleidoscopio sobre el uso de la fuerza (el conflicto sirio). *Revista electrónica de estudios internacionales (REEI),* 36, p.5. http://www.reei.org/index.php/revista/num36/articulos/caleidoscopio-sobre-uso-fuerza-conflicto-sirio
[32] *Ibid.*
[33] Document A/56/10 de la Comissió de Dret Internacional (CDI), Informe sobre la tasca realitzada en el 53è període de sessions de 2001, p.77.
[34] Cervell, M. J. (2018). *Op. cit*., p.5 i 6.
[35] Rafighdoust, H. (2018). *Op. cit*., p.34; també Sentència TIJ (República Democràtica del Congo v. Uganda), *op. cit*, p. 198, para. 51 i 52.

act i en aquesta s'han basat principalment els Estats Units per justificar els seus atacs en territori afganés o sirià[36].

La violació de les condicions acordades o la permanència militar no autoritzada, és a dir, si el consentiment expira o es revoca i les tropes militars estrangeres decideixen no retirar-se, estaríem davant d'una agressió d'acord amb l'article 3(e) de la Resolució 3314 (XXIX).

b) Consideracions particulars respecte a les *guerres civils*

Finalment, considero oportú fer una referència a la guerra civil, ja que guarda relació amb l'exposat al llarg d'aquest apartat. En principi, és un assumpte intern de l'Estat i una de les parts involucrades en el conflicte serà sempre un actor no estatal.

En cas d'una guerra civil, es tracta, en principi, d'un assumpte intern de l'Estat i, per tant, del seu Dret intern. Ara bé, la situació legal canviarà si els rebels aconsegueixen estabilitzar un règim *de facto*, donat que com entitats preestatals també estan vinculades i protegides per la prohibició de l'ús de la força[37]. A més a més, per alguns autors, un Estat sobirà també ha de continuar estant protegit per la prohibició encara que perdi el seu govern efectiu i es converteixi en un denominat Estat fallit[38].

No obstant això, si en el marc d'un conflicte intern, per exemple una guerra civil, es verifica el vincle de l'actor no estatal amb un altre Estat segons els criteris del TIJ, com dèiem anteriorment, internacionalitza el conflicte intern i entra en joc la prohibició d'ús de la força[39]. Evidentment, si la forma d'intervenció d'un altre estat en aquest conflicte intern és directe, també el transforma automàticament en un conflicte internacional.

Per acabar, respecte del consentiment en el context de la guerra civil, hem de tenir en compte dos corrents doctrinals. La primera, afirma que aquest no serà vàlid si l'objectiu és resoldre aquesta en favor del govern establert[40]. Mentre que la segona, sostenint-se principalment amb la pràctica Estatal, distingeix entre l'ajuda que es presta al govern internacionalment reconegut, que estaria permesa, i la que es presta als rebels que no ho estaria[41].

[36] Cervell, M. J. (2018). *Op. cit.*, p. 17.
[37] Dörr, O. (2019). *Op. cit.*, p.7, para. 21.
[38] *Ibid*., p.8, para. 26.
[39] Rafighdoust, H. (2018). *Op. cit.*, p.35.
[40] *Ibid*., p.33; també Cervell, M. J. (2018). *Op. cit.*, p. 7.
[41] Cervell, M. J. (2018). *Ibid.*

2. Interpretació àmplia de l'article 2(4) de la Carta

a) Interpretació del concepte de força

És per a tots sabut que l'apartat 4 de l'article 2 de la Carta utilitza el terme "força" sense definir el seu contingut. Autors com Kelsen, han apostat per una interpretació extensiva, entenent que "l'ús de la força" de l'article 2(4) de la Carta, inclou tant l'ús de les armes, com una violació de Dret Internacional que involucri un exercici de poder en l'àmbit territorial però sense l'ús d'aquestes[42]. Autors com Brownlie o Dinstein, també opten per una interpretació extensiva, però amb més precaució, entenent que és correcte assumir que l'article 2(4) s'aplica també a força distinta de l'armada[43]. En canvi, autors com Pastor o Dörr, entre molts altres, han entès que d'acord amb el context de la Carta ha d'interpretar-se clarament en el sentit que es refereixi únicament a la força armada o militar[44].

Segons Brownlie, si bé és cert que els *travaux préparatoires* no indiquen que la frase s'apliqués únicament a la força armada, no podem deduir d'aquests i de la pràctica estatal o de les Nacions Unides que s'assumeixi el significat proposat per Kelsen[45]. Dit això, els qui aposten per una interpretació restrictiva del concepte de "força", el seu argument gira al voltant de les referències a la "força armada" que utilitza la Carta en algunes de les seves disposicions[46]. Al·leguen que el paràgraf 7 del Preàmbul de la Carta, així com l'article 41, 44 i 46 fan ús d'aquesta terminologia[47]. Tanmateix, es recolzen en l'argument que a la Conferència de San Francisco una proposta brasilera tendent a prohibir les represàlies econòmiques no va prosperar[48]. També, perquè l'article 51 dedicat a la legítima defensa, principal excepció de l'article 2(4), parla d'"atac armat", de la mateixa manera que ho fa la resolució 3314 (XXIX) en definir el terme d'"agressió".

No obstant això, és majoritàriament acceptat que efectivament la prohibició de l'ús de la força no inclou la coerció política o econòmica, el que no vol dir que no sigui contrari al principi de no intervenció[49].

[42] Citat per Brownlie, I. (1963). *Op. cit.*, p.362.
[43] *Ibid*.; Dinstein, Y. (2005). *Op. cit*., p.87 i 88.
[44] Pastor, J. A. (2013). *Op. cit*., p.622; Dörr, O. (2019). *Op. cit*., p.5, para. 13.
[45] Brownlie, I. (1963). *Op. cit.*
[46] Ruys, T. (2014). The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?. *American Journal of International Law, 108*(2), 159-210, p.163. https://doi.org/10.5305/amerjintelaw.108.2.0159
[47] Dörr, O. (2019). *Op. cit*., p.4, para. 11.
[48] Pastor, J. A. (2013). *Op. cit.*
[49] Dörr, O. (2019). *Op. cit*., p.4, para. 12; Pastor, J. A. (1986). *Ibid*.; Brownlie, I. (1963). *Op. cit.*

Una interpretació extensiva, comportaria donar cabuda a la prohibició l'ús de força "física" distinta de l'armada o militar.

De manera que una altra gran majoria, d'acord amb l'argumentat fins ara, han entès que efectivament en un començament l'opinió predominant respecte a la força es limitava a la força armada, i que la prohibició la inclou, però avui en dia l'abast del terme "força" ha de denotar violència sense importar com siguin els mitjans, sintètics o electrònics, per portar-la a terme[50].

En el seu moment, Brownlie ja sostenia que s'havia de decidir si les armes que no implicaven cap efecte explosiu amb onades de xoc i calor suposaven un ús prohibit de la força. Estem parlant d'armes bacteriològiques, biològiques i dispositius químics. Segons l'autor l'ús d'aquestes armes s'assimilaria a l'ús de la força per dos motius: perquè les agències implicades les solien classificar com a "armes" o formes de "guerra"; i perquè són usades per a la destrucció de la vida i béns, normalment descrites com a "armes de destrucció massiva"[51]. Més difícil, segons l'autor, seria l'expulsió deliberada i forçosa de població, l'alliberament de grans quantitats d'aigua transfronterera, la propagació d'incendis transfronterers, entre altres[52].

Aquesta divisió doctrinal, per tant, es podria resumir en què segons els qui interpreten l'article 2(4) d'acord un estàndard basat en els mitjans (interpretació restrictiva) l'ús de la força de l'article 2(4) només es refereix a la força armada. En canvi, els que l'interpreten segons un estàndard basat en els efectes, consideren que si per distingir entre les modalitats d'usos de la força prohibida, seguint el disposat pel TIJ, i com tractarem més endavant, s'utilitza el criteri d'escala i efectes: el tipus d'arma utilitzada és irrellevant i l'important serà que s'aconsegueixi el llindar de gravetat exigit[53]. De manera que, un atac no armat o de força no armada (per exemple, armes biològiques, químiques o atacs cibernètics) amb els mateixos efectes que un atac amb força armada serà considerat com un ús de força prohibida.

Personalment, considero que el més adequat i ajustat a la realitat actual és interpretar el concepte de força de forma extensiva o segons un estàndard basat en els efectes. En primer lloc, perquè d'acord amb el Preàmbul de la Carta, una de les finalitats de les Nacions Unides és "preservar a les generacions futures del flagell de la guerra", i com molts autors han comentat, el món s'enfronta avui en dia a canvis en la naturalesa dels conflictes internacionals, amb l'aparició de noves armes altament letals que suposen una amenaça als propòsits de les Nacions Unides[54]. En

[50] Rafighdoust, H. (2018). *Op. cit.*, p.55 i 56.
[51] Brownlie, I. (1963). *Op. cit.*
[52] *Ibid.*, p.363.
[53] Rafighdoust, H. (2018). *Op. cit.*, p.63.
[54] *Ibid.*, p.56.

segon lloc, hem de recordar que les disposicions de la Carta són dinàmiques en lloc d'estàtiques i que poden canviar segons la pràctica estatal[55]. Aquesta interpretació extensiva, a més, guanya pes si tenim en compte la possibilitat de força indirecta, també prohibida d'acord amb l'assentat pel TIJ. Doncs aquí ja no s'està utilitzant força armada, sinó organitzant, assistint, instigant a altres perquè la portin a terme.

b) Interpretació de la prohibició

Si bé el concepte de "força" el podem entendre de forma restringida (únicament a força armada) o àmplia, la doctrina majoritària està d'acord en entendre la prohibició d'acord amb una interpretació àmplia. Només una limitada part dels autors i una limitada pràctica consuetudinària ha suggerit el contrari[56].

Aquests últims, d'acord amb una interpretació literal i formalista, entenen que l'ús de la força només està prohibida quan és dirigida contra "la integritat territorial o la independència política de qualsevol Estat o en qualsevol forma incompatible amb els propòsits de les Nacions Unides"[57]. Aleshores aquesta interpretació ens porta a pensar que si la força s'utilitza amb una finalitat distinta de la mencionada *expressis verbis* a l'article 2(4) (en cas que fos possible) o per fer complir algun dels propòsits de les Nacions Unides, estaríem davant de supòsits d'ús de la força no prohibida[58].

Respecte a aquesta última qüestió, sorgeix la problemàtica de les intervencions humanitàries. És difícil negar l'existència d'aquesta figura després de la importància que ha significat la Carta pel que fa a la protecció dels drets humans i llibertats fonamentals; i l'auge dels sistemes democràtics i de la protecció dels drets humans[59]. Això ha comportat, que les Nacions Unides tant pel que fa al dret d'autodeterminació dels pobles com pel que fa a la protecció dels drets humans, com ja sabem, hagi practicat una política constant i permanent, sobretot des de 1960, segons la qual aquestes matèries no es podien considerar com que formaven part essencialment de la jurisdicció interna dels Estats[60]. Ara bé, a l'hora de passar de la teoria a la pràctica, el cert és que les Nacions Unides no ha intervingut en ocasions en què la intervenció hagués estat legitimada. I una de les

[55] *Ibid*., p.62.
[56] Ruys, T. (2014). *Op. cit*., p.163.
[57] Pastor, J. A. (2013). *Op. cit*., p.623.
[58] *Ibid.*
[59] Bermejo, R. i López-Jacoiste, E. (2013). De la intervención por causas humanitarias a la responsabilidad de proteger. Fundamentos, similitudes y diferencias. Dins Ministerio de Defensa (ed.), *La respuesta del Derecho Internacional a los problemas actuales de la Seguridad Global* (17-76), p.29 i 30. https://www.ieee.es/Galerias/fichero/cuadernos/CE_210_RedesTranseuropeas.pdf
[60] *Ibid.*

principals raons ha sigut la ineficiència del sistema de seguretat col·lectiva de la Carta. Per això, a falta d'un mecanisme de les Nacions Unides envers la intervenció humanitària capaç d'actuar allà on sigui necessari, els Estats han intervingut quan han considerat que hi havia una extrema necessitat[61]. Respecte al TIJ, en l'assumpte de Nicaragua, va utilitzar formulacions que podrien interpretar-se com una declaració, almenys implícita, en contra de la intervenció humanitària, quan va assenyalar que l'ús de la força no podia ser el mètode adequat per supervisar o garantir aquest respecte (dels drets humans a Nicaragua)[62].

Els professors Remiro-Brotons i Gutiérrez, en aquest sentit, consideren que la intervenció humanitària no viola l'article 2(4) i, per tant, no pot ser prohibida pel Dret quan la societat internacional organitzada és incapaç de reprimir tals accions[63]. Altres, com Aréchaga o Pastor, consideren que tot ús de la força, excepte en legítima defensa, és prohibida per l'article 2(4). Bàsicament, perquè si bé la intervenció humanitària podria alinear-se amb els propòsits de les Nacions Unides, en particular l'article 1(3), consideren que el manteniment de la pau i la seguretat internacional, d'acord amb l'article 1(1), és el propòsit fonamental i dominant pel qual tots els altres s'han de subordinar. Doncs el compliment d'aquests últims depèn de l'èxit d'aquesta condició bàsica[64].

Personalment, considero que la intervenció humanitària no es pot justificar per la seva compatibilitat amb l'article 2(4). Si bé és cert que el sistema del Consell de Seguretat suposa en moltes ocasions un bloqueig o paràlisi ineficient, la pau i seguretat internacional són valors primordials i l'article 2(4) és un principi fonamental per aconseguir-ho, sense restriccions ni limitacions, sinó amb la màxima extensió o amplitud que pugui abastar tal prohibició. Una altra cosa molt diferent, és la justificació d'aquestes intervencions humanitàries d'acord amb el dret consuetudinari per l'aparició d'un nou dret o excepció al principi, com ho ha fet sovint el Regne Unit[65].

Tornant a la interpretació, la majoria de la doctrina, com hem dit, està d'acord en interpretar la prohibició de l'ús de la força de forma àmplia. En primer lloc, segons l'argument de la intenció dels redactors de la Carta, es considera que la prohibició no es limita a la força dirigida contra la integritat territorial o la seva independència política, sinó que la frase final de l'article 2(4), que parla de qualsevol força "incompatible amb els propòsits de les Nacions Unides" es tracta d'una

[61] *Ibid.*
[62] Dörr, O. (2019). *Op. cit.*, p.15, para. 49.
[63] Pastor, J. A. (2013). *Op. cit.*
[64] *Ibid.*, p.624.
[65] Wood, M. (2013). "The International Law on the Use of Force. What Happens in Practice?", *Indian Journal of International Law, 53*, 345-367, p.352. https://legal.un.org/avl/pdf/ls/Wood_article.pdf

disposició residual (*catch-all phrase*), deixant clar que consisteix en una prohibició global contra tot ús de la força[66]. En segon lloc, segons els *travaux préparatoires* de la Carta, la referència a la "integritat territorial" i a la "independència política" es va introduir en el text de la disposició per posar èmfasi a dues formes particularment greus d'ús prohibit de la força i en cap cas per restringir el seu abast[67]. En tercer lloc, el TIJ ja ha mencionat en determinades ocasions la impossibilitat d'una interpretació restrictiva. Això ho veiem a l'assumpte de Corfu Channel en què el Tribunal no accepta la reclamació del Regne Unit d'una interpretació restrictiva de l'article[68], així com en el cas de Nicaragua de 1986[69], en el de les Plataformes Petrolíferes[70], i en el de les Activitats armades en territori del Congo[71].

Segons Ruys, aquesta lectura és recolzada pel context, objectiu i la finalitat de la disposició: doncs els pares fundadors de les Nacions Unides desitjaven ampliar la prohibició preexistent del recurs a la guerra establert en el Pacte de París per "preservar a les generacions futures del flagell de la guerra"[72]. Per tant, l'origen, l'objecte i els treballs preparatoris suggereixen que la prohibició abasti tot ús de la força que dirigeixi un Estat contra un altre. I en tot cas, segons l'autor, la càrrega de la prova hauria de recaure en aquells que al·leguen una interpretació més restrictiva[73].

No obstant això, autors com Gray i Dörr, apunten que la problemàtica respecte a l'abast de l'article 2(4) té poques implicacions a la pràctica, donat que els Estats poques vegades intenten interpretar la disposició de manera restrictiva, sinó que l'objecte de discussió normalment es centra en l'abast i contingut de certes excepcions a la prohibició[74].

Personalment, considero que no aplicar la Carta a situacions d'ús de la força que no han sigut expressament excloses de l'aplicació de l'article 2(4), seria contradictori amb el desenvolupament progressiu del Dret Internacional[75] i minvaria la garantia de màxima protecció dels Estats més petits davant d'accions dels més grans i poderosos[76]. També crec que aquesta interpretació extensiva es fa encara més evident per la prohibició de la força indirecta.

---

[66] Ruys, T. (2014). *Op. cit.*, p.164; també Dörr, O. (2019). *Op. cit.*, p.5, para. 14.
[67] Dörr, O. (2019). *Ibid.*
[68] Ruys, T. (2014). *Op. cit.*, p.166.
[69] Sentència TIJ (Nicaragua v. Estats Units), *op. cit.*, p.103, para. 195.
[70] Sentència del Tribunal Internacional de Justícia (TIJ), 6 de novembre de 2003, assumpte relatiu a les Plataformes Petrolíferes (República Islàmica d'Iran v. Estats Units), p.186, para. 51.
[71] Sentència TIJ (República Democràtica del Congo v. Uganda), *op. cit.*, p.227, para. 164 i 165.
[72] Ruys, T. (2014). *Op. cit.*, p.164.
[73] *Ibid.*
[74] Dörr, O. (2019). *Op. cit.*, p.2, para. 2; també Gray, C. (2008). *International Law and the Use of Force* (3ª ed.). Oxford University Press, p.31 i 32. https://doi.org//10.1093/law/9780198808411.001.0001
[75] Rafighdoust, H. (2018). *Op. cit.*, p.54.
[76] Brownlie, I. (1963). *Op. cit.*, p.267.

Fins ara, hem parlat de la força directa que pot exercir un Estat contra un altre, però en el cas de Nicaragua, d'acord amb les Resolucions de l'AGNU 2131 (XX) i 2625 (XXV), el TIJ ja va entendre que organitzar forces rebels o bandes armades i participar en conflictes interns en un altre Estat és contrari a la prohibició d'ús de la força, a més d'una clara violació del principi de no intervenció[77]. No obstant això, hem de tenir en compte que no tota participació indirecta constituirà un ús de la força prohibida, ni tampoc del mateix tipus. En aquest sentit, el Tribunal expressava que el subministrament de fons a les forces irregulars no constituïa *per se* un ús de força prohibida[78]. Així mateix, perquè aquest ús de la força indirecta pugui considerar-se una agressió o atac armat, la gravetat de l'ús de la força irregular ha de ser similar a la que puguin portar a terme forces regulars[79]. De manera que el subministrament d'armes, logística, etc., no constituiria una agressió, però sí un ús de força indirecta prohibida. I aquí podrien aparèixer els problemes per determinar si l'ajuda prestada és certament militar o humanitària.

c) Llindar general de força prohibida i modalitats segons la gravetat

Arribats aquest punt, ens podríem preguntar si en realitat existeix algun llindar de força mínima que desencadeni la prohibició i el qual hagi d'assolir-se perquè pugui ser aplicada[80]. En el cas de Nicaragua, el TIJ va afirmar l'existència d'una bretxa entre els articles 2(4) i 51 (sobre el dret de legítima defensa), i per tant era necessari "distingir entre les formes més greus de l'ús de la força (atac armat) i d'altres menys greus", la diferència entre les quals, segons el Tribunal, radicava principalment en una qüestió d'"escala i efectes"[81], això és la gravetat de la força. També, les declaracions fetes durant les negociacions sobre la definició d'agressió de l'AGNU indiquen que la noció de força té un abast més ampli que l'atac armat o l'agressió i que incidents menors que no es qualifiquin d'agressió podran constituir, tanmateix, un ús de la força[82].

Per aquestes raons considero una equivocació entendre, com ho han fet alguns autors, el propòsit de l'article 2 (4) no com una prohibició, sinó com a pressupòsit de legitimitat per actuar. Ja que, es podria pensar que si només prohibeix l'atac armat o l'agressió, tots els altres usos de la força que quedessin per sota del llindar exigit per la prohibició, estarien permesos. Però, de nou, aquest article és més ampli que l'excepció de la legítima defensa de l'article 51 i comprèn altres usos de la força més enllà de les més greus.

[77] Cervell, M. J. (2018). *Op. cit*., p.12.
[78] Rafighdoust, H. (2018). *Op. cit*., p.66.
[79] *Ibid*., p.65.
[80] Dörr, O. (2019). *Op. cit*., p.6, para. 18.
[81] Ruys, T. (2014). *Op. cit*., p.165.
[82] *Ibid*., p.164.

En aquest sentit les modalitats d'usos de força prohibida (de la més greu a menys) es podrien classificar de la següent manera: Atac armat, Agressió, altres formes menys greus de força prohibida i altres formes de força potencialment prohibides[83]. La raó d'aquesta classificació serà entesa més endavant, quan veiem que no tota agressió es considera un atac armat, i que el nucli d'aquest últim tipus de força serà encara més reduït.

Autors com Corten i O'Connell han defensat aquest suposat llindar de mínims analitzant la pràctica consuetudinària corresponent[84]. Altres com Ruys, interpreten finalment que és encerat dir que l'aplicació de l'article 2(4) no està subjecte a un llindar general de gravetat[85] i que, per tant, depèn de les circumstàncies especials de cada cas. En opinió personal, l'estudi realitzat per Corten i O'Connell i les proves aportades per defensar el llindar de mínims, crec que és substancial i no ha de passar-se per alt així com així. No obstant, estic d'acord amb Ruys en què hem de ser cautelosos amb la qüestió. En primer lloc, i sobretot, perquè el fet que un Estat no utilitzi el llenguatge de l'ús de la força no sempre reflecteix una convicció jurídica subjacent; en segon lloc, perquè en diversos contextos també s'ha utilitzat el llenguatge de l'article 2(4) o 51 en relació a determinats actes de força de menor escala; i, en tercer lloc, perquè aquest llindar de mínims no està recolzat per la pràctica estatal i, per tant, de moment, s'ha de descartar[86].

C. La Legítima Defensa com a excepció al principi de la prohibició de l'ús de la força

1. Consideracions generals i característiques principals

La importància de la legítima defensa en el Dret Internacional contemporani deriva de la seva posició com a principal excepció a la prohibició general de l'ús de la força en l'article 2(4) de la Carta[87].

La legítima defensa com a norma convencional es troba reconeguda a l'article 51 de la Carta. Segons Franck, aquesta disposició es va incloure a la Carta perquè els seus redactors temien que el mecanisme d'acció col·lectiva previst a l'article 43, que desplegaria el Consell de Seguretat, no arribés a existir i que, en conseqüència, els Estats haguessin de continuar basant-se en el seu "dret inherent" d'autodefensa[88]. Per tant, el reconeixement d'un dret alternatiu de legítima defensa era essencial per la seguretat dels Estats en casos de bloqueig del funcionament del sistema de

[83] Rafighdoust, H. (2018). *Op. cit*., p.57 i 58.
[84] Ruys, T. (2014). *Op. cit*., p.208 i 209.
[85] *Ibid*., p.171.
[86] *Ibid*., p.209.
[87] Greenwood, C. (2011). Self-Defence. *Max Planck Encyclopedias of International Law*, p.2, para. 2. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e401
[88] Franck, T. M. (1970). *Op. cit*., p.839.

seguretat col·lectiva[89]. És per això, que tant per la terminologia usada com per la història de la disposició de la Carta, molts autors coincideixen que no crea cap dret nou, sinó que reconeix o confirma, dintre dels límits establerts en l'article 51, que es preserva el dret consuetudinari de legítima defensa[90]. De la mateixa manera, cal reconèixer que no totes les condicions i tots els requisits pel seu exercici estan expressats en el seu tenor literal, en aquest sentit, el requisit de necessitat i proporcionalitat són algunes de les característiques del dret consuetudinari que es requereixen tot i no mencionar-se en el text de la disposició[91]. En qualsevol cas, la qüestió respecte de si compleixen aquests requisits i condicions no depèn exclusivament del judici subjectiu de l'Estat que invoca la legítima defensa com a justificació del seu ús de la força, sinó que poden ser valorades i controlades pel TIJ[92]. Sent aquests requisits, segons les paraules del mateix TIJ, estrictes i objectius, sense deixar marge de discrecionalitat en la seva aplicació[93].

En aquest context, alguns Estats i autors recolzen l'expansió de l'abast de l'aplicació d'aquest dret, entenen que la norma consuetudinària coexisteix i que és més àmplia que la convencional[94]. Per exemple, el debat respecte de si la norma consuetudinària requeria un atac armat, o en realitat es permetia la legítima defensa davant de qualsevol ús de la força. Un major nombre de defensors, afirmen que la pràctica estatal ja l'havia restringit i la Carta l'únic que va fer és cristal·litzar-ho[95]. També el debat sobre si la norma consuetudinària permetria una legítima defensa preventiva.

El dret de la legítima defensa també es troba implícitament reconegut en les resolucions 2625 (XXV) i 3314 (XXIX) de l'AGNU, i explícitament reconegut a la resolució 42/22 de l'AGNU[96].

Segons la CDI, entén la legítima defensa com a circumstància que exclou la il·licitud d'un acte que d'altra manera seria il·lícit, sempre que, d'acord amb l'article 21 del Projecte d'articles sobre responsabilitat de l'Estat per fets internacionalment il·lícits, aquest s'hagi adoptat en legítima defensa conforme la Carta de les Nacions Unides. Això vol dir que quan un Estat amb dret a actuar en legítima defensa excedeixi dels límits fixats per la Carta (article 51), no s'exclourà la

[89] Casanovas, O. i Rodrigo, A. J. (2019). *Compendio de Derecho Internacional Público* (8ª ed.). Tecnos, p.434.
[90] Greenwood, C. (2017). *Op. cit.*, p.2, para. 3; també Pastor, J. A. (2013). *Op. cit.*, p.625.
[91] Greenwood, C. (2017). *Ibid.*
[92] Juste, J., Castillo, M., i Bou, V. (2018). Lecciones de Derecho Internacional Público (3ª ed.). Tirant lo Blanch, p.359. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788491906650
[93] *Ibid*., p.360.
[94] Rafighdoust, H. (2018). *Op. cit.*, p.102.
[95] Cervell, M. J. (2017). *La Legítima Defensa en el Derecho Internacional Contemporáneo*. Tirant lo Blanch, p.31. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788491690788
[96] Rafighdoust, H. (2018). *Op. cit.*

il·licitud de l'acte, i per tant violarà la prohibició de l'ús de la força. En aquest sentit, també és important recordar que l'actuació en legítima defensa (vàlida) no impedeix la infracció d'altres normes de Dret Internacional, sobretot les del *ius in bello*, i en particular les del Dret Internacional Humanitari, per exemple en utilitzar una arma prohibida per aquest[97].

Finalment, l'article 51 preserva no només la legítima defensa individual, sinó també la col·lectiva. Tot i que el text de la disposició no estableix cap distinció entre elles, la pràctica i la jurisprudència posteriors n'han identificat algunes[98]. No obstant això, en els apartats que segueixen ens atendrem a la individual.

2. Atac armat com a requisit principal per a l'exercici del dret a legítima defensa

El primer requisit i el més important de la legítima defensa és l'exsistència d'un atac armat. No obstant això, abans de res, és valuós tenir en compte, com ja destacàvem en els apartats corresponents a l'ús de la força, que la redacció de la Carta s'inscriu en un context històric en el qual el concepte d'"atac armat" difícilment podia concebre's al marge de les forces armades regulars d'un Estat[99]. També cal recordar, que l'atac armat és una de les formes prohibides d'ús de la força, però no l'única. No obstant, només la víctima d'un atac armat, i no d'un ús qualsevol de força prohibida, podrà invocar el dret a legítima defensa. En el cas de les Plataformes Petrolíferes, en Tribunal Internacional de Justícia va establir que la càrrega de la prova de l'existència de l'atac armat correspon a l'Estat que justifica el seu ús de la força en legítima defensa[100]. El TIJ ha qualificat aquest requisit com a condició *sine qua non* per a l'exercici del dret a legítima defensa[101]. Aquest consta a l'article 51 de la Carta, però també ha sigut reconegut pel TIJ en diverses ocasions. Tot i això, ni la Carta ni la jurisprudència, ofereixen una definició d'atac armat. És per això, que els dos referents a l'hora d'entendre quan aquest existirà seran, fonamentalment, la resolució 3314 (XXIX) i la jurisprudència del TIJ, que evitant sempre oferir un concepte general, sí que ha anat aclarint quines accions poden ser constitutives d'atac armat[102].

Juntament amb el concepte d'atac armat, apareix el d'agressió. En primer lloc, perquè tot i utilitzar el concepte d'atac armat a la versió espanyola i anglesa de la Carta, la francesa en l'article 51

[97] Greenwood, C. (2017). *Op. cit.*
[98] *Ibid*., p.3, para. 5.
[99] Sánchez, L. I. (2002). Una cara oscura del Derecho Internacional: legítima defensa y terrorismo internacional. *Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteiz*, 1, 217-266, p.276. Disponible a: https://www.ehu.eus/documents/10067636/10678077/2002-LuisIgnacio-Sanchez-Rodriguez.pdf
[100] Dinstein, Y. (2005). *Op. cit*., p.182.
[101] Juste, J., Castillo, M., i Bou, V. (2018). *Op. cit.*
[102] Cervell, M. J. (2017). *Op. cit*., p.81.

utilitza la terminologia "agression armée". En segon lloc, perquè ambdós conceptes apareixen en diferents disposicions de la Carta, a l'article 51 com "atac armat", i als articles 39 i 1 de la Carta com a "agressió". De la lectura d'aquests articles, sembla despendre's que ambdós conceptes no són iguals, i tampoc ha sigut aquest l'enfocament adoptat a la pràctica internacional[103]. Segons Cervell, el concepte d'atac armat és més limitat, en contingut, que el d'agressió, donat que a l'assumpte de Nicaragua el TIJ exigia un ús material de força armada que a més revestís una certa entitat. Brownlie, també està d'acord que l'ús de força ha de revestir certa gravetat per poder ser considerat com atac armat[104]. Per altres, la diferència entre ambdós conceptes és tan petita que moltes vegades és passada per alt, i l'atac armat només es produiria quan la força és usada en relativa gran escala amb suficient gravetat per tenir efectes substancials[105]. Per tant, tot i que a la pràctica, el concepte d'"ús de la força", "agressió" i "atac armat" s'utilitzen moltes vegades com equivalents, aquests no sempre coincideixen[106].

L'Associació de Dret Internacional (ILA), l'any 2016 ja constatava l'absència d'una definició clara d'atac armat i assenyalava alguns aspectes que ens podien ajudar a determinar la seva existència: la seva escala i efectes, la intenció hostil i la possible acumulació de successos menors[107]. En aquest sentit, l'aplicació descentralitzada del DIP comportarà que siguin els Estats els que en primera instància i de forma unilateral decideixin si existeix un comportament per part d'un altre Estat que constitueix un atac armat, i contra el que cal reaccionar en legítima defensa. En tot cas, segons l'article 51, la obligació de comunicar en un "breu període de temps" les accions dutes a terme en legitima defensa al Consell de Seguretat, fa que aquest òrgan sigui en última instància de determinar si hi ha hagut en realitat un atac armat previ. El cert és que el Consell de Seguretat no s'ha mostrat molt explícit en aquesta qüestió, evitant sempre referir-se a l'atac armat *stricto sensu* i limitant-se a indicar quines conductes o fets podrien considerar-se una amenaça o violació de la pau i la seguretat internacional[108].

La resolució 3314 (XXIX), a l'article 3, enumera sense ànim d'exhaustivitat, assumpcions clàssiques d'actes de gravetat suficients per a considerar-se agressions, en què, de fet, ens serveix per poder interpretar el terme d'atac armat, tenint en compte que com hem dit, la definició inclou actes que no necessàriament es qualifiquen d'"atacs armats"[109]. Dit d'una altra manera, els actes que s'inclouen en aquesta llista com a "agressions", subjectes a certes condicions, podran

[103] Greenwood, C. (2011). *Op. cit*., p.4, para. 10.
[104] Brownlie, I. (1963). *Op. cit*., p.366.
[105] Rafighdoust, H. (2018). *Op. cit*., p.114 i 115.
[106] *Ibid*., p.114.
[107] Cervell, M. J. (2017). *Op. cit*., p.86.
[108] *Ibid*., p.86 i 87.
[109] Rafighdoust, H. (2018). *Op. cit*., p.115.

qualificar-se com "atacs armats". Un exemple clar és la lletra g, ja que el TIJ en el cas de Nicaragua exigia que en els supòsits d'usos de força indirecta perquè es pogués considerar com un atac armat, l'atac de les forces irregulars havia de ser similar al que haguessin portat a terme les forces regulars d'un Estat; donat que havíem de diferenciar entre les formes més greus d'ús de la força, de les altres formes menys greus[110]. Per tant, els mers usos de força o actes d'agressió sense la suficient gravetat no podran, en cap cas, constituir un atac armat per justificar la legítima defensa.

Per tant, una altra qüestió a tractar és la del llindar de gravetat perquè es pugui considerar com "atac armat". El TIJ ha tingut diverses oportunitats per pronunciar-se, i ho ha fet de forma restrictiva[111]. Per exemple, en l'assumpte de les Plataformes Petrolíferes de 2003 en considerar un ús menor de la força, l'impacte d'una mina en un vaixell nord-americà i contra un altre d'interès nord-americà[112]. El Tribunal ha evidenciat altres exemples que podrien considerar-se com a tals, entre d'altres: trets a un vaixell o a un helicòpter, mers incidents fronterers, tolerar en el mateix territori d'un Estat activitats que ajudin a perpetuar actes terroristes, etc. De manera que, de nou, les circumstàncies especials i la realitat de cada cas seran determinants per perfilar i enquadrar l'acció concreta[113]. En aquest sentit, en un primer moment, tot i no indicar-nos el nivell o llindar de gravetat, sembla que sí que hauria d'existir. No obstant això, alguns autors com Dinstein, han criticat que el Tribunal al no establir quin llindar s'ha d'aconseguir perquè l'ús de la força es consideri un atac armat, no hi hauria motiu per excloure els atacs armats a petita escala de l'espectre dels atacs armats[114]. Aquesta tendència a l'extensió ha sigut generalitzada en els darrers anys.

Segons la jurisprudència del TIJ, molt cautelosa pel que fa a l'atac armat i la legítima defensa, hem de destacar que també va deixar la porta oberta a l'acumulació d'atacs menors, que estimats en conjunt poguessin arribar al llindar mínim de gravetat per considerar-se com un atac armat[115]. A més a més, també ha assenyalat que l'origen de l'atac ha de ser estatal perquè tingui lloc la legítima defensa[116]. Tot i que, com tractarem més endavant, aquesta tendència sembla que està canviant, i que també es permet enfront d'atacs d'actors no estatals, a partir sobretot dels successos de l'11-S. Una altra qüestió, tractada en el cas de les Plataformes Petrolíferes, és la intenció de l'agressor de perjudicar a un objectiu específic d'un Estat víctima, com a requisit per

[110] Sentència TIJ (Nicaragua v. Estats Units d'Amèrica), *op. cit.*, p.101, para. 191.
[111] Cervell, M. J. (2017). *Op. cit.*, p.92.
[112] Sentència TIJ (República Islàmica d'Iran v. Estats Units), *op. cit.*, p.191 i 192, para. 64.
[113] Cervell, M. J. (2017). *Op. cit.*
[114] Dinstein, Y. (2005). *Op. cit.*, p.195.
[115] Cervell, M. J. (2017). *Op. cit.*, p.106.
[116] Advisory Opinion TIJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, *op. cit.*, p.194, para. 139.

constatar un atac armat. Aquest punt de vista ha estat criticat per molts autors, com Cervell, que expressen que en realitat l'element "intencional" obeeix més a raons lògiques que jurídiques i en aquest assumpte es va utilitzar més com a requisit independent i no tant com a factor determinant per aclarir si l'ús de la força constituïa o no un atac armat[117]. Segons la mateixa autora, tampoc la pràctica estatal demostra el contrari, sinó que refuta incloure l'element intencional com a requisit específic.

Es poden plantejar altres qüestions, com per exemple l'objectiu que ha de tenir l'atac armat. Doncs perquè un Estat tingui dret a l'ús de la força en legítima defensa individual és necessari que es produeixi un atac armat contra aquest Estat, de manera que, es podria platejar la qüestió de què ha de considerar-se que constitueix "l'Estat" a aquests efectes. També la qüestió concernent a si és possible o no que l'atac armat es produeixi dintre del territori de l'Estat agressor. També respecte a la possibilitat que es va preveure en el cas de Nicaragua de contramesures, anàlogues però menys greus a la legítima defensa, en resposta d'usos de la força menys greus que un atac armat[118]. Tots aquests aspectes no seran abordats en deteniment en aquest apartat, sinó que es tractaran quan siguin necessaris en els pròxims apartats.

En opinió personal, considero que el TIJ s'ha mostrat clarament aferrat al passat, limitant-se a una interpretació de la legítima defensa estricta a la Carta i evitant noves interpretacions més flexibles que ja defensen la major part de la doctrina i, fins i tot, certes instàncies dins de les mateixes Nacions Unides[119]. De manera que estic d'acord amb Dinstein, en què l'atac armat ha de pressuposar un ús de la força que produeixi greus conseqüències, personificades en intrusions territorials, víctimes humanes o destruccions considerables de béns[120]. I per això, el tipus d'arma utilitzada és irrellevant, donat que d'acord amb l'Opinió Consultiva de la Legalitat de l'Amenaça o l'Ús d'Armes Nuclears, l'article 51 no només es refereix a armes específiques, sinó que s'aplica a qualsevol atac armat, amb independència de l'arma utilitzada[121]. Això és: convencional o no convencional, primitiva o sofisticada, sintètica o electrònica.

3. Altres requisits

a) Legítima defensa i Consell de Seguretat

L'article 51 de la Carta recull dues condicions o exigències per a l'exercici de la legítima defensa.

[117] Cervell, M. J. (2017). *Op. cit*., p.111.
[118] Dinstein, Y. (2005). *Op. cit*., p.194.
[119] Cervell, M. J. (2017). *Op. cit*., p.97.
[120] Dinstein, Y. (2005). *Op. cit*., p.193.
[121] *Ibid*., p.196.

La primera és un deure d'informació. L'Estat que adopta mesures de força en exercici del seu dret a legítima defensa és qui també ho ha de comunicar immediatament al Consell de Seguretat. El deure d'informació s'explica per la responsabilitat primordial que té aquest òrgan, com bé sabem, de manteniment de la pau i de la seguretat internacional[122]. No obstant això, l'opinió predominant és considerar l'Informe com un requisit merament procedimental, que en tot cas suposaria una violació de la norma de la Carta, però no la impossibilitat d'al·legar la legítima defensa; en tant que per la pràctica estatal, la jurisprudència del TIJ i la doctrina no l'entenen com un requisit ineludible ni equiparable als de necessitat o proporcionalitat[123].

La segona és el caràcter temporal que ha de tenir la legítima defensa empresa. Doncs, aquesta haurà de finalitzar, d'acord amb l'article 51 de la Carta, quan el Consell de Seguretat hagi pres les mesures necessàries. La funció principal de l'òrgan i la idea del mecanisme residual i excepcional que es tenia, en el moment de la redacció de la Carta, de la legítima defensa davant de l'actuació del Consell enfront qualsevol amenaça o ús de la força[124], explicarien el perquè d'aquesta condició juntament amb la lògica necessitat de repel·lir l'atac i, per tant, de la immediatesa en que ha de tenir lloc la defensa. Personalment, considero que si bé aquesta idea de provisionalitat i subsidiarietat encaixava perfectament en el model de seguretat col·lectiva que es tenia, avui en dia resulta difícil considerar que el Consell hagi portat a terme correctament aquesta funció.

b) Necessitat, Proporcionalitat i Immediatesa

Com hem dit, respecte als requisits i condicions per l'ús de la força en legítima defensa, no es troben únicament al text de l'article 51, sinó que també deriven del dret consuetudinari. La necessitat i proporcionalitat són requisits tradicionalment exigits per aquest que es remunten al cas *Caroline* de 1837. Tot i que la doctrina en moltes ocasions els hagi equiparat, són considerats pel TIJ com a dos requisits per separat[125] i reconeguts com a criteris per la legalitat de la legítima defensa en nombroses ocasions, no només pel Tribunal sinó també per la CDI[126].

Autors com Pastor, entenen que el Dret Internacional general de naturalesa consuetudinària també inclouria el requisit de la immediatesa[127]. Això és que la resposta en legítima defensa ha de ser immediata a l'atac patit o el que està tenint lloc en aquell moment. És a dir, que no transcorri un

[122] Juste, J., Castillo, M., i Bou, V. (2018). *Op. cit.*, p.366.
[123] Cervell, M. J. (2017). *Op. cit.*, p.144.
[124] *Ibid*., p.33 i 34.
[125] Greenwood, C. (2011). *Op. cit.*, p.8, para. 26.
[126] Cervell, M. J. (2017). *Op. cit.*, p.136.
[127] Pastor, J. A. (2013). *Op. cit*., p.623.

temps excessiu entre l'atac armat i l'exercici de la legítima defensa[128]. Aquest requisit té una relació estreta amb el requisit de necessitat perquè si no hi ha immediatesa, no hi ha necessitat de reaccionar. Respecte a la possibilitat d'actuar preventivament o davant d'un atac imminent serà tractat més endavant.

La necessitat implica que l'ús de la força sigui l'únic mitjà (*ultima ratio*) al que l'Estat pugui recórrer, sense tenir-ne d'altres a la seva disposició per parar l'atac armat i mantenir la seva integritat[129]. De manera que només complirà el requisit, si pot demostrar que no podia haver aconseguit l'objectiu (defensar-se de l'atac armat) sense recórrer a la força[130]. Això suposa que la legítima defensa sempre sigui per un propòsit defensiu i no per altres com represàlies, dissuadir, o castigar; per tal de no posar en perill la pau i la seguretat internacional[131]. En el cas de les Plataformes Petrolíferes, el TIJ ja va refutar la legítima defensa al·legada pels Estats Units per no considerar-la "necessària" en haver-se dirigit contra determinats objectius que el Tribunal no considerava adequats (la destrucció de les plataformes)[132].

Segons Cervell, es tracta d'un requisit estricte que ni el TIJ ha aplicat en tot el seu rigor, donat que de la seva jurisprudència sembla concebre la necessitat, segons l'autora, no tant en el sentit de ser l'última alternativa, sinó en el fet que les mesures adoptades siguin adequades o convenients per repel·lir l'atac armat[133]. El Manual Tallin 2.0 també sembla donar suport aquesta línia interpretativa[134].

D'acord amb Brownlie, la proporcionalitat és l'"essència" de la legítima defensa[135]. Respecte a aquest, el TIJ s'ha mostrat reticent en definir o oferir un anàlisi clar de les dimensions de la proporcionalitat en la legítima defensa[136].

En principi la proporcionalitat exigiria que el grau de força no excedís del raonablement necessari per posar fi a l'atac. És per això que es diu que necessitat i proporcionalitat són dues cares d'una mateixa moneda[137]. Autors com Dinstein, entenen el requisit com un equilibri o simetria entre l'agressió soferta i la resposta en legítima defensa, és a dir, que hi hagi una aproximació de la

[128] Dinstein, Y. (2005). *Op. cit*., p.210.
[129] Rafighdoust, H. (2018). *Op. cit*., p.150 i 151.
[130] Greenwood, C. (2011). *Op. cit*., p.8, para. 27.
[131] Rafighdoust, H. (2018). *Op. cit.*
[132] Cervell, M. J. (2017). *Op. cit*., p.137.
[133] *Ibid.*
[134] Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2a ed.). Cambridge University Press, p.348.
[135] Brownlie, I. (1963). *Op. cit*., p.389.
[136] Rafighdoust, H. (2018). *Op. cit*., p.161.
[137] Cervell, M. J. (2017). *Op. cit*., p.138.

gravetat (escala i efectes) d'ambdues forces[138]. Per altres, la proporcionalitat depèn de la finalitat, és a dir, de l'objectiu de defensar-se o repel·lir l'atac. De manera que, segons aquesta postura, no depèn de les armes utilitzades, sinó que la força utilitzada no excedís del que era necessari per repel·lir i defensar-se de l'atac armat[139]. En opinió personal, considero que la interpretació de la noció de la proporcionalitat més encertada i ajustada a Dret seria la segona. No obstant això, també crec que la proporcionalitat no obeeix a paràmetres estrictament definits o a criteris generals, sinó que la solució es trobarà en les circumstàncies concretes de cada cas particular.

[138] Dinstein, Y. (2005). *Op. cit*., p.237.
[139] Cervell, M. J. (2017). *Op. cit*., p.140.

CAPÍTOL 2

LA LEGÍTIMA DEFENSA CONTRA LES OPERACIONS CIBERNÈTIQUES PER PART DELS ESTATS I ACTORS NO ESTATALS

A. Conceptes i característiques d'operacions cibernètiques

Amb la creació d'internet, es va donar origen al que es coneix com el "ciberespai". Aquest és el "conjunt de sistemes d'informació interconnectats i crono-dependents, i els usuaris humans que interactuen amb aquests sistemes"[140]. Amb el desenvolupament tecnològic cada vegada es porten a terme més activitats variades, tant positives (educatives, comercials, de seguretat nacional, etc) com negatives (atacs en contra d'Estats, empreses, etc.)[141]. De fet, per alguna part de la doctrina ja el consideren com un espai més junt amb el terrestre, l'aeri, el marítim i els dos espais polars; al que resulta aplicable, per tant, l'ordenament jurídic internacional[142].

Aquesta revolució científica i tecnològica ha "canviat l'abast i el ritme de la batalla"[143]. Avui en dia, els ordinadors poden servir tant d'instrument de comandament, control, comunicacions i intel·ligència, però "l'ordinador modern també pot convertir-se en una arma en si mateixa al ser alienada per l'atac contra altres sistemes informàtics al servei de l'adversari"[144]. El ciberespai es converteix a la vegada en l'objectiu i el mitjà pel qual es realitza un atac[145].

A partir d'aquí se'ns planteja un primer problema, la terminologia. La doctrina utilitza diferents termes: operacions cibernètiques, operacions d'informació, atac cibernètic o ciberatac, atac a la xarxa informàtica (*computer network attack*), força cibernètica o guerra cibernètica[146]. No existeix un consens respecte a la terminologia o a definicions universalment o àmpliament acceptades en aquest àmbit.

L'únic acord internacional que s'aproxima a una definició dels atacs cibernètics és el Conveni sobre la Ciberdelinqüència de 23 de novembre de 2001. El Conveni exigeix als Estats signants

---

[140] Felipe, A., Serebrenik, S., Fernández, N. i Martínez-Vargas, J. R. (2019). *Robótica, Armas y Derecho Internacional*. Tirant lo Blanch, p.62. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788413135656

[141] *Ibid.*

[142] Cervell, M. J. (2017). *Op. cit*., p.296.

[143] Dinstein, Y. (2002). Computer Network Attacks and Self-Defense. *International law studies, 76*(20), 99-119, p.102. Disponible a: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1397&context=ils

[144] *Ibid.*

[145] Rafighdoust, H. (2018). *Op. cit*., p.202.

[146] *Ibid*., p.195.

que adoptin lleis que penalitzin el dany, eliminació, deteriorament, alteració o supressió de dades informàtiques sense dret, així com l'obstaculització greu i sense dret del funcionament d'un sistema informàtic (article 5). Tot i que el Conveni no arribar a regular del tot els atacs cibernètics, els seus intents per definir-los a escala internacional són de valorar.[147]

La falta de consens internacional sobre una definició d'atac cibernètic ha provocat que els Estats el defineixin atenen als seus interessos particulars. El Departament de Defensa dels Estats Units l'any 2011 va publicar la primera definició militar d'atac cibernètic:

> *"A hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyberattack are not necessarily limited to the targeted computer systems or data themselves-for instance, attacks on computer systems which are intended to degrade or destroy infrastructure of C2 capability. A cyberattack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyberattack may be widely separated temporally and geographically from the delivery"*[148].

Es tracta d'una definició restrictiva, basada en l'objectiu de l'atac (actes hostils amb la intenció de danyar un sistema cibernètic). Altres com l'Organització de Cooperació de Shanghai han optat per una interpretació més extensiva[149].

Roscini defineix un atac cibernètic com "un ús hostil de la força cibernètica, que podria ser un atac aïllat, el primer cop d'un conflicte armat, un atac en el context d'un conflicte armat ja iniciat, o una reacció contra un atac convencional o cibernètic previ"[150]. Aquesta definició, que es centra en els ordinadors i les xarxes informàtiques com a armes i no com a objectius, no cobreix atacs sintètics contra instal·lacions informàtiques, ciberespionatge o ciberpropaganda[151]. Segons el Manual Tallin un atac cibernètic és "una operació cibernètica, ja sigui ofensiva o defensiva, que raonablement s'espera que causi injúria o mort a persones, o danys o destrucció d'objectes"[152].

---

[147] Gervais, M. (2012). Cyber Attacks and the Laws of War. *Berkeley Journal of International Law, 40*, 525-579, p.532 i 533. https://doi.org/10.15779/Z38R66C

[148] US Department of Defense (DoD), Joint Terminology for Cyberspace Operation (2010), p.5. Visitat al 2 de març de 2023, de: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf

[149] Rafighdoust, H. (2018). *Op. cit*., p.198.

[150] Roscini, M. (2010). World Wide Warfare - *Jus Ad Bellum* and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, 14*, 85-130, p.96. https://ssrn.com/abstract=1683370

[151] *Ibid.*

[152] Schmitt, M. N. (2017). *Op. cit*., p.415.

Veiem doncs que els atacs cibernètics formen part d'una categoria més àmplia, les operacions cibernètiques. També cal dir que la noció d'atac cibernètic és més àmplia que la d'atac a la xarxa cibernètica o a la xarxa informàtica. Per altra banda, les operacions cibernètiques fa referència a tot un conjunt d'activitats al ciberespai per recol·lectar, exportar, destruir, canviar, xifrar dades o activar, alertar o manipular processos a través de la infiltració d'un sistema computacional[153]. De manera que es podrien definir com "la utilització de capacitats cibernètiques amb el propòsit principal d'aconseguir objectius al o mitjançant l'ús del ciberespai"[154]. Al seu torn, les operacions cibernètiques formen part d'una categoria més àmplia, les operacions d'informació (*information operations,* IO). Aquestes comprenen totes aquelles "accions empreses per afectar a la informació i sistemes d'informació de l'adversari"[155].

En aquest treball, per tant, considerem preferible utilitzar el terme d'operacions cibernètiques, ja que cobreix tot tipus d'activitat cibernètica que podria donar lloc a l'ús de la força en legítima defensa.

Finalment, les operacions cibernètiques tenen unes característiques úniques que les diferencien de qualsevol altra arma o àmbit. I tot i que hi ha diferents formes de descriure i categoritzar aquestes característiques, la doctrina sol utilitzar l'establerta per la professora Harrison Dinniss. En aquest sentit, s'identifiquen 4 carecterístiques de les operacions cibernètiques que les diferencien dels atacs convencionals en el marc de l'ús de la força: indirecta, intangible, el lloc (*locus*) i el resultat[156].

La indirecció és un factor distintiu i destacat, pel fet que diversos tipus d'operacions cibernètiques requereixen l'acció posterior d'un segon actor després de l'acte inicial. Per exemple, la inutilització de sistemes de control del tràfic aeri o l'atac contra un sistema de punteria d'un míssil[157].

La intangibilitat es refereix al fet que ni l'objectiu de l'atac ni l'arma utilitzada podrien existir en el món real. A més, el dany també pot no ser físic, per exemple, un cas d'atac a una borsa de valors. Inclús els atacs que acaben tenint conseqüències físiques tenen com a objectiu la

[153] Rafighdoust, H. (2018). *Op. cit*., p.200.
[154] Schmitt, M. N. (2017). *Op. cit*., p.15.
[155] Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law, 37*, 886-937, p.890. https://ssrn.com/abstract=1603800
[156] Kuru, H. (2017). Prohibition of use of force and cyber operations as "force". *Journal of Learning and Teaching in Digital Age, 2*(2), 46-53, p.48. https://dergipark.org.tr/en/pub/joltida/issue/55467/760088; també Rafighdoust, H. (2018). *Op. cit*., p.202.
[157] Kuru, H. (2017). *Ibid*.

informació resident en els ordinadors (*computer data*). Per exemple, el famós atac Stuxnet en modificar les freqüències de gir de les centrifugadores, va provocar danys físics a aquestes[158].

El factor *locus* té en compte el fet que, en alguns casos, pot ser difícil determinar l'origen de l'atac[159]. Doncs, el més probable és que l'atac es condueixi a través de diferents punts en diversos països amb la finalitat d'ocultar el veritable origen; per exemple a Estònia el 2007, el tràfic maliciós procedia de 178 països individuals[160]. Per tant, en l'àmbit de les operacions cibernètiques a part que poder ser llançades sense previ avís, l'anonimat també és una caracterísitca principal i molt important, el que significa que la identificació i l'atribució d'aquestes pot suposar un greu problema probatori[161].

El resultat de les operacions cibernètiques "inclouen una àmplia gamma de conseqüències que van des de les meres molèsties fins a la destrucció física"[162]. És aquesta indefinició i varietat dels resultats "el factor més difícil a l'hora de classificar les normes sobre l'ús de la força davant d'atacs cibernètics"[163]. A més, el resultat normalment serà més imprevisible que en el cas d'un atac sintètic i el lapse de temps transcorregut entre el llançament, l'operació en si, i el resultat, és realment curt en comparació a les altres[164].

A més, no podem passar per alt el fet que les operacions cibernètiques presenten importants avantatges respecte als atacs convencionals: relativament barat, la tecnologia necessària per portar-les a terme és fàcilment accessible i les eines molt variades (destrucció de xarxes, virus i cucs, bombes lògiques, *botnets*...). Per tant, els orígens del perill són molts, en constant evolució i innovació, i el dany pot resultar ser considerablement greu[165].

B. Operacions cibernètiques com a violacions del principi de la prohibició de l'ús de la força

Per a l'estudi que ens interessa, les operacions cibernètiques es poden classificar en tres categories: primer, les operacions que poden constituir una violació del principi de la prohibició

---

[158] *Ibid*.
[159] Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review, 56*, 569-606, p.570. https://ssrn.com/abstract=2184850
[160] Kuru, H. (2017). *Op. cit.*
[161] Rafighdoust, H. (2018). *Op. cit*., p.203.
[162] Kuru, H. (2017). *Op. cit*.
[163] *Ibid*.; també Moore, H., i Roberts, D. (2013, abril 23). *AP Twitter hack causes panic on Wall Street and sends dow plunging*. The Guardian. Visitat al 7 de març de 2023, de: https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall
[164] Rafighdoust, H. (2018). *Op. cit.*
[165] Cervell, M. J. (2017). *Op. cit*., p.292.

de l'ús de la força; segon, les operacions que poden considerar-se per sota del nivell d'usos de la força; i tercer, aquelles operacions cibernètiques que equivalen a un atac cibernètic en el sentit d'autoritzar l'exercici del dret a la legítima defensa. En aquest apartat, analitzarem les dues primeres categories.

1. Operacions cibernètiques com ús de la força

Aquesta classe d'armes han creat una nova forma de guerra que comporta reptes no només ètics, sinó també jurídics pels Estats i la comunitat internacional[166]. La primera, si les normes i principis de Dret Internacional existents són d'aplicació al ciberespai. Els instruments claus del *ius ad bellum* i del *ius in bello* del Dret Internacional són els Convenis de La Haia de 1899 i 1907, la Carta de les Nacions Unides de 1945, i els quatre Convenis de Ginebra sobre la protecció de les víctimes de guerra de 1949 i els seus dos Protocols de 1977, però cap d'ells fa referència a la qüestió cibernètica[167]. En aquest sentit, l'Opinió Consultiva del TIJ sobre el Sud-oest Africà, ja declarava que "un instrument internacional s'ha d'interpretar i aplicar en el marc de tot l'ordenament jurídic vigent al moment de la interpretació"[168]. Aquesta interpretació dinàmica també la trobem implícita en el text de l'article 3(b) del Conveni de Viena 1969[169]. I finalment, dues referències principals pel que fa a la regulació jurídica de la ciberguerra com són: la declaració de Harold Koh (exassessor jurídic del Departament d'Estat dels Estats Units) i el Manual Tallin; coincideixen a dir que tot i no haver tractats específics sobre la matèria, els principis generals del Dret Internacional són aplicables al ciberespai[170].

No obstant això, la potencial aplicació de l'article 2(4) a les operacions cibernètiques crea dificultats interpretatives sobretot respecte a la distinció de força i coacció. Com dèiem en apartats anteriors, és possible acceptar l'aplicació de la prohibició a força física distinta de l'armada o militar, però no, per tant, aquelles que no causen un dany físic. Això vol dir que és necessària una definició més extensiva de l'article 2(4) per donar cabuda a totes les operacions cibernètiques en l'àmbit d'aplicació de la prohibició, ja que el Dret Internacional tradicional no semblaria incloure

[166] Felipe, A., *et altr*. (2019). *Op. cit*., p.225.
[167] Rafighdoust, H. (2018). *Op. cit*., p.207.
[168] Advisory Opinion ICJ, Legal Consequences for States of the Contitiued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), I. C.J. Reports 1971, p.31, para. 53.
[169] Rafighdoust, H. (2018). *Op. cit*., p.208.
[170] Cervell, M. J. (2017). *Op. cit*., p.297.

tots aquells atacs cibernètics que no causin un dany físic, com pot ser una incursió electrònica i bloquejos, els quals actualment serien equivalents a actes de coacció econòmica i política[171].

Tres enfocaments són els acceptats per determinar si una operació cibernètica pot violar el principi de prohibició d'ús de la força: *instrument-based approach, targed-based approach* i *effect-based approach*[172]. Si ens hi fixem bé, al parlar del concepte de força ja hi hem fet referència. Doncs l'enfocament basat en els mitjans (*instrument-based approach*), es centra únicament en l'ús d'armes militars. De manera que, segons aquest criteri encara que un atac cibernètic causi danys físics mai podrà considerar-se un ús de la força d'acord amb l'article 2(4). Aquesta aproximació resulta antiquada i inadequada per les raons que ja s'han comentat.

L'enfocament basat en l'objectiu (*targed-based approach*) és una extensió de l'ús de la força, ja que aquest rebaixa el llindar d'ús de la força i augmenta el risc de respondre inclús a agressions menors[173]. Aquest enfocament, i com argumenta Sharp, qualsevol operació cibernètica contra una Infraestructura Nacional Crítica (*National Critical Infrastructure*, NCI) violaria l'article 2(4) de la Carta[174]. Aquest punt de vista resulta sobre inclusiu, la prohibició també cobriria les operacions que causen únicament inconveniències o les que simplement pretenen recavar informació d'una NCI[175]. De fet, segons aquest enfocament si la naturalesa de la informació robada o compromesa és considerada vital per la seguretat nacional (per exemple informació "classificada" relacionada amb codis d'armes nuclears, posició de tropes en un conflicte armat, etc.), tals accions podrien considerar-se equivalents a atacs armats "encara que no es produeixi pèrdues de vides humanes de forma immediata o destrucció"[176]. Un altre problema d'aquest enfocament és que no sembla haver-hi una definició generalment acceptada de NCI.

[171] Barkham, J. (2001). Information warfare and International Law on the use of force. *New York University Journal of International Law and Politics, 34*, 57-97, p.84 i 85. https://universityofleeds.github.io/philtaylorpapers/pmt/exhibits/523/barkham.pdf

[172] Roscini, M. (2014). *Cyber operations and the Use of Force in International Law*. OUP Oxford, p.46; també Kuru, H. (2017). *Op. cit*., p.48.

[173] Kuru, H. (2017). *Ibid*., p.50.

[174] Sharp, W. G. (1999). *Cyberspace and the use of force*. Aegis Research Corporation, p.129-132.

[175] Rafighdoust, H. (2018). *Op. cit*., p.212.

[176] Joyner, C. C. i Lotrionte C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825–865, p.855. https://doi.org/10.1093/ejil/12.5.825

L'enfocament basat en l'escala i els efectes o gravetat (*effect-based approach*) és el predominant entre la doctrina[177], el que ja han començat a adoptar alguns Estats[178], i probablement el més fàcil d'aplicar[179]. Respecte a aquest, sense repetir el que ja s'ha dit, els atacs cibernètics poden constituir una violació de l'article 2(4) quan els efectes que causen són comparables als d'operacions no cibernètiques suficients per vulnerar el principi. De manera que totes les operacions cibernètiques amb anàlogues conseqüències o efectes que qualsevol altre acte sintètic o no sintètic seran considerades usos de força. De fet, el sentit comú ens assenyala que si una operació cibernètica causa els mateixos efectes que deixar caure una bomba o llançar un míssil, aquestes també haurien de ser considerades com a usos de la força[180].

En el marc d'aquest enfocament apareix el reconegut Manual Tallin. El Grup d'Experts encarregat de la seva redacció, consideren els efectes que es produeixen i certs aspectes qualitatius de les operacions cibernètiques com a elements útils per indicar alguns criteris jurídicament informals per tal d'identificar les operacions cibernètiques com a usos de força. Aquests criteris són: gravetat, immediatesa, vincle directe entre acte i resultat, intromissió, capacitat de mesurament dels efectes, caràcter militar, implicació estatal i la presumpta legalitat de l'acció[181].

La gravetat, com dèiem, és evidentment el factor més important de l'anàlisi. I, per tant, els actes que lesionen o maten a persones o causen danys físics o destrueixen objectes són inequívocament usos de força[182]. El Manual també expressa clarament que els criteris presentats pretenen ser factors que influeixen en l'avaluació de l'ús de la força per part dels Estats i no criteris jurídics vinculants. A més, aquests no són exhaustius i en tot cas dependrà de les circumstàncies concretes del cas i de què els factors actuïn conjuntament[183]. Per exemple, és possible que un Estat acudeixi a altres criteris com l'objectiu de l'atac (infraestructura crítica).

Autors com Roscini, classifiquen els efectes que produeixen les operacions cibernètiques en tres tipologies: els efectes primaris (*primary effects*) que són els que es produirien al sistema,

[177] Silver, D. B. (2002). Computer network attack as a use of force under article 2(4) of the United Nations Charter. Dins Schmitt, M. N. i O'Donnell, B. T. (ed.), *Computer network attack and International Law* (74-97), p.81 i 82. https://digital-commons.usnwc.edu/ils/vol76/iss1/21/; Waxman, M. C. (2011). Cyber Attacks as 'Force' Under UN Charter Article 2(4). *International Law Studies*, *87*(1), 43-57, p. 52 i 53. https://scholarship.law.columbia.edu/faculty_scholarship/847; Cervell, M. J. (2017). *Op. cit*., p.297; Rafighdoust, H. (2018). *Op. cit*., p.213; Schmitt, M. N. (2011). *Op. cit*., p.588; etc.

[178] Per exemple US National Research Council (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyber attack capabilities*. National Academies Press, p.33 i 34.

[179] Kuru, H. (2017). *Op. cit*., p.48.

[180] Rafighdoust, H. (2018). *Op. cit*., p.214.

[181] Schmitt, M. N. (2017). *Op. cit*., p.334-336.

[182] *Ibid*., p.334.

[183] *Ibid*., p.337.

ordinador o xarxa atacats; els efectes secundaris (*secundary effects*) que es produeixen en les infraestructures operades pel sistema o xarxa atacada; i els efectes terciaris (*tertiary effects*) que serien els que es produeixen sobre les persones afectades per la destrucció o incapacitació del sistema atacat o infraestructura[184].

2. Operacions cibernètiques per sota del nivell de la prohibició de l'ús de la força

Com bé dèiem en l'apartat de l'ús de la força, la coacció econòmica i política no estaria inclosa en l'àmbit d'aplicació del principi de prohibició de l'ús de la força per les raons que s'han aportat. Això vol dir, que les operacions cibernètiques anàlogues a coaccions polítiques o econòmiques tampoc podran ser considerades com a ús de la força[185], per tant, per sota del nivell o llindar exigit per la prohibició. No obstant això, el problema de l'*effect-based approach* és que difuminaria la distinció que exclou la coacció económica o política de l'ús de la força tradicional, per exemple en els casos en què una coacció econòmica (normalment per llargs períodes de temps) produeixi danys físics[186].

Com ja s'ha fet referència i seguint la Resolució 2131 (XX), encara que la coacció política o econòmica o de qualsevol altra índole no vulnerin el principi de prohibició de l'ús de la força, no vol dir que no ho facin respecte al principi de no intervenció[187]. El llenguatge de la Resolució resulta prou ampli per entendre que s'inclouen aquelles operacions cibernètiques que es troben per sota del nivell de l'ús de la força, com per exemple les que no afectin una infraestructura crítica d'un altre Estat.

En aquest sentit, seguint el disposat pel Manual Tallin "les operacions psicològiques cibernètiques no destructives destinades únicament a soscavar la confiança en un govern o en una economia no es consideraran usos de la força"[188]. No obstant això, alguns Estats "poden classificar les operacions cibernètiques massives que paralitzen una economia com ús de la força, encara que la coacció econòmica sigui presumptament lícita"[189].

A més, en el cas de Nicaragua, com anteriorment també comentàvem, el mer subministrament de fons als contres no constitueix un ús de la força, tot i ser contrari al principi de no intervenció. De

[184] Roscini, M. (2014). *Op. cit*., p.52 i 53.
[185] Schmitt, M. N. (2017). *Op. cit*., p.331.
[186] Barkham, J. (2001). *Op. cit*., p.86.
[187] Resolució AGNU 2131 (XX) "Declaració sobre la inadmissibilitat de la intervenció en els assumptes interns dels Estats i protecció de la seva independència i sobirania", de 21 de desembre de 1965, p.13.
[188] Schmitt, M. N. (2017). *Op. cit*., p.331, para. 3.
[189] *Ibid*., p.337, para. 10.

manera que, el finançament de "hacktivistes" (*hacktivist*), és a dir, d'actors no estatals per efectuar operacions cibernètiques tampoc constituiria un ús de la força[190].

Finalment, considero important fer una menció a la difusió d'informació i propaganda, així com a les explotacions cibernètiques (*cyber exploitation*). Respecte a les primeres la difusió deliberadament falsa i destinada a produir dissensió o a animar als insurgents, és molt probable que no arribi al nivell d'ús de la força i, per tant, constitueixi una vulneració del principi de no intervenció[191]. Pel que fa a les segones, es tracten d'un tipus d'operació cibernètica consistents en "l'accés no autoritzat a un ordinador, sistmes informàtics i a les xarxes per extreure informació, però sense afectar a la funcionalitat del sistema accedit o corrompent, modificant o suprimint les dades residents en ella"[192]. Es poc probable que aquestes siguin considerades com a usos de la força bàsicament perquè és una nova forma d'espionatge contemporani, no prohibit pel Dret Internacional[193].

C. Operacions cibernètiques com un atac armat en el context del dret a legítima defensa

1. Operacions cibernètiques com atacs armats per Estats

Ja hem vist que una operació cibernètica pot constituir un ús de la força, però recordem que segons els criteris tradicionals perquè es pugui considerar un atac armat, a més a més, haurà de ser de tal entitat que pugui merèixer aquesta qualificació[194].

Recordem, com ja hem dit anteriorment, que el Dret Internacional no defineix el terme "atac armat", i que l'instrument en el qual ens recolzàvem per identificar un atac armat era la Resolució 3314 (XXIX). Aquesta no defineix el terme, però si ens aporta exemples d'accions que poden ser considerades atacs armats. En aquest sentit, l'article 3(b), que es refereix a "l'ús de qualsevol arma per un Estat contra el territori d'un altre Estat"[195], per la terminologia usada, ja sembla suficient per incloure també els atacs cibernètics[196].

[190] *Ibid*., p.331, para. 3.
[191] Jamnejad, M., i Wood, M. (2009). The principle of non-intervention. *Leiden Journal of International Law, 22*(2), 345-381, p.374. https://doi.org/10.1017/S0922156509005858
[192] Roscini, M. (2014). *Op. cit*., p.65.
[193] *Ibid*., p.66; també Schmitt, M. N. (2017). *Op. cit*., p.170, para. 6.
[194] Cervell, M. J. (2017). *Op. cit*., p.300.
[195] Resolució AGNU 3314 (XXIX), *op. cit.*
[196] Roscini, M. (2014). *Op. cit*., p.72.

També, dèiem que el TIJ hauria reconegut que el terme d'agressió és més ampli que el d'atac armat[197] i que l'article 51 no es refereix a armes específiques i s'aplica a qualsevol atac armat, "independentment de l'arma utilitzada"[198].

Així mateix, la comunitat internacional generalment accepta el *Pictet's scope, duration and intesity test* com a punt de partida per avaluar si un ús de la força constitueix un atac armat. Segons aquest, un ús de la força es pot considerar atac armat quan sigui d'abast, duració i intensitat suficients[199]. No obstant això, de la mateixa manera que molts altres conceptes jurídics internacionals, els Estats, organitzacions internacionals, i autors han interpretat l'abast, la duració i la intensitat de formes molt diferents[200].

De manera que des d'una perspectiva legal, d'acord amb un enfocament basat en els efectes o conseqüències (*effect-based approach*), com hem sostingut fins ara, no sembla haver-hi una raó per diferenciar entre els mitjans d'atac sintètics o electrònics. Un *CNA* destructiu premeditat pot qualificar-se com un atac armat tant com pot un atac sintètic que produeixi el resultat d'un atac armat[201]. La legítima defensa, en resum, podria exercir-se per aquell Estat que hagi patit un atac cibernètic les conseqüències del qual siguin equiparables a les d'un atac armat en el sentit tradicional del terme (escala, efectes) i que causi morts i danys materials[202].

Aquesta punt de vista és recolzat implícitament per les Resolucions 1368 i 1373 de 2001, ja que en aquestes es defensa l'exercici del dret a legítima defensa en resposta dels avions segrestats de l'11S[203]. I també recolzat explícitament pel Manual Tallin quan diu que "Un Estat que és un objectiu d'un atac cibernètic que s'eleva al nivell d'un atac armat pot exercir el seu dret inherent de legítima defensa"[204]. Alguns Estats com els Estats Units, Regne Unit, Rússia i Alemanya també s'han manifestat a favor de considerar que les operacions cibernètiques poden ser qualificades d'atacs armats; així com el Grup d'Experts de les Nacions Unides i l'OTAN[205].

---

[197] Sentència TIJ (Nicaragua v. Estats Units d'Amèrica), *op. cit*., p.103 i 104, para. 195.
[198] Advisory Opinion ICJ, Legality of the Threat or Use of Nuclear Weapon, I. C.J. Reports 1996, p.244, para. 39.
[199] Carr, J. (2009). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media, p.58.
[200] *Ibid*.
[201] Dinstein, Y. (2002). *Op. cit*., p.103.
[202] Cervell, M. J. (2017). *Op. cit*., p.302.
[203] Resolució CSNU 1368, relativa a les amenaces a la pau i la seguretat internacionals creades per actes de terrorisme, de 12 de setembre de 2001, p.1; Resolució CSNU 1373, relativa a les amenaces a la pau i la seguretat internacionals creades per actes de terrorisme, de 28 de setembre de 2001, p.1; i Rafighdoust, H. (2018). *Op. cit*., p.229.
[204] Schmitt, M. N. (2017). *Op. cit*., p.339.
[205] Rafighdoust, H. (2018). *Op. cit*., p.229 a 232.

També és necessari recordar, que no tots els autors estarien d'acord amb aquest enfocament. Alguns més partidaris d'un enfocament basat en l'instrument o el mitjà, entre altres arguments, mantindrien que traslladar les normes existents del *ius ad bellum* a les activitats cibernètiques produiria una extensiva incertesa, ja que una operació cibernètica manca de les tradicionals característiques físiques associades a la coerció militar[206]. En opinió personal, considero que si bé no hem arribat al moment en què els atacs cibernètics arribin al nivell mínim per ser considerats atacs armats, per exemple per no causar morts o danys significants a béns; no vol dir que en un futur més pròxim que llunyà, puguin aconseguir-ho. I per això, tot i la incertesa de l'aplicació de l'actual Dret Internacional, els Estats destinataris d'atacs cibernètics haurien de poder respondre en legítima defensa si aquests atacs arriben al nivell d'un atac armat.

Finalment, considero important tractar la qüestió respecte a la possibilitat d'exercir el dret de legítima defensa per víctimes accidentals (sense intenció) d'operacions cibernètiques. Doncs, per les qualitats o característiques d'aquestes últimes és relativament senzill que puguin afectar a víctimes no previstes abans de portar-les a terme. Com comentàvem anteriorment, el TIJ en el cas concernent a les Plataformes Petrolíferes ja va declarar que un atac armat havia de portar-se a terme amb "l'específica intenció de danyar (*with the specific intention of harming*)"[207]. No obstant això, la "intenció" sempre ha sigut objecte de debat.

La majoria d'experts del Manual Tallin creuen que "la intenció és irrellevant a l'hora de qualificar una operació d'atac armat i només importa l'escala i efectes"[208]. Això significaria que un atac cibernètic de l'Estat A a un Estat B amb efectes desbordants (amb suficient escala i efectes per ser considerats atac armat) a un Estat C, aquest últim té dret a recórrer a l'ús de la força en legítima defensa; sempre que la resposta, evidentment, sigui ajustada als criteris de necessitat i proporcionalitat[209].

Tot i això, alguns experts del Manual Tallin sí que creuen necessari considerar la intenció com a criteri per qualificar una operació cibernètica d'atac armat. Altres autors també es mostren a favor d'aquesta idea. Roscini ens diu que "una reacció en legítima defensa de l'Estat C no seria necessària, ja que l'Estat A probablement aturarà l'atac a C"[210], per tant, la intencionalitat és un element a tenir en compte. En aquest mateix sentit també es pronuncia Sharp[211]. En opinió personal, considero que és necessària una intenció hostil com a criteri per qualificar una operació

[206] *Ibid*., p.232.
[207] Sentència TIJ (República Islàmica d'Iran v. Estats Units), *op. cit*., p.192, para. 64.
[208] Schmitt, M. N. (2017). *Op. cit*., p.57, para. 11.
[209] *Ibid*., para. 12.
[210] Roscini, M. (2014). *Op. cit*., p.77.
[211] Sharp, W. G. (1999). *Op. cit*., p.132 i 133.

cibernètica d'atac armat; donat que em sembla el raonament més lògic i ajustat amb l'article 1(1) de la Carta. En aquests casos, l'Estat indirectament afectat (sense intenció de l'Estat atacant) podria optar per altres mecanismes més adients com contramesures o qualsevol altra mesura de resposta que no equivalgui a un ús de la força ni violi un tractat existent o una obligació de dret consuetudinari; per exemple, un bloqueig de les transmissions cibernètiques entrants procedents de l'Estat que ha fet ús de la força contra ell[212].

a) Acumulació d'operacions cibernètiques menors

En primer lloc, hem vist durant el llarg d'aquestes pàgines que el criteri per determinar les accions considerades com atac armat de les que no ho poden ser, era el de l'"escala i efectes". Però els paràmetres d'aquest criteri segueixen sense resoldre's més enllà de la indicació que han de ser "greus"[213] o d'utilitzar el *Pictet's test*. I per això dèiem, que en el cas de les operacions cibernètiques que produeixin danys materials, destruccions considerables de béns o víctimes humanes satisfarien el requisit d'escala i efectes. Tot i així, avui en dia, tampoc és clar l'abast d'aquests resultats perquè l'operació cibernètica pugui considerar-se un atac armat. A més a més, segons el grup d'experts, per avaluar-ho s'haurien de tenir en compte totes les conseqüències raonablement previsibles de l'operació cibernètica[214]. No obstant això, el cas d'aquelles que no tinguin aquests resultats, però que tinguin uns efectes negatius extensos, segueix també sense resoldre's[215]. Com dèiem abans, segons el Dret Internacional tradicional i per l'absència de pràctica estatal al respecte, resulta difícil que una operació cibernètica que no causi danys físics pugui tenir tal consideració. Però, futurs successos poden determinar l'evolució del dret actual en direccions inesperades i no podem passar per alt altres arguments a tenir en compte; com per exemple, que "l'operació cibernètica dirigida contra una infraestructura crítica d'un Estat que causi efectes greus, encara que no destructius, es consideraria un atac armat"[216]. De fet, aquest últim, ja sembla acceptar-se per bona part de la doctrina tal com exposarem en el següent apartat.

En segon lloc, els actes que finalment no arribessin al llindar d'atac armat, quan hi ha una estratègia subjacent darrere d'aquests atacs de baix nivell i els seus efectes cumulatius són considerables, arribem a una conclusió diferent[217]. En aquest sentit, és àmpliament acceptat que el factor determinant seria si l'originador (o originadors si actuen en conjunt) ha portat a terme aquests incidents o atacs de menor escala relacionats entre si i que en conjunt compleixen el

[212] Schmitt, M. N. (2011). *Op. cit*., p.581.
[213] Schmitt, M. N. (2017). *Op. cit*., p.341, para. 7.
[214] *Ibid*., p.343, para. 13.
[215] *Ibid*., p.342 i 343, para. 12.
[216] *Ibid*.
[217] Rafighdoust, H. (2018). *Op. cit*., p.238.

requisit d'escala i efectes; si hi ha proves suficients de què això és així, hi hauria motius suficients per tractar aquests incidents com un atac armat compost[218]. Evidentment, si aquests atacs cibernètics menors són components d'una operació militar global, de força armada militar, no cal que siguin considerats individualment o en el seu conjunt per saber si l'Estat pot reaccionar en legítima defensa, aquest últim podrà fer-ho mentre formin part d'un atac armat tradicional[219]. Per tant, un atac armat pot portar-se a terme de diverses maneres, des d'una invasió a gran escala fins a una sèrie d'usos de la força a petita escala a la mateixa ofensiva contra el mateix objectiu[220].

Finalment, hem de tenir en compte que en el cas d'acceptar la legítima defensa en aquests casos que hem comentat, sobretot en els primers en què no es produeix un dany físic, s'haurien d'establir límits. Per exemple, conseqüències merament financeres o de descontrol de grans infraestructures d'un Estat, en aquests casos la legítima defensa s'hauria d'ajustar més que mai a la proporcionalitat i operar, per tant, en el mateix "terreny intangible" en què s'ha desencadenat l'atac cibernètic, sense que sigui possible una resposta armada contra ell[221].

b) Objectiu de l'atac

Quan parlem que ha d'existir un atac armat contra un Estat perquè pugui exercir el seu dret a legítima defensa, sorgeix la qüestió de què hem de considerar com a "Estat". No hi ha dubte que un atac armat contra el territori d'un Estat és efectivament un atac armat contra aquest; també és generalment acceptat que ho sigui quan es produeix contra òrgans de l'Estat fora del seu territori[222]. Més dubtes plantegen altres figures, que el TIJ ha tingut l'oportunitat de pronunciar-se sobre alguna d'elles, com vaixells comercials privats o nacionals d'un Estat fora del seu territori. No obstant això, no seran analitzades per escapar-se de l'objecte d'aquest treball.

En aquest sentit, autors com Sharp consideren que "qualsevol atac a una xarxa informàtica (comès per un Estat) que causi intencionadament qualsevol efecte destructiu al territori sobirà d'un altre Estat és un ús il·legal de la força que pot constituir un atac armat que doni lloc al dret de legítima defensa"[223]. En opinió personal, considero que és difícil acceptar aquesta posició, ja que de moment els atacs cibernètics no estan capacitats per produir efectes destructius com els que pot causar un atac militar tradicional; per això serà necessari un objectiu més fràgil o problemàtic, que com a resultat de la seva afectació pugui produir uns efectes similars.

[218] Schmitt, M. N. (2017). *Op. cit*., p.342, para. 11.
[219] Schmitt, M. N. (2011). *Op. cit*., p.588.
[220] Rafighdoust, H. (2018). *Op. cit*., p.239.
[221] Cervell, M. J. (2017). *Op. cit*., p.303.
[222] Greenwood, C. (2011). *Op. cit*., p.7, para. 20 i 21.
[223] Sharp, W. G. (1999). *Op. cit*., p.133.

En aquest sentit, Roscini, considera que les operacions cibernètiques que causin danys físics de suficient gravetat a infraestructures crítiques o pertorbin greument el seu funcionament o la incapacitin, poden constituir potencialment un atac armat i permetre exercir el dret a legítima defensa[224]. I aquí és quan entra en joc el *Pictet's test* per avaluar la gravetat de les conseqüències.

D'acord amb Dinstein "la interrupció de les comunicacions i els serveis digitalitzats per error induït dels sistemes informàtics, sense causar víctimes humanes ni destrucció significativa de béns" és un atac cibernètic, "però com que l'acte no comporta conseqüències prou greus", no pot constituir un atac armat[225]. No obstant això, continua dient que "morts causades per la pèrdua de sistemes de manteniment de la vida controlats per ordinadors; un tall generalitzat de la xarxa elèctrica (apagada) amb repercussions perjudicials considerables; una apagada dels ordinadors que controlen les obres hidràuliques i les preses, amb les conseqüents inundacions de zones habitades; accidents mortals provocats deliberadament (per exemple, mitjançant informació errònia als ordinadors dels avions), etc.", es consideraria un atac armat[226]. Per tant, es podria acceptar que aquelles operacions cibernètiques en infraestructures crítiques d'un Estat que pertorbin/alterin massivament han de considerar-se un atac armat, encara que no causin lesions humanes o danys materials immediats[227].

No obstant, pel que fa al concepte d'infraestructures crítiques, no sembla haver-hi acceptació general respecte quin tipus d'infraestructures són crítiques. De fet, la Resolució de l'AGNU 58/199 reconeix que "cada Estat determinarà les seves pròpies infraestructures crítiques d'informació"[228].

c) Autoria dels atacs cibernètics

En aquest apartat es plantegen 3 qüestions importants: la problemàtica de l'atribució d'operacions cibernètiques a un Estat; el criteri del Dret Internacional per a l'atribució directa d'aquests atacs als Estats; i el criteri d'atribució indirecte als Estats d'atacs realitzats per actors no estatals.

Un dels majors problemes per a l'ús del dret a legítima defensa contra un atac cibernètic és el consistent en atribuir o determinar d'on procedia l'atac i qui estava involucrat en ell[229]. I això és degut principalment a tres característiques del ciberespai que fan extremadament difícil atribuir

[224] Roscini, M. (2014). *Op. cit.*, p.77.
[225] Dinstein, Y. (2002). *Op. cit.*, p.105.
[226] *Ibid.*
[227] Rafighdoust, H. (2018). *Op. cit.*, p.242.
[228] Resolució AGNU 58/199 "Creació d'una cultura mundial de seguretat cibernètica i protecció de les infraestructures dinformació essencials", 23 de desembre de 2003, p.1.
[229] Rafighdoust, H. (2018). *Op. cit.*, p.253.

una operació cibernètica a un Estat: i) anonimat, ii) les diverses fases dels atacs cibernètics (*multi-stage cyber attacks*), i iii) la velocitat en què un atac cibernètic pot ser materialitzat[230].

I tot i que la ciència està desenvolupant contínuament mecanismes d'atribució que poden rastrejar la màquina que va llançar l'atac, o la seva geolocalització, alhora, també s'estan desenvolupant mecanismes d'"antiatribució" que poden amagar la procedència de l'atac[231]. A més, el fet que avui en dia els atacs cibernètics puguin ser llançats fins i tot més fàcilment per individus o per grups, fa que la identificació de l'atacant mai pugui ser definitiva. Per tant, "encara que es pugui identificar als autors, pot ser difícil determinar en nom de qui actuen"[232].

En aquest sentit, haurien d'aplicar-se les normes generals de la responsabilitat dels Estats, per més que apareguin problemes afegits[233]. Així també ho va entendre el Grup d'Experts del Manual Tallin[234]. De manera que, li seran atribuïbles a l'Estat els fets o omissions dels seus òrgans, el que en aquest cas inclouria qualsevol activitat portada a terme per agències estatals d'intel·ligència militar, seguretat interna, duanes o qualsevol altre (*de jure organs*); així com la que emani de persones que no siguin òrgans de l'Estat, però que estiguin revestides d'autoritat governamental[235] (*de facto organs*). I els atacs cibernètics que emanin d'un particular només seran atribuïbles a l'Estat, com ja sabem, si són instruïdes, dirigides, controlades per aquest[236] (*de facto organs*). Per tant, en general, per atribuir un atac armat a un Estat tindríem aquestes dos principals situacions.

Pel que fa a la primera (*de jure organs*), l'Estat víctima pot legítimament emprendre accions en legítima defensa només si es compleixen les normes d'atribució del Dret Internacional als òrgans *de jure* d'un Estat[237]. D'acord amb l'article 4 del Projecte d'articles sobre la Responsabilitat de l'Estat per fets il·lícits internacionals, hem d'entendre el concepte "*de jure organs*" de forma àmplia. No es limita als òrgans del govern central i s'estén als òrgans de govern de qualsevol tipus o classificació, que exerceixin qualsevol funció i qualsevol nivell jeràrquic, inclosos els provincials i fins i tot els locals[238]. Així mateix, ho entén el Manual Tallin[239]. De manera que, si un òrgan *de jure* d'un Estat comet un atac cibernètic, l'atac s'atribuirà a l'Estat que es convertirà

[230] Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244, p.233. https://ssrn.com/abstract=2538271
[231] *Ibid*., p.234.
[232] Waxman, M. C. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of international Law*, *36*(2), 421-459, p.444. http://hdl.handle.net/20.500.13051/6629
[233] Cervell, M. J. (2017). *Op. cit*., p.305.
[234] Schmitt, M. N. (2017). *Op. cit*., p.84.
[235] Cervell, M. J. (2017). *Op. cit*., p.306.
[236] *Ibid.*
[237] Tsagourias, N. (2012). *Op. cit*., p.236.
[238] Document A/56/10 CDI, *op. cit*., p.41.
[239] Schmitt, M. N. (2017). *Op. cit*., p.87.

llavors en l'objectiu legítim de la resposta en legítima defensa[240]. A més, hem de destacar que recentment molts Estats ja han creat ciberunitats per portar a terme operacions cibernètiques; per exemple, en el cas d'Espanya el Centro Criptológico Nacional – *Computer Emergency Response Team* (CCN-CERT)[241].

No obstant això, per recórrer al dret a legítima defensa contra un altre Estat, l'Estat víctima ha d'aportar les proves adequades que demostrin l'atac armat a aquest Estat[242]. En l'àmbit de l'atribució o l'autoria, la prova és definida com "la necessària per provar tant els elements objectius (sigui una acció o una omissió) com subjectius d'un fet internacionalment il·lícit"[243]. El Dret Internacional no estableix un estàndard de prova específic o normes probatòries al respecte[244]. En aquest sentit, el TIJ en el cas de Nicaragua va declarar que "dins dels límits del seu Estatut i Reglament, té llibertat per estimar el valor dels diversos elements de prova"[245]; i en altres casos s'ha referit a "proves concloents" (*conclusive evidence*) o "a cert grau de certesa" (*a degree of certainty*)[246]. Per tant, tal com afirma Schmitt, per exercir el dret a legítima defensa, semblen ser necessàries "proves clares o convincents"[247], ja que en tractar-se d'una excepció a la prohibició d'ús de la força, l'estàndard de prova ha de ser suficientment alt per limitar i prevenir l'abús d'aquest dret[248]. Per exemple, el mer fet que una operació cibernètica hagi estat llançada des d'una infraestructura governamental normalment seria prova insuficient per atribuir l'operació a aquest Estat[249].

Pel que fa a la segona (*de facto organs*), d'acord amb la CDI:

> Com a principi general, el comportament de persones o entitats privades no és imputable a l'Estat en virtut del dret internacional. No obstant això, es poden donar circumstàncies en què aquesta conducta sigui atribuïble a l'Estat perquè hi hagi una relació de fet específica entre la persona o l'entitat que la realitza i l'Estat[250].

---

[240] Tsagourias, N. (2012). *Op. cit.*
[241] Rafighdoust, H. (2018). *Op. cit.*, p.259.
[242] *Ibid.*
[243] Roscini, M. (2014). *Op. cit.*, p.97 i 98.
[244] Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. Dins National Research Council (ed.), *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (151 a 178), p.168. https://doi.org/10.17226/12997.
[245] Sentència TIJ (Nicaragua v. Estats Units d'Amèrica), *op. cit.*, p.40, para. 60.
[246] Rafighdoust, H. (2018). *Op. cit.*, p.260.
[247] Schmitt, M. N. (2010). *Op. cit.*
[248] Roscini, M. (2014). *Op. cit.*, p.99.
[249] Schmitt, M. N. (2017). *Op. cit.*, p.91, para. 13.
[250] Document A/56/10 CDI, *op. cit.*, p.47.

Segons la CDI, *de facto organs*, són, per una banda, entitats facultades per les autoritats d'un Estat que s'assimilen o que són absorbides per l'aparell estatal (article 5) i, per altra banda, inclou aquelles entitats que actuen sota les instruccions, direcció o control d'un Estat (article 8).

Respecte a les primeres, són empreses o individus que no es poden qualificar d'òrgans de l'Estat per la seva pròpia naturalesa, però estan facultades pel dret intern (per exemple, per la llei, actes administratius, o, si el dret intern ho permet, per contracte) per realitzar elements de l'autoritat governamental[251]. És a dir, estarien revestides de poder estatal (*iure imperii*) per actuar en aquesta instància concreta i, per tant, serà atribuïble a l'Estat.

Respecte a les segones, serà atribuïble segons l'article 8 del Projecte d'articles quan l'atac cibernètic que emani d'un particular o entitat privada s'hagi realitzat sota les instruccions, la direcció o el control de l'Estat[252], i aquesta norma és especialment rellevant en el context cibernètic, en què els Estats solen encarregar aquestes operacions a empreses que s'ocupen d'això o a individus[253]. Aquest enfocament, es troba implícit, com ja hem comentat anteriorment al parlar de l'ús de força indirecta, en el raonament expressat pel TIJ en el cas de Nicaragua; en què l'atac armat d'actors no estatals podria ser atribuïble a un Estat que hi estigués involucrat. No obstant, en aquest context, el Grup d'Experts del Manual Tallin debatia respecte a l'existència de les dues tendències en l'atribució d'aquestes conductes: la del control general i la del control efectiu; per decantar-se finalment per aquesta última que, com hem dit, és també la posició sostinguda pel TIJ[254]:

> Aquesta conducta només serà atribuïble a l'Estat si aquest va dirigir o va controlar l'operació específica i la conducta denunciada en formava part integrant. El principi no s'aplica als comportaments associats de manera incidental o perifèrica a una operació i que escapen a la direcció o control de l'Estat[255].

Per tant, sense entrar amb detall respecte al concepte de "control efectiu", ja que s'escapa de l'objecte d'aquest treball, hem d'entendre que aquest control efectiu pressuposa que l'Estat sigui qui determina l'execució i el curs de l'operació; així com, la capacitat de fer que es produeixin les activitats constitutives de l'operació, com la capacitat d'ordenar el cessament de les que estan en curs[256]. Aquestes situacions, per tant, han de ser distingides dels casos en què individus privats, en la seva pròpia iniciativa, porten a terme operacions cibernètiques, com per exemple *hacktivists*

[251] Schmitt, M. N. (2017). *Op. cit*., p.89, para. 8.
[252] *Ibid.*
[253] Cervell, M. J. (2017). *Op. cit*., p.306.
[254] *Ibid.*
[255] Document A/56/10 CDI, *op. cit.*
[256] Schmitt, M. N. (2017). *Op. cit*., p.96, para. 6.

o *patriotic hackers*, ja que el mer foment o ànim d'actes independents d'actors no estatals no compliria amb l'estàndard de l'article 8[257]. Això últim, pot suposar un problema quan els Estats inciten a aquestes conductes, com per exemple Rússia en suggerir atacs cibernètics contra Estònia el 2007 apel·lant al patriotisme dels hackers[258]. Per acabar, en opinió personal, considero que mentre aquest control efectiu, més estricte, permet que no s'abusi de la legítima defensa i no s'acusi malintencionadament a l'Estat de cada atac cibernètic; també permet cobrir amb més facilitat als particulars contractats per l'Estat per realitzar aquestes conductes.

2. Operacions cibernètiques com atacs armats per actors no estatals

Pot succeir inclús que després de la investigació de l'autoria reveli que no hi ha un Estat al darrere, sinó una organització terrorista[259]. De fet, en el ciberespai, els actors no estatals, també han guanyat protagonisme en els últims anys, i la majoria de les operacions cibernètiques contra Estats són portades a terme per aquests[260]. I això és així per raons lògiques, les eines són barates, accessibles i fàcils de "convertir en armes"; de manera que, no només poden realitzar aquests atacs destructius Estats, sinó també líders d'una oposició, radicals ideològics, organitzacions terroristes i particulars[261].

Com ja comentàvem anteriorment, la Carta de les Nacions Unides no fa referència als actors no estatals com a subjectes de la prohibició de l'ús de la força, i la legítima defensa només es permet contra atacs armats portats a terme directe o indirectament per Estats. No obstant això, la recent pràctica estatal i les Resolucions 1368 i 1373 de 2001 del Consell de Seguretat, ens mostra que la comunitat internacional tendeix a donar suport a l'ús del dret a legítima defensa contra actors no estatals[262]. Doncs a partir dels successos de l'11S la comunitat internacional es va adonar que s'enfrontava a nous reptes per part d'actors no estatals; per una banda, la voluntat de matar a persones en massa per part d'aquests grups i, per altra banda, l'extraordinària capacitat per crear xarxes mundials i portar a terme operacions cibernètiques.

Al tractar aquesta qüestió, és veritat que es parla d'atacs armats convencionals (sintètics), però per tot el que s'ha explicat fins ara en aquest treball, podríem entendre que la mateixa conclusió podria extreure's pels atacs cibernètics d'escala i efectes equiparables. Autors com Cervell o Schmitt, també ho han entès així[263]. En aquest mateix sentit, el Manual Tallin ens diu que un atac

[257] Rafighdoust, H. (2018). *Op. cit.*, p.260.
[258] Cervell, M. J. (2017). *Op. cit.*, p.307.
[259] *Ibid.*, p.308.
[260] Roscini, M. (2014). *Op. cit.*, p.80.
[261] Rafighdoust, H. (2018). *Op. cit.*, p.246.
[262] *Ibid.*; també Cervell, M. J. (2017). *Op. cit.*
[263] *Ibid.*; i Schmitt, M. N. (2010). *Op. cit.*, p.172.

cibernètic per part d'un actor no estatal contra una infraestructura crítica d'un Estat i sense la implicació o participació d'un altre Estat pot constituir un atac armat[264]. I per això, ens diu que "l'objecte d'una operació cibernètica que compleixi amb els requisits transfronterers i d'escala i efectes també pot determinar si es qualifica com un atac armat" i, per tant, "si consisteix en béns o persones dins del territori de l'Estat afectat, sigui governamental o privat, l'acció és un atac armat contra aquest Estat"[265]. No obstant això, respecte a aquesta última qüestió, no existeix consens entre els experts del Manual Tallin; mentre uns consideren que els atacs motivats únicament per un interès privat, no poden constituir un atac armat per justificar el dret a legítima defensa, els altres els són indiferents les seves motivacions[266]. Personalment, considero que per actuar en legítima defensa l'objectiu o la finalitat dels atacs ha de ser contra la seguretat política o nacional d'un altre Estat per tal que puguin violar la seva sobirania. En aquest sentit, la ciberdelinqüència transfronterera (per exemple, tot frau a Internet, robatori d'identitat, pirateria, etc.), poden ser ciberdelictes, però no atacs cibernètics.

Respecte a la possibilitat d'actuar en legítima defensa contra Estats no directament culpables de l'atac, però que s'haguessin mostrat incapaços o reticents (*unable or unwilling*) per evitar-lo, tenint en compte la importància de la implicació dels Estats en la prevenció d'aquestes conductes[267], la qüestió planteja més dubtes. Els Estats Units ha recalcat de manera expressa que els Estats tenen l'obligació d'adoptar totes les mesures necessàries perquè en el seu territori no pugui ser utilitzat per portar a terme aquests tipus d'atacs, i a conclusions similars arriba l'Informe del Grup d'Experts sobre els avenços en la informació i les telecomunicacions en el context de la seguretat internacionals de 2013 i el Manual Tallin[268]. Per tant, seguint aquesta doctrina, semblaria que en casos extrems i basats en el criteri de necessitat, l'Estat víctima, se'l permet actuar en legítima defensa contra un actor no estatal en territori d'un altre Estat en què les operacions cibernètiques tenen objectius o finalitats polítiques o de seguretat nacional[269]. És a dir, estem parlant d'accions en legítima defensa no en el territori del propi Estat, sinó en un altre que no és directament culpable, però és incapaç o es mostra reticent a repel·lir l'atac. En opinió personal, considero que tot i ser certa, l'obligació dels Estats d'evitar que des del seu territori es causin danys a un altre, em sembla perillosa la generalització d'aquesta doctrina i poder actuar en legítima defensa en territori d'un tercer (sense consentiment de l'Estat o del Consell de Seguretat). En primer lloc, perquè pot portar a abusos contraris a la concepció excepcional de la figura de la legítima defensa. I, en segon lloc, per la dificultat, atesa la naturalesa dels atacs cibernètics,

[264] Schmitt, M. N. (2017). *Op. cit*., p.345, para. 19.
[265] *Ibid*., p.346, para. 21.
[266] *Ibid*.
[267] Cervell, M. J. (2017). *Op. cit*., p.308 i 309.
[268] *Ibid.*
[269] Rafighdoust, H. (2018). *Op. cit*., p.252.

d'avaluar no només la "incapacitat" cibernèticament parlant de l'Estat per repel·lir l'atac, sinó també de la "la falta de voluntat" de l'Estat.

D. Altres requisits per l'exercici del dret a legítima defensa davant atacs cibernètics

Per molt clara que ens sembli avui en dia l'aplicació de les normes tradicionals de l'ús de la força al ciberespai, pot quedar obsoleta en un futur no tan llunyà; el que vol dir no aparcar la qüestió, sinó reflexionar des d'aquest moment sobre ella[270]. En aquest sentit, d'acord amb el Dret Internacional, quan un atac cibernètic equival a un atac armat, l'Estat víctima haurà de complir amb els requisits de necessitat, proporcionalitat i immediatesa per poder actuar en legítima defensa[271]. Per tant, el dret de legítima defensa ha d'estar limitat al que sigui necessari per abordar un atac armat imminent o actual i ha de ser proporcionat al repte el qual s'enfronta[272].

1. Necessitat i proporcionalitat

Com ja hem dit, el requisit de necessitat fa referència al fet que les mesures adoptades siguin adequades o convenients per repel·lir l'atac armat. En el context dels atacs cibernètics, el Manual Tallin expressa que "l'ús de la força en operacions cibernètiques per un Estat en exercici del seu dret de legítima defensa ha de ser necessari i proporcionat"[273].

En primer lloc, per satisfer el requisit de necessitat, com es pot entendre de l'expressat pel TIJ en el cas concernent a les Plataformes Petrolíferes, l'ús de la força com a reacció en legítima defensa ha de ser l'últim recurs per fer front a l'atac armat imminent o el que està tenint lloc en aquell moment. En aquest conflicte, el tribunal no va acceptar la justificació del dret a legítima defensa per part dels Estats Units, per no haver realitzat cap esforç previ en resoldre el conflicte diplomàticament[274]. De manera que "la clau de l'anàlisi de la necessitat en el context cibernètic és l'existència, o la manca d'aquesta, de cursos d'acció alternatius que no impliquin l'ús de la força"[275]. En aquest sentit, si les defenses cibernètiques passives o operacions cibernètiques que no arriben al nivell d'ús de la força fossin adequades per frustrar un ciberatac armat (futur o en curs), no es permetria l'ús de la força (cibernètica o sintètica) com a mesura defensiva[276]. Ara bé, la qüestió aquí tractada no és blanc o negre, ús de la força o mesures no forçoses, sinó que les

[270] Cervell, M. J. (2017). *Op. cit.*, p.303 i 304.
[271] Schmitt, M. N. (2017). *Op. cit.*, p.348 a 354; també Roscini, M. (2014). *Op. cit.*, p.88.
[272] Rafighdoust, H. (2018). *Op. cit.*, p.273.
[273] Schmitt, M. N. (2017). *Op. cit.*, p.348.
[274] Sentència TIJ (República Islàmica d'Iran v. Estats Units), *op. cit.*, p.198, para. 76.
[275] Schmitt, M. N. (2010). *Op. cit.*, p.167.
[276] *Ibid.*

mesures coercitives es poden combinar amb mesures no coercitives, com la diplomàcia o les sancions econòmiques[277].

En segon lloc, la necessitat exigeix també assegurar-se que l'atac cibernètic "no és accidental, verificar la veritable identitat de l'Estat -o entitat no estatal- que porta a terme l'atac (per no posar en perill parts innocents), i concloure que l'ús de la força com a contramesura és indispensable"[278]. A més a més, hem de tenir en compte que la necessitat d'utilitzar la força en legítima defensa és jutjada des de la perspectiva de l'Estat víctima; de manera que la determinació d'aquesta necessitat ha de ser raonable atenent a les circumstàncies específiques del cas particular[279].

A part del requisit de necessitat, a la vegada, el Dret Internacional obliga que qualsevol reacció en exercici del dret a legítima defensa sigui proporcionada a l'atac cibernètic[280]. És a dir, a guardar un cert equilibri entre l'atac i la resposta, però no, com ja hem comentat, que la resposta fos de la mateixa naturalesa que la del atac[281]; sinó que les mesures adoptades en legítima defensa siguin les més adequades per repel·lir l'atac i no merament equiparables. Per tant, la força utilitzada (com a ultima ratio) en cap cas pot ser irraonable o excessiva per aconseguir l'objectiu de defensar-se. En aquest sentit, el Manual Tallin considera que la proporcionalitat fa referència a quanta força cibernètica està permesa un cop ha sigut considerada necessària, afirmant que "el criteri limita l'escala, l'abast, la durada i la intensitat de la resposta defensiva a la necessària per posar fi a la situació que ha donat lloc al dret de legítima defensa"[282].

Ara bé, com acabem de comentar, i com implícitament va declarar el TIJ en l'Opinió consultiva de l'ús d'armes nuclears i com la majoria dels autors consideren, la resposta no ha de ser de la mateixa naturalesa que la de l'atac. De manera que, la utilització de força sintètica en resposta d'un ciberatac armat, i viceversa, seria perfectament admisible[283]; sobretot si tenim en compte que no tots els Estats podrien estar tecnològicament suficientment preparats per una efectiva resposta cibernètica[284].

No obstant això, en el context dels atacs cibernètics, sembla molt difícil determinar el nivell de força permesa per respondre a aquests i aleshores complir amb el requisit de proporcionalitat. Tant la velocitat com la naturalesa oculta dels atacs cibernètics fan difícil comptabilitzar la seva magnitud i les seves conseqüències per reaccionar en legítima defensa i complir el requisit de

[277] *Ibid.*
[278] Dinstein, Y. (2002). *Op. cit*., p.109.
[279] Schmitt, M. N. (2017). *Op. cit*., p.349, para. 4.
[280] Rafighdoust, H. (2018). *Op. cit*., p.275.
[281] Cervell, M. J. (2017). *Op. cit*., p.304.
[282] Schmitt, M. N. (2017). *Op. cit*., para. 5.
[283] *Ibid*.; també Cervell, M. J. (2017). *Op. cit.*
[284] *Ibid.*

proporcionalitat[285]. A més, pot ser que els efectes d'alguns atacs cibernètics no siguin instantanis i triguin algun temps a aparèixer, com per exemple el cas del Stuxnet[286]. I no només això, sinó que un cop decidits a respondre (cibernèticament) a l'atac armat és molt difícil poder limitar els seus efectes únicament a l'Estat afectat o a l'actor no estatal[287]. Per això, en opinió personal, considero que la proporcionalitat, tot i ser un requisit per la legalitat de l'exercici del dret a legítima defensa, una reacció cibernètica desproporcionada no hauria de convertir-la automàticament en una represàlia il·legal, "només faria responsable a l'Estat d'un acte d'excés (o abús) de legítima defensa"[288].

En resum, podríem dir, per una banda, que es pot exercir el dret a legítima defensa per repel·lir atacs cibernètics, però hi ha discussions importants respecte en quines situacions (necessitat) i com (proporcionalitat); i, per altra banda, les respostes cibernètiques en legítima defensa semblen difícils que puguin seguir el requisit de proporcionalitat[289].

2. Immediatesa

La immediatesa suggereix intrínsecament que l'activació del dret a legítima defensa no pot ser massa tardana[290]. Segons alguns autors, com Dinstein, aquesta condició s'hauria d'interpretar "en sentit ampli"[291]. En aquesta dirrecció, el Manual Tallin ens diu que "factors com la proximitat temporal entre atac i resposta, el període necessari per identificar l'atacant, i el temps requerit per preparar una resposta són rellevants en aquest aspecte"[292].

a) El problema de la ràpida identificació de l'atacant en els atacs cibernètics i la resposta a *posteriori*

Aquí sorgeixen dos problemes evidents. En primer lloc, com hem dit, el Dret Internacional no permet un ús de la força en legítima defensa que sigui transfronterer, a no ser que es pugui identificar a un actor Estatal o no estatal que opera des del territori d'un tercer Estat. A part d'això, la identificació de l'atacant i la seva intenció és una exigència del requisit de necessitat. I, en segon lloc, com també hem dit, una de les característiques principals dels atacs cibernètics és

[285] Roscini, M. (2014). *Op. cit.*, p.90.
[286] Rafighdoust, H. (2018). *Op. cit.*, p.278.
[287] *Ibid.*
[288] Ronzitti, N. (2006). The Expanding Law of Self-Defence. *Journal of Conflict & Security Law*, *11*(3), 343–359, p.355. http://www.jstor.org/stable/26294445
[289] Rafighdoust, H. (2018). *Op. cit.*, p.279.
[290] Dinstein, Y. (2002). *Op. cit.*, p.110.
[291] *Ibid.*
[292] Schmitt, M. N. (2017). *Op. cit.*, p.353, para. 12.

l'anonimat. Aquesta facilitat d'amagar la procedència dels atacs fa que sigui molt difícil i, en ocasions, impossible de discernir l'atribució de l'atac de manera ràpida i acurada[293].

Així mateix, el Manual Tallin ha reconegut les dificultats que presenta el requisit de la immediatesa en el context de les operacions cibernètiques remarcant que "el fet que s'ha produït o s'està produint un ciberatac armat pot no ser evident durant algun temps. I això pot ser perquè no s'ha identificat la causa del dany o la lesió", o perquè "l'originador de l'atac no pot ser identificat fins molt després de l'atac"[294]. D'aquesta manera, i seguint aquesta visió, en moltes ocasions el requisit de la immediatesa contra algunes operacions cibernètiques no podrà complir-se.

És per això, com dèiem, que alguns autors han entès que el requisit de la immediatesa en el context dels atacs cibernètics s'ha d'interpretar "en sentit ampli". En aquest sentit, Roscini ens diu que "immediatesa no significa 'instantani' i s'ha d'aplicar amb flexibilitat", ja que resulta lògic, en algunes circumstàncies, que l'Estat víctima necessiti temps per reunir les proves suficients per acusar a un Estat o un actor no estatal concret d'haver realitzat l'atac cibernètic[295]. En conseqüència, en alguns casos, no es pot impedir a l'Estat víctima d'exercir el seu dret a legítima defensa "per no ser capaç de respondre instantàniament o per no estar segur de qui és el responsable de l'atac o d'on es va originar"[296]. I per això, degut a la naturalesa dels atacs cibernètics, en la majoria dels casos, l'ús de la força en legítima defensa serà exercida a *posteriori*[297].

b) Dret a la legítima defensa anticipada i operacions cibernètiques

L'objectiu del dret a legítima defensa és repel·lir un atac armat, en aquest cas un ciberatac armat. En aquest sentit, no podem confondre el requisit de la immediatesa amb la imminència d'un atac cibernètic en el context de la legítima defensa anticipada[298].

Com bé sabem, a partir dels atemptats de l'11 de setembre de 2001 es va marcar un abans i un després a la concepció de la legítima defensa. Tot i així, avui en dia el debat segueix respecte de si és o no possible la legítima defensa davant atacs armats no consumats, donant lloc a una extensa literatura sobre la legítima defensa anticipada, preventiva i altres formes de mesures preventives o interceptives. No obstant això, no existeix cap definició precisa i acceptada universalment

[293] Rafighdoust, H. (2018). *Op. cit.*, p.280.
[294] Schmitt, M. N. (2017). *Op. cit.*, p.354, para. 14.
[295] Roscini, M. (2014). *Op. cit.*, p.91.
[296] Gill, T. D. i Ducheine P. A. (2013). Anticipatory Self-Defense in the Cyber Context. *International Law Studies, 89*, 438-471, p.451. https://digital-commons.usnwc.edu/ils/vol89/iss1/6/
[297] Roscini, M. (2014). *Op. cit.*; també Cervell, M. J. (2017). *Op. cit.*, p.305.
[298] Roscini, M. (2014). *Ibid.*

respecte a aquests termes, de manera que molts dels autors li atribueixen diferents significats a cadascuna d'ells. El TIJ ha evitat pronunciar-se al respecte, i quan ha hagut de tractar amb la legítima defensa ha optat sempre per una interpretació tradicional i ancorada a l'article 51, és a dir, a la legítima defensa únicament davant l'existència d'atacs armats consumats[299]. En canvi, altres textos com l'Informe del Grup d'Alt Nivell sobre les amenaces, els reptes i el canvi publicat el 2004 com a conseqüència del seu encàrrec per part del Secretari General de les Nacions Unides el 2003; així com, l'Informe del Secretari General l'any següent a la publicació (2005), amb el títol "Un concepte més ampli de la llibertat: desenvolupament, seguretat i drets humans per a tots"; admeten, ambdós, la legítima defensa davant d'atacs imminents[300]. Hem de tenir en compte la importància que suposa aquest últim, ja que prové d'una de les principals institucions de les Nacions Unides segons la Carta. A més a més, a partir d'aquí apareixen altres textos que confirmen aquest canvi de tendència: la Resolució de l'Institut de Dret Internacional (IDI) el 2007, els Principis generals de Dret Internacional sobre l'ús de la força pels Estats en legítima defensa de la *Chatham House* de 2005, el Manual Tallin i la conferència de la *International Law Assosiation* (ILA) el 2016[301]. Evidentment, cadascun d'ells ho accepta, però amb els seus propis matisos amb menor o major mesura, que no passarem a analitzar. Així mateix, bona part de la doctrina també l'accepta, i alguns autors consideren que la legítima defensa anticipada ja es podia inferir del cas *Caroline* de 1937 i posteriorment afirmat pel Tribunal de Nuremberg el 1946[302]. De fet, actualment es parla del canvi en el debat entre aquells que accepten la legítima defensa preventiva, però limitada a atacs imminents i els que no, mentre que els qui defensen la legítima defensa preventiva sense limitació, o més ben dit, la possibilitat de legítima defensa davant d'atacs "latents" segueixen sent una minoria[303]. En opinió personal, considero que a partir de tot l'exposat podem veure una tendència de la comunitat internacional a reconèixer explícitament la possibilitat d'utilitzar la força davant d'atacs imminents. A més, considero poc raonable que un Estat hagi d'esperar a ser atacat per exercir el seu dret a legítima defensa quan existeixen motius manifestos i suficients per entendre que l'atac és imminent; tenint en compte les amenaces terroristes,

[299] Cervell, M. J. (2017). *Op. cit.*, p.170.

[300] Document A/59/565, Informe del Grup d'Alt Nivell sobre les amanaces, els reptes i el canvi, de 2 de desembre de 2004, p.61; i Document A/59/2005, Informe del Secretari General sobre un concepte més ampli de la llibertat: desenvolupament, seguretat i drets humans per a tots, de 21 de març de 2005, p.37 para. 124.

[301] Resolució IDI, "Problemes actuals de l'ús de força armada en el Dret Internacional. A. Legítima Defensa", de 27 d'octubre de 2007, p.1 para. 3; The Chatham House (2006). Principles of International Law on the Use of Force in Self-Defence. *The International and Comparative Law Quarterly*, 55(4), 963–972, p.965. http://www.jstor.org/stable/4092626; Schmitt, M. N. (2017). *Op. cit.*, p.350; i ILA (2016). Use of force. *Johannesburg Conference*, 1-20, p.10. https://www.ila-hq.org/en_GB/documents/conference-report-johannesburg-2016-9

[302] Greenwood, C. (2011). *Op. cit.*, p.12, para. 45; també Rafighdoust, H. (2018). *Op. cit.*, p.184.

[303] Cervell, M. J. (2017). *Op. cit.*, p.202.

nuclears, d'atacs cibernètics i tecnologia cada cop més complexa en què ens enfrontem avui en dia.

Ara bé, el que ens interessa en aquest treball és l'anàlisi d'aquesta figura en el context cibernètic. En aquest sentit, primerament si un Estat té coneixement que els seus sistemes han estat compromesos per un atac cibernètic, pot adoptar mesures passives o actives de ciberdefensa per neutralitzar l'amenaça. I en tot cas, si fallen tots els altres mitjans per neutralitzar l'amenaça cibernètica, o disposa d'informació que indiqui que la penetració forma part d'un atac global, l'Estat podrà recórrer a la legítima defensa anticipada[304]. Ara bé, el repte més difícil en l'anàlisi de la legítima defensa anticipada en els casos d'atacs cibernètics és la determinació d'una amenaça imminent[305]. Perquè a diferència dels tradicionals es realitzen sense previ avís, no hi ha insinuacions d'un atac imminent com pot ser la propaganda, declaracions bèl·liques, moviments de tropes a la frontera, etc[306]. I encara que es pogués identificar, en els atacs cibernètics resultaria difícil saber si seran de suficient gravetat per considerar-se atacs armats, així com la intenció real de l'atacant[307].

Respecte a aquesta última problemàtica es creu que el millor seria, com ja hem dit en un apartat anterior, tenir en compte totes les conseqüències raonablement previsibles d'una operació cibernètica per qualificar aquesta operació d'atac armat[308]. Tot i així, de moment, ho considero extremadament difícil de portar-ho a la pràctica, ja que no només hem de saber que ens enfrontem a un ciberatac armat, sinó que la resposta anticipada s'haurà d'ajustar igualment al criteri de necessitat i proporcionalitat.

Respecte a la primera, la determinació d'una amenaça imminent, per alguns autors sembla que el més convenient en el context cibernètic, seria optar per una visió més flexible del concepte d'"imminència" i no tan restrictiva com la que podria venir imperant fins ara. Doncs com és sabut la naturalesa de la guerra al segle XXI ha evolucionat dràsticament i, segons els partidaris d'aquesta visió, no es pot seguir depenent del criteri tradicional de la proximitat temporal que troba els seus orígens en el cas *Caroline*. En aquest sentit, Estats i autors han exposat diferents propostes amb alguns matisos entre elles, però bastant encaminades a la idea d'avaluar cada cas concret i tenir en compte per això que hi hagués algun tipus d'acció preparatòria o algun pla destinat específicament a atacar a un Estat, la gravetat de l'amenaça projectada, els mitjans emparats per portar-la a terme (naturalesa de l'amenaça), etc[309]. Doncs, d'aquesta manera, la

[304] Tsagourias, N. (2012). *Op. cit.*, p.232.
[305] Rafighdoust, H. (2018). *Op. cit.*, p.283 i 284.
[306] *Ibid.*
[307] *Ibid.*
[308] Schmitt, M. N. (2017). *Op. cit.*, p.343, para. 13.
[309] Cervell, M. J. (2017). *Op. cit.*, p.205.

imminència de l'atac s'ha de valorar no només en funció del factor temps, sinó també de les circumstàncies de cada cas concret[310]. També resulta interessant el criteri adoptat pel Manual Tallin, el qual rebutja l'estricte criteri temporal per determinar la imminència i opta, en canvi, per valorar el risc que correria l'Estat si dilatés massa la seva resposta ("*last feasible window of opportunity*")[311], el que es coneix entre la doctrina com el criteri d'última oportunitat o *last opportunity*. I com ens diu Roscini, per utilitzar una legítima defensa anticipada efectiva en base aquest criteri dependrà de l'avaluació de la informació disponible en aquell moment basada en la bona fe[312]. No obstant, hem de tenir en compte que com més flexibilitzem, més probabilitat hi ha d'abusos; sobretot tenint en compte que la línia entre un atac imminent i un atac latent, o més ben dit, entre la legítima defensa anticipada i la preventiva és molt fina.

Finalment, en opinió personal, m'agradaria destacar dues coses. La primera, és que avui en dia és molt difícil que es pugui portar a terme una legítima defensa anticipada, almenys de forma legal, per un ciberatac imminent. El més raonable, actualment, és que aquesta s'arribi a dur a terme quan els atacs cibernètics no equivalguin a atacs armats, però siguin precursors d'un atac sintètic[313]. Per exemple, quan els Estats intenten a través d'atacs cibernètics destruir el sistema electrònic de comandament i control, comunicacions, intel·ligència o xarxes de control d'armes[314], prèviament a un atac armat. De fet, alguns exemples reals en què la legítima defensa anticipada podria ser vàlida, és en el cas dels atacs cibernètics Russos a les pàgines web del Govern de Geòrgia del 2008 previs al començament del conflicte, així com les operacions cibernètiques d'Israel el 2007 per desactivar els sistemes de defensa antiaèria sirians prèvies a l'atac aeri a la planta nuclear[315]. I la segona que m'agradaria comentar, és que la complexitat d'aquesta qüestió, no hauria de ser motiu per deixar-la sense resoldre, tenint en compte, a més, la facilitat i la capacitat dels actors no estatals per realitzar aquests tipus d'accions com ja hem comentat. Per això, crec que per una major seguretat jurídica, s'hauria d'arribar a algun tipus d'acord internacional, un pronunciament del TIJ, conferència internacional, o inclús, del Consell de Seguretat que fixes uns paràmetres mínims per determinar quan un atac hauria de ser considerat imminent més enllà de la criticada Resolució 2249 del 2015.

En resum, d'acord amb l'estat actual de les coses en el camp cibernètic, estic d'acord amb Cervell que per determinar quan un atac és imminent i, per tant, poder actuar en legítima defensa s'hauria de tenir en compte el següent: en primer lloc, no perdre de vista els requisits de necessitat i

[310] Roscini, M. (2010). *Op. cit.*, p.122.
[311] *Ibid*.; també Schmitt, M. N. (2017). *Op. cit*., p.351, para. 4.
[312] Roscini, M. (2014). *Op. cit.*, p.79.
[313] Rafighdoust, H. (2018). *Op. cit.*, p.286.
[314] *Ibid.*
[315] *Ibid.*

proporcionalitat, tot i la dificultat que això suposa en els atacs cibernètics que ja hem comentat; i, en segon lloc, exigir, almenys, un mínim d'accions que demostrin que l'atac, tot i no haver-se desencadenat, es trobi en una fase preliminar en tant que existeixi algun tipus de prova fefaent de què hi ha algun tipus de preparatiu encaminat a posar-lo en pràctica[316].

[316] Cervell, M. J. (2017). *Op. cit*., p.207 i 208.

CONCLUSIONS

El desenvolupament tecnològic a l'àmbit del ciberespai ha creat noves amenaces per a la seguretat nacional dels Estats. Però, tant el Dret Internacional com la Carta de les Nacions Unides, s'han concebut, fins ara, per abordar activitats sintètiques. La Carta es va redactar abans de l'aparició de l'Internet i, com a conseqüència, les operacions cibernètiques presenten un repte únic i real a la definició tradicional del que constitueix un ús de la força. La tecnologia ha avançat més ràpidament que el Dret, i a mesura que la tecnologia es torna cada vegada més sofisticada, els problemes a les normes que regeixen els atacs cibernètics i la ciberseguretat creixen exponencialment. Les seves característiques específiques presenten reptes essencials i, per tant, seran necessàries noves traduccions de les normes fonamentals del Dret Internacional relatives a l'àmbit cibernètic per poder fer-los front. És per això, que ens plantejàvem la qüestió de si l'aplicació dels principis jurídics preexistents a la tecnologia moderna eren suficients a la llum de les característiques especials de la cibernètica.

Amb l'anàlisi realitzat, hem vist que el Dret Internacional té serioses deficiències en la seva aplicació envers les operacions cibernètiques; principalment per la incertesa de no saber quan un atac cibernètic constitueix un atac armat i per les dificultats a l'hora d'atribuir aquests atacs a Estats o actors no estatals. Tot i aquesta dificultat, l'ús recurrent i la gravetat que representa l'amenaça de les noves tecnologies exigeix que la comunitat internacional arribi a un consens tant sobre el significat d'atac cibernètic com d'atac armat en el marc del *ius ad bellum*. També, sobre les opcions de què disposen els Estats víctimes per contrarestar aquests atacs, com per exemple el dret de legítima defensa. Qüestions que es revisaran a continuació.

En el context de les relacions internacionals el principi de prohibició de l'ús de la força és la pedra angular i norma fonamental del Dret Internacional. De manera que, ha estat un dels èxits més importants de la comunitat internacional durant el segle XX. El principi és aplicable a les relacions interestatals i no en el marc dels assumptes interns dels Estats, excepte de les situacions en què els conflictes interestatals s'internacionalitzen. Tot i això, la presència militar estrangera en un conflicte intern d'un altre Estat amb el consentiment d'aquest últim no pot vulnerar aquest principi. Per tant, en el context de les operacions cibernètiques, aquells atacs cibernètics transfronterers portats a terme directament o indirectament pels Estats contra altres Estats poden violar el principi de la prohibició de l'ús de la força.

En el marc del principi de prohibició de l'ús de la força no pot existir una visió restrictiva. Per arribar a tal conclusió hem abordat la problemàtica des de tres perspectives: si la força podia ser diferent de la força armada (*armed force*); si aquesta força es limitava a la dirigida contra el territori o la independència política d'un Estat; i finalment, el llindar de força prohibida pel

principi. En aquest sentit, el que hem vist és que l'opinió predominant sobre el significat de la força durant els anys següents a l'adopció de la Carta, es limitava a una força armada, però atès que el Dret Internacional és dinàmic i no estàtic, i d'acord amb l'enfocament basat en els efectes (*effect-based approach*), la prohibició de l'ús de la força també s'estén a la força no militar quan aquesta ostenta els mateixos efectes que els d'una força armada. En aquest sentit, les armes biològiques i químiques o les operacions cibernètiques amb capacitat per destruir vides i propietats poden violar el principi de prohibició l'ús de la força. Per tant, el principi inclou qualsevol tipus de força, independentment que atempti contra la integritat territorial o la independència política d'altres Estats. En aquest sentit, tot ús de la força que sigui incompatible amb el manteniment de la pau i la seguretat internacionals pot violar aquest principi, fins i tot violacions menors en les fronteres estatals poden violar aquest principi.

Pel que fa al llindar de força prohibit, hem de distingir entre les formes més greus i altres formes menys greus de l'ús de la força d'acord amb el criteri d'"escala i efectes" assentat pel TIJ. El que donaria lloc a les modalitats de força prohibides pel principi; l'agressió i en particular l'atac armat són les formes més greus d'ús de la força, mentre que altres accions per sota del llindar d'agressió són menys greus. Així mateix, pels redactors de la Carta i la comunitat internacional en les darreres dècades, sembla ser que les coaccions polítiques, diplomàtiques o econòmiques no poden transgredir el principi de la prohibició de l'ús de la força. No obstant això, amb l'aparició de força no armada (química, biològica, nuclear, drons o la cibernètica) han sorgit nous debats entre la doctrina respecte a l'enfocament o criteri de l'escala i efectes. Doncs com comentàvem en el treball, es debat que si el criteri és acceptat majoritàriament i, per tant, s'accepta la força no armada; és incompatible sostenir que les coaccions econòmiques, amb efectes destructius, no poden violar el principi de la prohibició de l'ús de la força. Ara bé, considerem que sostenir l'existència d'un llindar general de mínims, almenys de moment, sembla precipitat i a la vegada perillós; de manera que, el millor seria analitzar les circumstàncies especials de cada cas.

De tot això, al nostre entendre, considerem que totes les operacions cibernètiques amb escala i efectes anàlegs als d'altres operacions sintètiques o no sintètiques s'accepten com a ús de la força. I per això, d'acord amb l'opinió predominant, les operacions cibernètiques que causin o puguin causar danys físics a la propietat, pèrdua de vides o lesions a les persones poden violar el principi de la prohibició de l'ús de la força. En canvi, altres activitats cibernètiques, com l'espionatge i la recopilació d'informació, no poden violar aquest principi perquè no són capaços de causar conseqüències destructives directes o indirectes iguals a les d'un atac militar o una força armada. Així mateix, quan una força no armada té efectes d'alta gravetat, pot constituir un atac armat i donar dret a la legítima defensa en virtut de l'article 51 de la Carta. Pel que fa a les operacions cibernètiques amb uns efectes anàlegs als de coacció política, diplomàtica o econòmica, entenem

que no poden violar el principi de prohibició de l'ús de la força. No obstant, quan la coacció econòmica, especialment a través d'atacs cibernètics, constitueixi una pressió considerable i, per tant, una impossibilitat a l'Estat de la seva vida normal (per exemple, operacions cibernètiques massives que paralitzin l'economia d'un Estat), sí que constituirien una violació del principi; inclús un atac armat, si els efectes destructius o disruptius són greus similars als que podria causar un atac armat.

El dret de legítima defensa és la principal excepció al principi de prohibició de l'ús de la força que autoritza qualsevol Estat a recórrer a l'ús de la força contra un altre Estat. Contrari a l'argumentat pel principi de la prohibició de l'ús de la força, l'opinió predominant sobre el dret de defensa legítima, com a excepció del principi de prohibició de l'ús de la força, és un enfocament restrictiu per evitar que els Estats abusin d'aquest dret. Tot i això, el dret de legítima defensa està permès contra un atac armat com a forma més greu d'ús de la força; per tant, la mera violació del principi de la prohibició l'ús de la força no pot justificar l'exercici del dret a legítima defensa. En aquest sentit, de conformitat amb les modalitats d'ús de la força, només l'agressió d'alta gravetat pot constituir un atac armat. Avui dia, aquestes modalitats més greus d'ús de la força també es poden dur a terme mitjançant operacions cibernètiques. De manera que quan els efectes d'una operació cibernètica siguin greus podrà constituir un atac armat. Tot i la manca d'una definició de gravetat, sota l'enfocament basat en els efectes, l'escala i els efectes és el criteri, com ja hem dit, per identificar les operacions cibernètiques com a atac armat. En aquest sentit, poden constituir un atac armat aquelles operacions cibernètiques que lesionin o causin la mort de persones, destrueixin propietats o pertorbin greument el funcionament d'infraestructures crítiques dels Estats amb efectes i conseqüències de gran escala. Tot i així, més enllà del *Pictet's test* generalment acceptat per la comunitat internacional, els paràmetres d'aquest criteri segueixen sense resoldre's i, per tant, no és clar l'abast d'aquests resultats perquè l'operació cibernètica pugui considerar-se un atac armat. En aquest sentit, al nostre entendre, amb la tecnologia actual resulta difícil imaginar que estigui capacitada per causar directament, o més ben dit, per si sola, uns efectes similars als d'un atac armat tradicional. Per això, en aquest treball argumentàvem que es necessita, de moment, un objectiu més fràgil o crucial, com una infraestructura crítica, perquè un atac cibernètic pugui considerar-se un atac armat. No obstant, no existeix un consens general sobre la definició d'infraestructures crítiques.

Per poder utilitzar la força en exercici del dret a legítima defensa contra un altre Estat, l'atac armat s'ha d'atribuir a aquest últim. En aquest sentit, un atac armat es pot atribuir directament a un òrgan *de jure* d'un Estat o indirectament als òrgans *de facto*. L'òrgan *de jure* d'un Estat, inclou totes les activitats de les entitats individuals o col·lectives que componen l'organització o estructura de l'Estat i actuen en nom seu. Els atacs cibernètics per part d'un òrgan de jure de l'Estat, es portaran

a terme, normalment, per les unitats cibernètiques d'un Estat contra un altre. Però, per poder atribuir directament l'atac armat a un òrgan *de jure*, serà necessari que l'Estat víctima aporti "proves clares o convincents", ja que en tractar-se d'una excepció a la prohibició d'ús de la força, l'estàndard de prova ha de ser suficientment alt per limitar i prevenir l'abús d'aquest dret. Tanmateix, en el context dels atacs cibernètics aquesta atribució és un dels majors problemes per a l'ús del dret a legítima defensa degut principalment a tres característiques del ciberespai: l'anonimat, les diverses fases dels atacs cibernètics (*multi-stage cyber attacks*), i la velocitat en què un atac cibernètic pot ser materialitzat.

Segons la CDI, els òrgans *de facto*, són, per una banda, entitats facultades per les autoritats d'un Estat que s'assimilen o que són absorbides per l'aparell estatal. És a dir, empreses o individus que no es poden qualificar d'òrgans de l'Estat per la seva pròpia naturalesa, però estan facultades pel dret intern (per exemple, per la llei, actes administratius, o, si el dret intern ho permet, per contracte) per realitzar elements de l'autoritat governamental. De manera que, estarien revestides de poder estatal (*iure imperii*) per actuar en aquesta instància concreta i, per tant, serà atribuïble a l'Estat. Alhora, inclou aquelles entitats que actuen sota les instruccions, direcció o control d'un Estat. És a dir, serà atribuïble a l'Estat quan l'atac cibernètic que emani d'un particular o entitat privada s'hagi realitzat sota les instruccions, la direcció o el control de l'Estat. Aquesta norma és especialment rellevant en el context cibernètic, en què els Estats solen encarregar aquestes operacions a empreses que s'ocupen d'això o a individus. L'opinió predominant en aquest context és la prova del control efectiu. Es tracta d'un punt de vista més estricte i restrictiu, ja que no es conforma amb el control sobre els actors que porten a terme l'operació cibernètica, sinó que posa èmfasi en el control sobre l'acte. A més, hem de tenir en compte que el mer foment, ànim o suport a actors no estatals no pot atribuir un atac armat a un Estat per justificar el dret de legítima defensa. El que pot suposar un problema quan els Estats inciten a aquestes conductes, com per exemple Rússia en suggerir atacs cibernètics contra Estònia el 2007 apel·lant al patriotisme dels hackers.

La Carta de les Nacions Unides no fa referència als actors no estatals com a subjectes de la prohibició de l'ús de la força, i la legítima defensa, d'acord amb l'enfocament o visió restrictiva, només es permet contra atacs armats portats a terme directe o indirectament per Estats. Tot i això, en les últimes dècades han aparegut noves amenaces. Doncs a partir dels successos de l'11S la comunitat internacional es va adonar que s'enfrontava a nous reptes per part d'actors no estatals amb extraordinària capacitat per crear xarxes mundials i portar a terme operacions catastròfiques; canviant, d'aquesta manera, la interpretació tradicional i restrictiva del dret a legítima defensa. No obstant això, mentre que la recent pràctica estatal i les Resolucions 1368 i 1373 de 2001 del Consell de Seguretat, ens mostra que la comunitat internacional tendeix a donar suport a l'ús del dret a legítima defensa contra actors no estatals; més dubtes planteja l'assentament de la doctrina

sobre la possibilitat d'actuar en legítima defensa contra Estats no directament culpables de l'atac, però que s'haguessin mostrat incapaços o reticents (unable or unwilling) per evitar-ho. És a dir, a actuar en legítima defensa en territori d'un altre Estat sense el seu consentiment o el del Consell de Seguretat. Considerem que la generalització d'aquesta conducta pot ser molt perillosa, ja que pot donar lloc a abusos de la legítima defensa i per la dificultat, en el context cibernètic, que suposa avaluar la "incapacitat" i la "falta de voluntat" de l'Estat.

D'acord amb el Dret Internacional, s'han de complir amb determinats requisits per poder actuar en legítima defensa. El requisit de necessitat significa que l'ús de la força és l'única possibilitat (última *ratio*) de repel·lir un atac armat i que no existeix cap altra alternativa legal possible per aconseguir l'objectiu. Per tant, en el context de les operacions cibernètiques, si la defensa cibernètica passiva és adequada per frustrar l'atac cibernètic, o si hi ha l'oportunitat d'iniciar negociacions, les mesures defensives utilitzant la força quedarien desautoritzades. Així mateix, per complir el requisit de necessitat, l'atac cibernètic ha de tenir intencions hostils i no pot ser accidental. Pel que fa a la proporcionalitat, es refereix al fet que la resposta en exercici del dret a legítima defensa ha de ser proporcional a l'atac armat, ni excessiva ni irraonable. En aquest sentit, en general, és acceptat que: el tipus de mitjans en l'acció defensiva és irrellevant, no han de ser necessàriament els mateixos mitjans que s'han usat per a l'atac; i la resposta ha de limitar-se al propòsit defensiu i no excedir la quantitat de força necessària per repel·lir l'atac armat. En el context cibernètic, els Estats poden respondre al ciberatac armat tant de forma cibernètica com sintètica (igualment a la inversa). No obstant això, tenint en compte la naturalesa del ciberespai, aplicar el criteri de proporcionalitat a l'exercici del dret de legítima defensa és molt difícil, si no impossible. Per això, considerem que en cas d'una reacció cibernètica desproporcionada no hauria de convertir-la automàticament en una represàlia il·legal, sinó en un excés (o abús) de defensa legítima. Finalment, el requisit d'immediatesa, significa l'existència d'una proximitat temporal entre l'atac armat i la resposta. Al nostre entendre, és aconsellable tenir una visió flexible i àmplia del criteri en relació amb els atacs cibernètics, però sense un desfasament temporal indegut entre l'atac i la resposta. Perquè, degut a les característiques de l'àmbit cibernètic, pot transcórrer un lapse de temps entre l'inici de l'atac cibernètic i els efectes d'aquest; de manera que, immediatesa no pot significar instantaneïtat. Així mateix, també entenem que per la naturalesa del ciberespai, en algunes circumstàncies, aquest dret pugui justificar-se a *posteriori* davant d'atacs cibernètics.

No obstant, el requisit d'immediatesa no pot ser confós amb la imminència en el context de la legítima defensa anticipada. Per les raons exposades en aquest treball, considerem que podem veure una tendència de la comunitat internacional a reconèixer explícitament la possibilitat d'utilitzar la força davant d'atacs imminents. Però, no, en canvi, respecte a la legítima defensa preventiva, és a dir, utilitzar la força quan l'amenaça és "latent" però no imminent. A més,

considerem que recórrer al dret de legítima defensa només contra un atac consumat no és realista per fer front als atacs cibernètics, especialment amb una tecnologia cada cop més complexa. Per tant, en el context de les operacions cibernètiques, un Estat no està obligat a esperar inactivament fins que es produeixi l'atac cibernètic. Si un Estat s'assabenta que pot ser objecte d'un atac cibernètic, pot adoptar mesures passives o actives de ciberdefensa per frustrar-lo. I en el cas que totes aquestes mesures fracassessin, podria recórrer a la legítima defensa anticipada. Ara bé, identificar un atac imminent en el camp cibernètic és més difícil que en el sintètic; donat que, normalment no hi ha cap advertència que indiqui que l'atac és imminent i l'interval entre el llançament de l'atac i l'aparició dels efectes pot ser qüestió de segons. De manera que, per fer front a aquesta problemàtica, alguns autors rebutgen l'estricte criteri temporal per determinar la imminència i opten per valorar el risc que correria l'Estat si dilatés massa la seva resposta (*last feasible window of opportunity*). En conseqüència, en el context de les operacions cibernètiques, l'aplicació dels requisits de la legítima defensa és molt difícil i s'ha d'examinar cas per cas. En la majoria dels casos, la determinació de les condicions per poder recórrer al dret de legítima defensa es basaria en una avaluació raonable de l'Estat defensor que, a la pràctica, pot obrir la porta a abusos. Així mateix, entenem que per l'aparició d'actes terroristes duts a terme per actors no estatals i pel naixement de noves formes d'ús de la força a nivell internacional, especialment a través del ciberespai; la concepció del dret de legítima defensa ha canviat cap a una visió més àmplia.

Finalment, al nostre entendre i com a conclusió final d'aquest treball, creiem que l'aplicació de les normes preexistents del Dret Internacional al ciberespai, en particular a l'àmbit de l'ús de la força i a l'espera de noves pràctiques entre els Estats perquè l'acceptació generalitzada d'aquestes pugui consolidar noves normes de Dret Internacional, no és el mètode més adequat per abordar la problemàtica. I ho creiem, perquè entenem que facilita l'ambigüitat de les normes, mentre afavoreix als interessos dels Estats més potents. Per tant, considerem que les interpretacions del TIJ, més adaptades a la realitat actual, pot ser la solució més adequada i viable als reptes de ciberespai. Per altra banda, la revisió de les normes actuals sembla una fita impossible a la llum del poc interès al respecte per les grans potències, en especial dels membres permanents del Consell de Seguretat, per la raó que acabem d'exposar. Una altra opció és un tractat general, tanmateix, per aquest interès en l'ambigüitat, també sembla difícil assolir un consens general per a l'adopció d'aquestes normes específiques. A més, l'experiència que ens precedeix és que els Estats s'inclinen principalment per acords regionals o bilaterals, en àmbits molt específics, com el Conveni sobre la ciberdelinqüència del 2001. De manera que, de moment, i si res canvia, no sembla factible assolir un nou consens mundial per a l'acceptació de normes específiques sobre l'ús de la força en el ciberespai.

REFERÈNCIES BIBLIOGRÀFIQUES

A. Referències documentals

1. Documents Institucionals

a) AGNU

i) Resolucions

- Resolució AGNU 2131 (XX) “Declaració sobre la inadmissibilitat de la intervenció en els assumptes interns dels Estats i protecció de la seva independència i sobirania”, de 21 de desembre de 1965.
- Resolució AGNU 2625 (XXV) “Declaració sobre els principis de dret internacional referents a les relacions d'amistat i la cooperació entre els estats de conformitat amb la Carta de les Nacions Unides”, 24 d’octubre de 1970.
- Resolució AGNU 3314 (XXIX) “Definició d’agressió”, 14 de desembre de 1974.
- Resolució AGNU 58/199 “Creació d’una cultura mundial de seguretat cibernètica i protecció de les infraestructures dinformació essencials”, 23 de desembre de 2003.

ii) Altres documents

- Document A/59/565, Informe del Grup d’Alt Nivell sobre les amanaces, els reptes i el canvi, de 2 de desembre de 2004.
- Document A/59/2005, Informe del Secretari General sobre un concepte més ampli de la llibertat: desenvolupament, seguretat i drets humans per a tots, de 21 de març de 2005.

b) CSNU

- Resolució CSNU 1368, relativa a les amenaces a la pau i la seguretat internacionals creades per actes de terrorisme, de 12 de setembre de 2001.
- Resolució CSNU 1373, relativa a les amenaces a la pau i la seguretat internacionals creades per actes de terrorisme, de 28 de setembre de 2001
- Resolució CSNU 2249, relativa a les amenaces a la pau i la seguretat internacional causades per actes terroristes, de 20 de novembre de 2015.

c) CDI

- Document A/56/10 de la Comissió de Dret Internacional (CDI), Informe sobre la tasca realitzada en el 53è període de sessions de 2001.

2. Instruments internacionals

a) Tractats

- Carta de Nacions Unides, firmada el 26 de juny de 1945 a San Francisco. Entrada en vigor el 24 d'octubre de 1945.
- Tractat constitutiu de l'OTAN, firmat el 4 d'abril de 1949 a Washington.
- Conveni sobre Ciberdelinqüència, firmat el 23 de novembre de 2001 a Budapest. Entrada en vigor el 1 de juliol de 2004.

3. Documents unilaterals

- US Department of Defense (DoD), Joint Terminology for Cyberspace Operation (2010). Visitat al 2 de març de 2023, de: http://www.nsci-va.org/CyberReferenceLib/2010-11-joint%20Terminology%20for%20Cyberspace%20Operations.pdf
- US National Research Council (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyber attack capabilities*. National Academies Press.

4. Altres documents

- The Chatham House (2006). Principles of International Law on the Use of Force in Self-Defence. *The International and Comparative Law Quarterly*, 55(4), 963–972. http://www.jstor.org/stable/4092626
- Resolució IDI, "Problemes actuals de l'ús de força armada en el Dret Internacional. A. Legítima Defensa", de 27 d'octubre de 2007.
- ILA (2016). Use of force. *Johannesburg Conference*, 1-20. https://www.ila-hq.org/en_GB/documents/conference-report-johannesburg-2016-9

B. Referències jurisprudencials

1. Tribunal Internacional de Justícia

- Advisory Opinion ICJ, Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970), I. C.J. Reports 1971.
- Sentència del Tribunal Internacional de Justícia (TIJ), 27 de juny de 1986, assumpte relatiu a les activitats militars i paramilitars contra Nicaragua (Nicaragua v. Estats Units d'Amèrica).
- Advisory Opinion ICJ, Legality of the Threat or Use of Nuclear Weapon, I. C.J. Reports 1996.
- Sentència del Tribunal Internacional de Justícia (TIJ), 6 de novembre de 2003, assumpte relatiu a les Plataformes Petrolíferes (República Islàmica d'Iran v. Estats Units).
- Advisory Opinion ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, I. C.J. Reports 2004.
- Sentència del Tribunal Internacional de Justícia (TIJ), 19 de desembre de 2005, assumpte relatiu a les activitats armades en territori del Congo (República Democràtica del Congo v. Uganda).

C. Referències doctrinals

1. Llibres, articles i obres generals

- Barkham, J. (2001). Information warfare and International Law on the use of force. *New York University Journal of International Law and Politics, 34*, 57-97. https://universityofleeds.github.io/philtaylorpapers/pmt/exhibits/523/barkham.pdf
- Bermejo, R. i López-Jacoiste, E. (2013). De la intervención por causas humanitarias a la responsabilidad de proteger. Fundamentos, similitudes y diferencias. Dins Ministerio de Defensa (ed.), *La respuesta del Derecho Internacional a los problemas actuales de la Seguridad Global* (17-76). https://www.ieee.es/Galerias/fichero/cuadernos/CE_210_RedesTranseuropeas.pdf
- Brownlie, I. (1963). *International Law and the Use of Force by States*. Oxford University Press.
- Carr, J. (2009). *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media.
- Casanovas, O. i Rodrigo, A. J. (2019). *Compendio de Derecho Internacional Público* (8ª ed.). Tecnos.
- Cervell, M. J. (2017). *La Legítima Defensa en el Derecho Internacional Contemporáneo*. Tirant lo Blanch. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788491690788

- Cervell, M. J. (2018). The Use of Force against International Terrorrism: Everything Changes, Nothing Remains Still. *Paix et Sécurité Internationales,* 6, 47-65. http://dx.doi.org/10.25267/Paix sécur_int.2018.i6.03
- Cervell, M. J. (2018). Un caleidoscopio sobre el uso de la fuerza (el conflicto sirio). *Revista electrónica de estudios internacionales (REEI)*, 36. http://www.reei.org/index.php/revista/num36/articulos/caleidoscopio-sobre-uso-fuerza-conflicto-sirio
- Dinstein, Y. (2002). Computer Network Attacks and Self-Defense. *International law studies*, *76*(20), 99-119. Disponible a: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1397&context=ils
- Dinstein, Y. (2005). *War, Aggression and Self-Defence* (4ª ed.). Cambridge: Cambridge University Press.
- Dörr, O. (2019). Use of force, Prohibition of. *The Max Planck Encyclopedia of Public International Law*. http://opil.ouplaw.com
- Dutra, M. (2017). Uso de la Fuerza: ¿Conflicto entre la prohibición de su uso y la validez de la legítima defensa preventiva en el contexto de la lucha contra el terrorismo organizado?. *Política y Estrategia*, 45-87. https://doi.org/10.26797/rpye.v0i129.71
- Felipe, A., Serebrenik, S., Fernández, N. i Martínez-Vargas, J. R. (2019). *Robótica, Armas y Derecho Internacional*. Tirant lo Blanch. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788413135656
- Fernández, A. F., Ortega, J. M., Forcada, I., Sánchez, Á., Ballesteros, V. i Martínez, M. (2022). *Curso de Derecho Internacional Público* (2ª ed.). Tirant lo Blanch. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788411472296
- Franck, T. M. (1970). Who Killed Article 2(4)? Changing Norms Governing the Use of Force by States. *The American Journal of International Law*, *64*(5), 809-837. https://doi.org/10.2307/2198919
- Fuentes, X. (2014). La prohibición de la amenaza y del uso de la fuerza por el derecho internacional. *Araucaria, 16*(32), 255-267. https://revistascientificas.us.es/index.php/araucaria/article/view/779
- Gervais, M. (2012). Cyber Attacks and the Laws of War. *Berkeley Journal of International Law, 40*, 525-579. https://doi.org/10.15779/Z38R66C
- Gill, T. D. i Ducheine P. A. (2013). Anticipatory Self-Defense in the Cyber Context. *International Law Studies, 89*, 438-471. https://digital-commons.usnwc.edu/ils/vol89/iss1/6/

- Gray, C. (2008). *International Law and the Use of Force* (3ª ed.). Oxford University Press. https://doi.org//10.1093/law/9780198808411.001.0001
- Green, J. A. (2011). Questioning the Peremptory Status of The Prohibition of the Use of Force. *Michigan Journal of International Law, 32*(2), 215-257. https://repository.law.umich.edu/mjil/vol32/iss2/1
- Greenwood, C. (2011). Self-Defence. *Max Planck Encyclopedias of International Law*. https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e401
- Hernández, A. (2000). Uso de la fuerza en el derecho internacional: aplicación en conflictos internos. *Agenda internacional, 7*(15), 161-181. https://revistas.pucp.edu.pe/index.php/agendainternacional/article/view/7272
- Jamnejad, M., i Wood, M. (2009). The principle of non-intervention. *Leiden Journal of International Law, 22*(2), 345-381. https://doi.org/10.1017/S0922156509005858
- Joyner, C. C. i Lotrionte C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law, 12*(5), 825–865. https://doi.org/10.1093/ejil/12.5.825
- Juste, J., Castillo, M., i Bou, V. (2018). Lecciones de Derecho Internacional Público (3ª ed.). Tirant lo Blanch. Disponible a: https://biblioteca-tirant-com.eu1.proxy.openathens.net/cloudLibrary/ebook/info/9788491906650
- Kuru, H. (2017). Prohibition of use of force and cyber operations as "force". *Journal of Learning and Teaching in Digital Age, 2*(2), 46-53. https://dergipark.org.tr/en/pub/joltida/issue/55467/760088
- Pastor, J. A. (2013). *Curso de Derecho Internacional Público y Organizaciones Internacionales* (17ª ed.). Tecnos.
- Rafighdoust, H. (2018). *The right of self-defense against cyber attacks by states and non-state actors.* [Tesi doctoral, Universitat Autònoma de Barcelona]. Tesis Doctorals en Xarxa (TDX). http://hdl.handle.net/10803/666857
- Ronzitti, N. (2006). The Expanding Law of Self-Defence. *Journal of Conflict & Security Law, 11*(3), 343–359. http://www.jstor.org/stable/26294445
- Roscini, M. (2010). World Wide Warfare - *Jus Ad Bellum* and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law, 14*, 85-130. https://ssrn.com/abstract=1683370
- Roscini, M. (2014). *Cyber operations and the Use of Force in International Law*. OUP Oxford.
- Ruys, T. (2014). The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?. *American Journal of International Law, 108*(2), 159-210. https://doi.org/10.5305/amerjintelaw.108.2.0159

- Sánchez, L. I. (2002). Una cara oscura del Derecho Internacional: legítima defensa y terrorismo internacional. *Cursos de derecho internacional y relaciones internacionales de Vitoria-Gasteiz,* 1, 217-266. Disponible a: https://www.ehu.eus/documents/10067636/10678077/2002-LuisIgnacio-Sanchez-Rodriguez.pdf
- Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law, 37*, 886-937. https://ssrn.com/abstract=1603800
- Schmitt, M. N. (2010). Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts. Dins National Research Council (ed.), *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (151 a 178). https://doi.org/10.17226/12997.
- Schmitt, M. N. (2011). Cyber Operations and the Jus Ad Bellum Revisited. *Villanova Law Review, 56*, 569-606. https://ssrn.com/abstract=2184850
- Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (2a ed.). Cambridge University Press.
- Sharp, W. G. (1999). *Cyberspace and the use of force*. Aegis Research Corporation.
- Silver, D. B. (2002). Computer network attack as a use of force under article 2(4) of the United Nations Charter. Dins Schmitt, M. N. i O'Donnell, B. T. (ed.), *Computer network attack and International Law* (74-97). https://digital-commons.usnwc.edu/ils/vol76/iss1/21/
- Tsagourias, N. (2012). Cyber Attacks, Self-Defence and the Problem of Attribution. *Journal of Conflict and Security Law, 17*(2), 229–244. https://ssrn.com/abstract=2538271
- Waxman, M. C. (2011). Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of international Law, 36*(2), 421-459. http://hdl.handle.net/20.500.13051/6629
- Waxman, M. C. (2011). Cyber Attacks as 'Force' Under UN Charter Article 2(4). *International Law Studies, 87*(1), 43-57. https://scholarship.law.columbia.edu/faculty_scholarship/847
- Wood, M. (2013). "The International Law on the Use of Force. What Happens in Practice?", *Indian Journal of International Law, 53*, 345-367. https://legal.un.org/avl/pdf/ls/Wood_article.pdf

2. Article periodístic

- Moore, H., i Roberts, D. (2013, abril 23). *AP Twitter hack causes panic on Wall Street and sends dow plunging*. The Guardian. Visitat al 7 de març de 2023, de: https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall