DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN DIRITTI E TUTELE NEI MERCATI GLOBALIZZATI

XXXVII CICLO

Il regime giuridico delle *cyber operations* nel diritto internazionale

Tutor: Prof.ssa Marina Castellaneta

Candidato: Giuseppe Gallo

Anno Accademico 2023/2024

INDICE

Introduzione

Capitolo I

L'applicabilità del diritto dei conflitti armati ai *computer network attacks*

Capitolo II

Le norme e i principi che regolano la condotta dei belligeranti

Capitolo III

Lo *status* giuridico degli attori coinvolti nella pianificazione ed esecuzione di attacchi informatici in contesti di conflitto armato

INTRODUZIONE

1. Definizione di attacco informatico

Negli ultimi anni si discute sempre più spesso, nella dottrina internazionalistica, di "guerra informatica" (c.d. *cyberwarfare*) e della possibilità di farvi fronte o con le norme di diritto internazionale attualmente in vigore, opportunamente interpretate e adattate, oppure introducendone di nuove[1].

Il presupposto è la crescente dipendenza degli Stati e dei loro servizi pubblici essenziali, come quelli relativi alla distribuzione energetica, alle telecomunicazioni, ai servizi finanziari e alle stesse strutture militari, da sistemi informatici connessi alla rete[2].

A ben guardare, negli ultimi decenni, le reti informatiche sono apparse tutt'altro che impenetrabili, mettendo così in luce la presenza di nuovi rischi per la sicurezza degli Stati[3]. Le infrastrutture fondamentali di ogni Stato risultano, infatti, oramai sotto la costante minaccia di quelli che vengono definiti «attacchi informatici»[4].

Con l'espressione «attacchi informatici», secondo la definizione fornita nel 1999 dal Dipartimento della Difesa americano, si deve intendere: «*any operations to*

[1] L. M. J. Boer, *International Law As We Know It. Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship*, Cambridge, 2021; F. Delerue, *Cyber Operations and International Law*, Cambridge, 2020; H. H. Dinniss, *Cyber Warfare and the Laws of War*, Cambridge, 2012; S. Haataja, *Cyber Attacks and International Law on the Use of Force*, London, 2020; K. Kittichaisaree, *Public International Law of Cyberspace*, Heidelberg, 2017; H. Lahmann, *Unilateral Remedies to Cyber Operations*, Cambridge, 2020; P. A. Palojarvi, *A Battle in Bits and Bytes: Computer Network Attacks and the Law of Armed Conflict*, Helsinki, 2009; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015; J. C. Woltag, *Cyber Warfare*, Cambridge, 2014.

[2] C. Focarelli, *Trattato di diritto internazionale*, Torino, 2015, p. 1828.

[3] O. A. Hathaway, *The Law of Cyber-Attack*, in *California Law Review*, 2012, p. 822 ss.

[4] *Ibidem*.

disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves»[5].

Per quanto concerne i potenziali autori di simili attacchi, la possibilità diffusa di accesso ad Internet fa sì che con pochi strumenti a disposizione anche piccoli Stati, organizzazioni non statali, gruppi terroristici e persino singoli individui possono minacciare le infrastrutture critiche di uno Stato, come il suo sistema sanitario, bancario o di distribuzione dei beni primari[6].

Anche le conseguenze di siffatti attacchi meritano particolare attenzione. Questi, invero, possono rivelarsi di un'entità tale, in termini di danni materiali a beni e strutture, da essere a tutti gli effetti paragonabili ad attacchi militari convenzionali[7]. Peraltro, delle volte, un attacco cibernetico può mettere in ginocchio un intero Paese ancora più di un attacco condotto con armi convenzionali, determinandone la totale paralisi[8]. Tuttavia, detti attacchi possono raggiungere un obiettivo militare anche senza provocare la perdita di vite umane o alcun danno fisico[9]. Gli effetti prodotti da un attacco cibernetico possono, inoltre, non essere immediati, ma manifestarsi dopo un lungo arco temporale, rendendo in tal modo complesso determinare con certezza la portata dell'operazione[10].

In termini di modalità tecniche, gli attacchi cibernetici, diversamente da quelli convenzionali, possono essere sferrati a bassissimo costo, da un numero pressoché illimitato di utenti, la cui identità risulta assai difficile (se non impossibile) da

---

[5] United States Department of Defence, *An Assessment of International Legal Issues in Information Operations*, maggio 1999, p. 1 ss.

[6] È proprio la facilità di accesso ad Internet, in termini di costi e modalità, a modificare in maniera sostanziale i tradizionali rapporti di forza internazionali fondati sulla potenza militare ed economica, determinando l'asimmetria delle guerre informatiche. G. T. Merlo, *Il Dominio degli Spazi: Il cosmo, la cyberwar, la guerra futura*, in *La Comunità internazionale*, 2010, p. 546.

[7] A. Bufalini, *Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico*, in A. Tanzi, A. Lanciotti (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2011, p. 407.

[8] C. C. Joyner, C. Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, in *European Journal of International Law*, 2001, p. 842 ss.

[9] S. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, in *Berkley Journal of International Law*, 2008, p. 198 ss.

[10] *Ibidem*.

individuare[11]. Tali attacchi possono anche essere effettuati da località remote (c.d. *remote warfare*) e in preparazione oppure in concomitanza di un attacco armato convenzionale[12].

Non sorprende, dunque, che il c.d. ciberspazio sia oggi considerato come un quinto teatro di guerra in aggiunta a terra, mare, aria e spazio extra-atmosferico[13]. La crescente militarizzazione di tale dimensione si riflette non solo nell'incorporazione delle operazioni informatiche nelle dottrine militari di molti Paesi, ma anche nella creazione di unità specializzate in operazioni informatiche (offensive e difensive) all'interno delle loro forze armate[14].

Ora, nel diritto internazionale il fenomeno degli attacchi informatici può essere osservato da diversi punti di vista. In primo luogo, ci si può porre sul piano dello *jus in bello* e, quindi, affrontare i problemi di non poco conto sollevati dall'impiego delle tecnologie informatiche nei conflitti armati contemporanei[15]. In secondo luogo, si può porre il problema di stabilire se un attacco condotto per via telematica ricade nell'ambito di applicazione delle regole in materia di *jus ad bellum*.

In tema di *ius in bello* il progresso tecnologico ha portato all'attenzione nuovi mezzi e metodi di conduzione delle ostilità, rappresentati principalmente dai sistemi autonomi di combattimento (c.d. *autonomous weapons system*) e dalle tecnologie informatiche. I primi non sono di per sé illegali, ma devono essere programmati in modo che il loro utilizzo sia conforme al diritto umanitario[16]. Diversamente, per quanto riguarda gli attacchi informatici, risulta più difficile stabilire se questi possano ritenersi vincolati alle regole del diritto bellico. Come osservato nel 2011

---

[11] La varietà di tecniche con cui risulta possibile effettuare un attacco informatico consente ai suoi autori, il più delle volte, di operare in perfetto anonimato. G. T. Merlo, *Il Dominio degli Spazi: Il cosmo, la cyberwar, la guerra futura*, cit., p. 548.

[12] J. D. Ohlin, *Research Handbook on Remote Warfare*, Cheltenham, 2017.

[13] M. Roscini, *World Wide Warfare: Jus ad bellum and the Use of Cyber Force*, in *Max Planck Yearbook of United Nations Law*, 2010, p. 86 ss.

[14] *Ibidem*.

[15] Nella presente indagine, nonostante le note sfumature terminologiche, le espressioni *ius in bello*, diritto internazionale umanitario, diritto internazionale bellico e, ancora, diritto internazionale dei conflitti armati verranno utilizzati come sinonimi per ragioni di praticità.

[16] In argomento, D. Amoroso, *Autonomous Weapons Systems and International Law*, Napoli, 2020; T. Mc Farland, *Autonomous Weapon Systems and the Law of Armed Conflict*, Cambridge, 2020; H. Nasu, R. Mc Laughlin, *New Technologies and the Law of Armed Conflict*, Heidelberg, 2013; D. Saxon (ed.), *International Humanitarian Law and the Changing Technology of War*, Leiden, 2013.

dall'Assemblea generale delle Nazioni Unite, l'applicazione nel contesto informatico del diritto dei conflitti armati, che come è noto è stato concepito in relazione alle armi cinetiche, rappresenta: «*new and unique challenges that will require consultation and cooperation among nations*»[17].

Dal punto di vista dello *ius ad bellum*, i problemi che sorgono sono altrettanto complessi, trattandosi di stabilire se un attacco informatico costituisce una violazione del divieto della minaccia e dell'uso della forza di cui all'art. 2, par. 4, della Carta delle Nazioni Unite, oppure un vero e proprio «attacco armato» ai sensi dell'art. 51 della Carta.

Per affrontare le suindicate questioni si deve necessariamente presumere che il diritto internazionale sia applicabile nel ciberspazio. Per ovvi motivi cronologici, nessun trattato internazionale finora adottato fa esplicito riferimento agli attacchi telematici. Ciononostante, esiste un'ampia prassi statale, espressa in numerose dichiarazioni ufficiali, documenti governativi e manuali militari, che dimostra come la maggioranza degli Stati e delle organizzazioni internazionali, incluso il Comitato internazionale della Croce Rossa, considerino le vigenti norme dello *ius ad bellum* e dello *ius in bello* applicabili alle operazioni informatiche[18]. Parimenti, anche il rapporto del 2013 del Gruppo di esperti governativi sugli sviluppi nel campo dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale (GGE), creato in seno alle Nazioni Unite, ha confermato che il diritto internazionale e, in particolare, la Carta delle Nazioni Unite, sono perfettamente applicabili allo spazio cibernetico[19].

Ammessa, pertanto, l'applicabilità del diritto internazionale alle attività condotte dagli Stati nel *cyberspace*, prima di entrare nel merito delle suelencate questioni giuridiche, a cui la presente analisi intende dare risposta, occorre preliminarmente effettuare talune precisazioni terminologiche.

Con l'espressione «*cyber warfare»* si intendono diversi tipi di reazione, informatica o cinetica, ad attacchi informatici. L'ipotesi più importante e problematica, finora

[17] UN Doc A/66/152, 15 luglio 2011, p. 19.
[18] Come vedremo, il problema non è tanto *se* ma piuttosto *quando* e *come* le norme di diritto internazionale si applicano alle operazioni informatiche e con quali conseguenze.
[19] UN Doc A/68/98, 24 giugno 2013, p. 8.

mai avvenuta, ma comunque prospettata da molteplici Stati, è quella di un attacco informatico sferrato in risposta ad un attacco cibernetico precedentemente subito.

Il concetto di «*cyber warfare*» deve essere distinto tanto da quello di «*electronic warfare*», quanto dalla nozione di «*information warfare*»[20]. Come sottolineato: «*Information warfare is the battlespace use and management of information and communication technology in pursuit of a competitive advantage over an opponent. It is defined as the integrated employment of these core capabilities in concert with specified and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting the own*»[21]. Viceversa, con l'espressione «*electronic warfare*» si fa riferimento a: «*any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy. High power electromagnetic energy can be used as a tool to overload or disrupt the electrical circuitry of almost any equipment that uses transistors, micro-circuits, or metal wiring. Directed energy weapons amplify, or disrupt, the power of an electro-magnetic field by projecting enough energy to overheat and permanently damage circuitry, or jam, overpower, and misdirect the processing in computerized systems*»[22].

La «*cyber war*» deve essere distinta altresì dal c.d. «*cyber crime*»[23]. Di solito, si tende a ridurre gli attacchi informatici a meri crimini individuali commessi in rete[24]. Tuttavia, soltanto se un'operazione informatica viene condotta da individui e non da Stati, essa configura un crimine informatico[25].

In conclusione, oggetto del presente studio sono solamente gli attacchi cibernetici condotti in tempo di guerra. Esulano, pertanto, dalla portata di questo lavoro: a) sia

---

[20] F. Schreier, *On Cyberwarfare*, DCAF Horizon 2015 Working Paper n. 7, p. 19; W. A. Qureshi, *Information Warfare, International Law, and the Changing Battlefield*, in *Fordham International Law Journal*, 2020, pp. 907-908.

[21] *Ibidem*.

[22] JCS, Joint Doctrine for Electronic Warfare, Washington D.C., GPO, 7 April 2000.

[23] S. Brenner, *Cybercrime, Cyberterrorisme and Cyberwarfare*, in *Revue Internationale de Droit Pénal*, 2006, p. 453 ss.; J. Clough, *Principles of Cybercrime*, Cambridge, 2010.

[24] C. Focarelli, *Trattato di diritto internazionale*, cit., p. 1833.

[25] Di rilievo, in materia di criminalità informatica, è la Convenzione di Budapest del 2001 sul crimine informatico, conclusa nell'ambito del Consiglio d'Europa ma aperta anche a Stati terzi, e in vigore dal 1° luglio 2004. La citata Convenzione esclude però dal suo campo di applicazione le operazioni informatiche condotte dagli Stati.

quelle operazioni informatiche effettuate, in tempo di pace, ai fini di spionaggio[26], le quali costituiscono una grave violazione della sovranità statale dello Stato vittima laddove comportino un'intrusione non autorizzata nell'infrastruttura informatica ubicata nel territorio di detto Stato[27]; b) sia le operazioni informatiche di disturbo – come le campagne di disinformazione effettuate in assenza di un conflitto armato – che costituiscono, qualora attribuibili ad uno Stato, una violazione del principio di non intervento negli affari interni[28].

2. Il significato del termine «forza» ai sensi dell'art. 2, par. 4, della Carta delle Nazioni Unite

Prima dell'entrata in vigore della Carta delle Nazioni Unite, gli Stati godevano di un'ampia libertà di ricorrere alla forza bellica[29]. Era, infatti, opinione diffusa e non controvertibile che la guerra fosse sempre ammessa e dovesse essere disciplinata dall'ordinamento internazionale – tramite le regole proprie del diritto bellico – soltanto rispetto alle sue modalità di svolgimento[30].

Una prima restrizione al diritto illimitato di ricorrere alle armi si ebbe solamente tra la fine del XIX secolo e gli inizi del XX secolo, con la Convenzione dell'Aia del

[26] Lo spionaggio può essere, in genere, economico, industriale, politico o militare.

[27] P. B. M. J. Pijpers, *Influence Operations in Cyberspace and the Applicability of International Law*, Cheltenham, 2023; B. Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*: *International Law, International Relations and Diplomacy*, NATO CCD COE Publications, Tallinn, 2013, p. 189 ss.

[28] A. Bonfanti, *Attacchi cibernetici in tempo di pace: le intrusioni nelle elezioni presidenziali statunitensi del 2016 alla luce del diritto internazionale*, in *Rivista diritto internazionale*, 2019, p. 694 ss.; T. Moulin, *Reviving the Principle of Non-Intervention: The Path Forward*, in *Journal of Conflict and Security Law*, 2020, p. 423 ss.; B. Sanders, *Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections*, in *Chinese Journal of International Law*, 2019, p. 1 ss.; S. Watts, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in J. D. Ohlin (ed.), *Cyber War: Law and Ethics for Virtual Conflicts*, Oxford, 2015, p. 249 ss.

[29] Per un'accurata ricostruzione storica del divieto della minaccia e dell'uso della forza nei rapporti fra Stati, si veda: A. Verdebout, *Rewriting Histories of The Use of Force: The Narrative of "Indifference"*, Cambridge, 2021.

[30] In quest'ottica, la guerra poteva essere intrapresa tanto come reazione alla violazione di un diritto, quanto per il perseguimento di interessi non giuridicamente protetti. Essa veniva considerata un mezzo strumentale alla soluzione delle controversie internazionali, in particolare di quelle politiche, nonché un fattore di mutamento giuridico legittimo.

1899 relativa alla soluzione pacifica delle controversie[31] e la Convenzione dell'Aia del 1907 sulla limitazione dell'uso della forza per il recupero dei debiti contrattuali[32].

Successivamente, di grande rilievo fu il Patto della Società delle Nazioni, il quale affermava il principio del rispetto dell'integrità territoriale e dell'indipendenza politica dei Membri della Società da ogni eventuale aggressione esterna compiuta da un altro Membro (art. 10)[33].

Degni di nota risultano, poi, il Protocollo di Ginevra del 1924[34] e il Patto Briand-Kellogg dell'agosto 1928, dal nome dei due Ministri che ne assunsero l'iniziativa[35]. Quest'ultimo, che si componeva di soli tre articoli, gettò le basi giuridiche per i futuri processi di Norimberga e di Tokyo, dal momento che sanciva la rinuncia alla guerra come strumento di politica nazionale e ne condannava il ricorso come mezzo per la soluzione delle controversie internazionali[36].

È però con la Carta delle Nazioni Unite, entrata in vigore il 24 ottobre 1945, che il divieto dell'utilizzo (nonché della semplice minaccia) della forza si è decisamente imposto sul piano internazionale. Sotto l'influsso della Carta, invero, il divieto in commento ha non solo consolidato il proprio carattere di norma consuetudinaria, ma ha anche assunto l'efficacia di principio fondamentale dell'intero impianto normativo internazionale, tanto da essere sovente indicato quale sicura espressione di un precetto di diritto imperativo[37].

---

[31] La Convenzione, all'art. 1, prevedeva che le Potenze firmatarie convenissero nel compiere tutti gli sforzi necessari a prevenire, nella misura del possibile, l'utilizzo della forza nelle relazioni fra Stati.

[32] La Convenzione vietava sì il ricorso alla forza bellica per il recupero di debiti contrattuali dovuti da uno Stato nei confronti dei cittadini di un altro Stato, ma solo nelle ipotesi in cui lo Stato debitore non si rifiutasse di sottoporre la controversia ad arbitrato (art. 1, par. 2).

[33] Il Patto, concluso nel 1919, sanciva il dovere di risolvere pacificamente le controversie, imponendo agli Stati di sottoporre le stesse a decisione arbitrale, oppure al Consiglio della Società delle Nazioni.

[34] Nel Preambolo del summenzionato Protocollo si riconosceva la «solidarietà dei membri della comunità internazionale» e si bandiva la guerra in quanto chiara «violazione di tale solidarietà».

[35] R. Lesaffer, *Kellogg-Briand Pact (1928)*, in *MPEPIL*, 2010.

[36] Seppure con riserve che ne ridimensionavano notevolmente l'impatto sul diritto internazionale, al Patto aderirono ben cinquantasette Paesi, ossia la maggior parte degli Stati della comunità internazionale di allora.

[37] Tale norma – contenente, peraltro, un obbligo *erga omnes* – vincola, pertanto, tutti gli Stati della comunità internazionale, non soltanto quelli divenuti membri delle Nazioni Unite. La sua veste di regola essenziale della Carta è stata affermata dalla Corte internazionale di giustizia nella sentenza

Sul piano dei rapporti tra fonti, la natura cogente della proibizione si manifesta in termini di inderogabilità, determinando l'invalidità di qualsiasi trattato che abbia per oggetto un utilizzo della forza ad essa contrario[38]. Sul piano della responsabilità internazionale, invece, ne deriva l'impossibilità di invocare una qualunque causa di esclusione dell'illecito allo scopo di giustificare la sua violazione[39].

Non manca chi, a seguito delle molteplici guerre che si sono succedute a partire dalla fine del secondo conflitto mondiale, si è detto scettico in merito all'effettiva validità del divieto in parola[40]. Tuttavia, la sua persistente vigenza si evince dal fatto che tutti gli Stati sostengono l'illiceità dell'impiego della forza militare, protestando fermamente quando un altro Stato fa a questa illegittimamente ricorso[41].

L'art. 2, par. 4, della Carta stabilisce, come è noto, che «i Membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale oppure l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite».

In dottrina si è ampiamente dibattuto circa l'esatta portata della disposizione. Sebbene la formula si presti, nel complesso, ad esprimere una nozione abbastanza stringente del divieto in questione, essa lascia, comunque, spazio ad alcuni dubbi interpretativi[42].

La norma, a ben vedere, circoscrive l'operatività della proibizione alle «relazioni internazionali»[43]. Di conseguenza, secondo l'interpretazione corrente, essa riguarda

---

inerente alle *Attività armate nel territorio del Congo* (Corte internazionale di giustizia, 19 dicembre 2005, *Democratic Republic of Congo v. Uganda*, par. 148).

[38] Convenzione di Vienna sul diritto dei trattati del 23 maggio 1969, art. 53.

[39] In presenza di "gravi violazioni" del divieto in oggetto, tutti gli Stati sono tenuti a rispettare i previsti obblighi di non riconoscimento e non assistenza nei confronti dell'autore di tali violazioni, oltre che legittimati a invocare la sua responsabilità e farne valere le conseguenze.

[40] T. M. Franck, *Who Killed Article 2(4)? or: Changing Norms Governing the Use of Force by States*, in *American Journal of International Law*, 1970, p. 809 ss.

[41] Oltretutto, quando uno Stato ricorre alla forza presuppone la sussistenza del divieto dal momento che si preoccupa sistematicamente di fornire motivazioni giuridiche al comportamento posto in essere. Esso è ben consapevole che la forza bellica, in principio, è illecita e che tale illiceità limita significativamente la sua condotta in termini di ampiezza e durata delle operazioni militari.

[42] M. Arcari, *Uso della Forza*, in *Diritto on line Treccani Enciclopedia Italiana*, 2014, p. 7.

[43] R. Kolb, *Ius contra bellum, Le droit international relatif au maintien de la paix*, Bruxelles, 2003, p. 167.

le sole ipotesi di ricorso alla forza tra Stati e costoro ne sono gli unici destinatari[44]. Sono, pertanto, esclusi dal suo ambito di applicazione quei fenomeni di ricorso alla forza confinati all'interno del territorio dello Stato (disordini interni, nonché vere e proprie guerre civili[45]), i quali possono, ad ogni modo, assumere rilievo nel caso in cui vengano qualificati dal Consiglio di sicurezza come eventi minacciosi per la pace e la sicurezza internazionale ai sensi del capitolo VII della Carta[46]. Viceversa, risulta coperta dal divieto sia la forza rivolta contro i corpi di truppa lecitamente stanziati nel territorio statale, sia quella usata contro la sede della rappresentanza diplomatica di uno Stato estero[47].

L'art. 2, par. 4, nel vietare la minaccia o l'impiego della forza militare, precisa come il divieto abbia per oggetto tanto la forza rivolta contro l'integrità territoriale o l'indipendenza politica di un qualunque Stato, quanto quella usata in qualsiasi altra maniera incompatibile con le finalità delle Nazioni Unite[48]. Segue che, forme di intervento armato non dirette contro l'integrità territoriale o l'indipendenza politica di un altro Stato[49], se in contrasto con gli scopi contemplati dall'art. 1 della Carta, saranno nondimeno vietate[50].

L'art. 2, par. 4, proibisce non solamente l'utilizzo della forza, ma anche la semplice minaccia[51]. Tuttavia, non sempre risulta agevole determinare cosa possa intendersi

---

[44] In altri termini deve trattarsi di forza esercitata nell'ambito territoriale di altri Stati, oppure in spazi non soggetti alla sovranità di alcuno, come l'alto mare.

[45] In questi casi l'impiego della forza da parte dello Stato è pressoché diretto al mantenimento dell'ordine pubblico entro il proprio territorio, oppure contro gli insorti.

[46] La prassi del Consiglio, soprattutto quella successiva alla caduta del muro di Berlino, fornisce numerosi esempi nei quali l'organo in discorso, a termini del capitolo VII della Carta, ha autorizzato gli Stati membri a intervenire nel contesto di guerre civili, per garantire l'assistenza umanitaria e la salvaguardia delle popolazioni civili coinvolte oppure, ancora, per assicurare la realizzazione di un mandato di *peace-keeping*.

[47] Le sedi diplomatiche, pur essendo interamente sottoposte alla sovranità dello Stato territoriale (con i limiti del regime delle immunità derivanti dal diritto internazionale), costituiscono una chiara espressione dell'attività sovrana dello Stato nazionale all'estero. Un attacco specificamente diretto contro di esse (che superi una certa soglia di gravità) può, dunque, secondo noi, essere considerato alla stregua di un attacco armato.

[48] N. Schrijver, *Article 2, Paragraphe 4*, in J. P. Cot, A. Pellet, M. Forteau (sous la direction de), *La Charte des Nations Unies. Commentaire article par article*, vol. I, Paris, 2005, p. 125.

[49] S. K. N. Blay, *Territorial Integrity and Political Independence*, in *MPEPIL*, 2010.

[50] O. Dörr, *Use of Force, Prohibition of*, in *MPEPIL*, 2019.

[51] Vedi: N. Stürchler, *The Threat of Force in International Law*, Cambridge, 2009, p. 1 ss.; A. Kleczkowska, *Threats of Force and International Law. Practice, Responses and Consequences*, London, 2023, p. 6 ss.

con quest'ultima espressione[52]. La Corte internazionale di giustizia (CIG), nella controversia tra Nicaragua e Stati Uniti, ha escluso che la messa a punto di un notevole livello di militarizzazione da parte di uno Stato possa essere considerata una minaccia della forza nei confronti dei Paesi vicini, non essendo previsti dal diritto consuetudinario vincoli al livello di armamento di ciascuno Stato[53].

Un problema particolare si è posto, inoltre, per le armi nucleari. A tale proposito, la Corte – nel parere consultivo del 1996 – ha affermato la simmetria esistente tra le nozioni di "uso" e di "minaccia" presenti nel testo della norma, nel senso che se in un caso specifico un utilizzo della forza è illecito, illecita ne sarà pure la minaccia[54]. Alla luce di tale criterio, è stato escluso che la politica di dissuasione nucleare possa integrare una minaccia della forza[55].

Da ultimo, la norma non specifica se la forza la cui minaccia o il cui utilizzo sono proibiti sia solamente quella di tipo militare o, al contrario, anche quella avente natura economica oppure politica. Sia dall'interpretazione sistematica e storica della Carta, che dalla prassi si ricava – e si ammette generalmente in dottrina[56] – che si tratta soltanto della forza bellica, perpetrata mediante ricorso alle armi[57]. Misure di coercizione economica o politica saranno, invece, sicuramente illecite se impiegate per interferire negli affari interni di un altro Stato[58].

---

[52] Non configura una minaccia ricadente nel divieto in esame l'esercizio di un diritto, quale può essere, per esempio, il passaggio inoffensivo di navi da guerra attraverso uno stretto internazionale (Corte internazionale di giustizia, 9 aprile 1949, *Corfu Channel Case*, *United Kingdom of Great Britain and Northern Ireland v. Albania*, par. 30).

[53] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), *Merits*, 1986, in ICJ *Reports*, par. 269.

[54] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, *Advisory Opinion*, 1996, in ICJ *Reports*, par. 47-48.

[55] M. Wood, *Use of Force, Prohibition of Threat*, in *MPEPIL*, 2013.

[56] V. Starace, *Uso della forza nell'ordinamento internazionale*, in *Enciclopedia Giuridica*, vol. XXXII, Roma, 1994, p. 3.

[57] È noto come, durante la Conferenza di San Francisco che portò all'adozione della Carta delle Nazioni Unite, una proposta avanzata dal Brasile mirante ad estendere il divieto dell'uso della forza alle pressioni economiche fu respinta. Inoltre, nelle altre disposizioni in cui la Carta usa il termine forza, esso è accompagnato dalla precisazione che si tratta di forza armata (art. 44; Preambolo, par. 7).

[58] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), cit., par. 202-209.

Una volta individuata la tipologia di forza vietata dalla Carta delle Nazioni Unite, occorre ora chiedersi, ai fini della nostra indagine, se un attacco informatico possa essere ricompreso nell'ambito di applicazione del suesposto divieto.

3. Attacchi informatici come violazione del divieto della minaccia e dell'uso della forza armata

Secondo alcuni autori, si deve dubitare che un attacco telematico, quale che sia la sua entità, possa configurare un uso della forza proibito, non comportando vittime dirette[59]. Il più delle volte un simile attacco costituirebbe, pertanto, un reato informatico, anche gravissimo, perseguibile penalmente a livello nazionale[60].
Tali autori muovono dal presupposto che anche a voler ammettere che un attacco cibernetico possa effettivamente qualificarsi come una violazione dell'art. 2, par. 4, della Carta delle Nazioni Unite, i consueti criteri di attribuzione della condotta si rivelano scarsamente praticabili nella dimensione del ciberspazio e, di conseguenza, resta assai difficile imputare con certezza e tempestività il comportamento illecito allo Stato autore della violazione[61].
A nostro giudizio, una siffatta impostazione non appare condivisibile. Se risulta complesso identificare l'esecutore materiale di un attacco informatico e provare che nella sua condotta sia convolto, direttamente o indirettamente, un determinato Stato, individuare la collocazione geografica del terminale da cui l'attacco è stato lanciato non è, comunque, impossibile[62]. Specifici programmi informatici consentono, inoltre, di risalire non soltanto alla macchina ed al soggetto che ha sferrato l'attacco, ma altresì all'entità governativa che lo ha commissionato ed al tipo di rapporto

[59] D. B. Hollis, *Why States Need an International Law for Information Operations*, in *Lewis & Clark Law Review*, 2007, p. 1041.
[60] J. Goldsmith, *How Cyber Changes the Laws of War,* in *European Journal of International Law*, 2013, p. 132.
[61] *Ivi*, p. 131.
[62] N. Tsagourias, M. Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, in *European Journal of International Law*, 2020, p. 967.

sussistente tra questa e l'individuo da cui l'attacco è partito[63]. In taluni casi, peraltro, potrebbero essere gli Stati stessi ad assumersi la paternità dell'operazione[64].

Secondo altri autori, invece, un attacco informatico non potrebbe mai raggiungere la soglia dell'uso della forza poiché, per sua natura, non rientrerebbe nella nozione classica di arma (c.d. *instrument-based approach*)[65].

Tale circostanza, come vedremo, non si può escludere a priori[66]. Se, in passato, la forza armata è stata associata per lo più a mezzi e metodi di conduzione delle ostilità convenzionali, oggi, questa visione deve ritenersi ampiamente superata, altrimenti talune particolari tipologie di armi, quali, per esempio, quelle chimiche o quelle batteriologiche, non sarebbero coperte dal divieto, in quanto non suscettibili di produrre una forza di tipo cinetico.

Pertanto, la suesposta tesi – la quale si basa, quindi, su una concezione classica di uso della forza, cioè sulla tipologia di arma impiegata[67] – deve essere respinta. Del resto, come ribadito dalla Corte internazionale di giustizia nel caso riguardante la liceità dell'impiego delle armi nucleari, le norme in materia di *ius ad bellum* «*do not refer to specific weapons*»[68].

Secondo un diverso orientamento, un attacco cibernetico sarebbe espressione di un uso della forza vietato solo sulla base delle infrastrutture colpite[69]. In altri termini, affinché detto attacco si possa definire contrario all'art. 2, par. 4, della Carta, è

---

[63] C. Antonopoulos, *State Responsibility in Cyberspace*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 71.

[64] A. Bufalini, *Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico*, in A. Tanzi, A. Lanciotti (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, cit., p. 431.

[65] Tra i fautori di questo approccio: D. E. Graham, *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 2010, p. 90.

[66] In questo senso anche Dinstein, per il quale: "*cyber must be looked upon as a new means of warfare – in other words, a weapon: no less and no more than other weapons*". Y. Dinstein, *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, in *International Law Studies*, 2013, p. 280.

[67] S. G. Handler, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, in *Standford Journal of International Law*, 2012, p. 227.

[68] Corte internazionale di giustizia, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 39.

[69] C. C. Joyner, C. Lotrionte, *Information Warfare as International Coercion: Elements of a Legal Framework*, cit., p. 855.

necessario che, indipendentemente dal suo grado di offensività, esso sia rivolto contro infrastrutture vitali dello Stato nemico (c.d. *target-based approach*)[70].

Anche quest'ultima lettura deve però essere rifiutata, non essendovi, sul piano internazionale, una definizione condivisa ed accettata di «infrastruttura critica»[71]. Se, per un verso, tale lettura ha il pregio di prendere in considerazione la centralità dei sistemi informatici nelle società moderne, per altro verso, essa impone, allo stesso tempo, la necessità di stabilire con esattezza quali infrastrutture nazionali devono essere considerate come essenziali, operazione tutt'altro che semplice in mancanza di un attuale *consensus* tra gli Stati[72].

Inoltre, la suddetta impostazione porta inevitabilmente ad includere nella portata del divieto talune tipologie di attacchi telematici che difficilmente sembrano potervi rientrare, per il semplice fatto che tali attacchi abbiano ad oggetto infrastrutture fondamentali dello Stato avversario[73]. Ad esempio, è stato sostenuto che un attacco informatico ai mercati finanziari o ai sistemi bancari di uno Stato potrebbe ritenersi una violazione dell'art. 2, par. 4, della Carta Onu, pur non comportando alcun danno materiale a persone o cose[74].

Tale tesi non ci pare, tuttavia, adeguatamente ragionata e dimostrata[75]. Simili attacchi telematici, non comportando danni fisici e tangibili a persone o cose, potrebbero concretizzare, semmai, forme di coercizione politica o economica e,

---

[70] E. T. Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, in *Stanford Journal of International Law*, 2002, p. 226.

[71] Lo *United States Patriot Act* del 2001 definisce alla stregua di infrastrutture critiche: «*any systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*». Ancora, la Commissione dell'Unione Europea definisce tali: «*those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments*». EU Commission, *Green Paper on a European Program on Critical Infrastructure Protection*, 17 November 2005, p. 20.

[72] H. Lahmann, *Unilateral Remedies to Cyber Operations*, cit., p. 24.

[73] *Ibidem*.

[74] W. G. Sharp, *Cyberspace and the Use of Force*, Virginia, 1999, p. 102.

[75] Risulta pacifico, infatti, che non si possa ammettere un'estensione del divieto della minaccia o dell'uso della forza armata fino ad includere anche la coercizione economica e politica. D. Bowett, *International Law and Economic Coercion*, in *Virginia Journal of International law*, 1975, p. 245.

conseguentemente, costituire una violazione dell'integrità territoriale o dell'indipendenza politica dello Stato colpito[76].

Viceversa, buona parte della dottrina ritiene che, qualora un attacco telematico causi effetti del tutto simili, se non più gravi, a quelli che si sarebbero potuti verificare attraverso il ricorso a mezzi e metodi di conduzione delle ostilità tradizionali, tale attacco non possa che essere qualificato come una violazione dell'art. 2, par. 4, della Carta delle Nazioni Unite[77]. Questi autori muovono dal presupposto che il testo della norma non prevede alcuna distinzione in merito allo strumento attraverso cui l'uso della forza armata debba, in concreto, realizzarsi e, di conseguenza, non è immaginabile una sua lettura tale da limitarne l'ambito di applicazione alle sole armi esistenti all'epoca della stesura della Carta[78].

A nostro parere, quest'ultimo approccio teorico – fondato, dunque, sulle possibili conseguenze distruttive di un attacco cibernetico su persone o cose (c.d. *effect-based approach*) – deve essere preferito. Esso resta non soltanto quello più richiamato in dottrina[79] ma, come si evince da diverse dichiarazioni, sembra anche quello maggiormente condiviso dagli Stati.

Il governo federale tedesco ha affermato nel 2021, ad esempio, che: «*Whenever scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it would constitute a breach of art. 2 para. 4 UN Charter*»[80]. Una posizione analoga è stata assunta altresì da Belgio, Australia, Nuova Zelanda, Francia, Paesi Bassi, Regno Unito, Stati Uniti, Canada, Brasile, Giappone, Corea del Sud, Argentina e Italia[81].

---

[76] T. A. Morth, *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, in *Case Western Reserve Journal of International Law*, 1998, pp. 592-597.

[77] R. Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, in *Journal of Conflict and Security Law*, 2012, p. 212.

[78] D. B. Silver, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in *International Law Studies*, 2002, p. 84.

[79] M. N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, pp. 914-915; M. Waxman, *Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011, pp. 433-435.

[80] Vedi: on-the-application-of-international-law-in-cyberspace-data.pdf (auswaertiges-amt.de).

[81] Per le rispettive posizioni dei suelencati Stati: Use of force - International cyber law: interactive toolkit (ccdcoe.org).

Se la valutazione degli effetti distruttivi dell'operazione costituisce il solo criterio determinante per stabilire quando un attacco informatico possa essere qualificato come una violazione del divieto della minaccia o dell'uso della forza armata, risulta allora chiaro che, nella maggior parte dei casi, tali attacchi non costituiranno forme di violenza bellica, ma potranno, al limite, essere considerati alla stregua di forme di violenza economica o politica[82].

Ad ogni modo, quando un attacco telematico è capace di provocare danni materiali a persone o cose in misura analoga a quanto farebbe un attacco effettuato con armi tradizionali, questo potrà dirsi sicuramente contrario all'art. 2, par. 4, della Carta delle Nazioni Unite. Si pensi, a titolo di esempio, all'ipotesi in cui uno Stato tramite un attacco cibernetico riesca a manomettere il sistema di controllo del traffico aereo nemico, causando la caduta di un aeroplano e la morte dei suoi passeggeri.

In conclusione, l'art. 2, par. 4, della Carta non è stato immaginato per applicarsi agli attacchi informatici, inesistenti nel 1945[83]. La norma parla di «forza» – per tale intendendosi, come detto, la sola forza di tipo militare – ma non di conseguenze della stessa[84]. Poiché si ritiene che gli effetti siano il miglior parametro per stabilire il corretto significato del termine in parola, risulta ovvio che gli attacchi telematici suscettibili di produrre danni fisici equiparabili, per dimensioni e gravità, a quelli provocati da un impiego della forza "tradizionale", saranno coperti dal divieto, al pari di quanto accade, ad esempio, per gli attacchi radiologici, biologici o nucleari[85]. Come opportunamente evidenziato da Roscini: "*Those worried that, by qualifying seriously disruptive cyber operations as a use of force, the risk of inter-state conflicts will increase should be reassured: indeed, a use of force, in itself, is not sufficient to entitle the victim state to react in self-defence, unless it is serious enough to amount to an armed attack*"[86].

---

[82] M. Roscini, *Cyber Operations as a Use of Force*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 236.
[83] M. Benatar, *The Use of Cyber Force: Need for Legal Justification?*, in *Göttingen Journal of International Law*, 2009, p. 380.
[84] E. Pobjie, *Prohibited Force. The Meaning of "Use of Force" in International Law*, Cambridge, 2024, p. 132.
[85] M. Benatar, *The Use of Cyber Force: Need for Legal Justification?*, cit., p. 389.
[86] M. Roscini, *Cyber Operations as a Use of Force*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 250.

4. Nozione di «attacco» rilevante ai fini della legittima difesa

È controverso se il divieto di cui all'art. 2, par. 4, della Carta delle Nazioni Unite copra tutti gli usi della forza bellica o soltanto quelli più gravi.

Secondo una parte della dottrina, la lettera della norma si presta a coprire anche le forme di coercizione militare di entità inferiore rispetto alla vera e propria guerra[87].

Al contrario, buona parte della dottrina esclude dall'ambito di applicazione della disposizione gli atti violenti extraterritoriali che non superano una certa «soglia di gravità», come, ad esempio, le uccisioni mirate, i sequestri di persona, gli interventi non autorizzati da parte delle forze di polizia in territorio altrui, oppure a bordo di navi o di aeromobili stranieri, e le operazioni militari circoscritte o temporanee[88].

A nostro giudizio, quest'ultima tesi è certamente da preferire, in quanto la prassi sembra confermare che tali usi *minoris generis* della forza bellica ricadono piuttosto sotto i regimi convenzionali relativi agli spazi aerei e marittimi, oppure riguardano la norma consuetudinaria posta a protezione della sovranità territoriale degli Stati[89].

Ciò premesso, occorre fare attenzione a non confondere la gravità che concerne la violazione dell'art. 2, par. 4, della Carta, cioè la soglia della forza armata rilevante ai fini della proibizione, dalla gravità dell'«attacco armato» subito da uno Stato ai fini della legittima difesa[90]. Un conto, infatti, è stabilire quali usi della forza rientrano nell'art. 2, par. 4, della Carta, altro conto è statuire a quali usi della forza, tra quelli rientranti nel divieto, è possibile rispondere in legittima difesa[91].

---

[87] T. Ruys, *The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from Un Charter Article 2(4)?*, in *American Journal of International Law*, 2014, p. 159 ss.

[88] M. E. O'Connell, *The Prohibition on the Use of Force*, in N. D. White, C. Henderson (eds.), *Research Handbook of International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum*, Cheltenham, 2013, p. 102.

[89] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), cit., par. 111-112.

[90] I. Brownlie, *International Law and the Use of Force by States*, Oxford, 1963, pp. 361-368.

[91] J. Klabbers, *Intervention, Armed Intervention, Armed Attack, Threat to Peace, Act of Aggression, and Threat or Use of Force: What's the Difference?*, in M. Weller, *The Oxford Handbook of the Use of Force in International Law*, Oxford, 2016, pp. 488-506.

Affinché uno Stato possa agire in legittima difesa è necessario che si sia verificato o sia in corso un «attacco armato»[92]. Tuttavia, non sempre risulta agevole stabilire che tipo di «attacco armato» giustifichi l'esercizio del diritto alla legittima difesa[93]. Nella sentenza di merito sul caso delle *attività militari e paramilitari in e contro il Nicaragua*, la Corte internazionale di giustizia ha distinto tra «forme più gravi» e «forme meno gravi» di utlizzo della forza armata ai fini della legittima difesa[94]. Secondo la Corte, non ogni violazione dell'art. 2, par. 4, costituisce un «attacco armato», ma soltanto quelle violazioni che – per la loro portata e i loro effetti (*scale and effects*) – possono ritenersi sufficientemente serie[95]. La Corte, dunque, esclude che meri incidenti di frontiera, benché violazioni dell'art. 2, par. 4, possano rappresentare «attacchi armati» suscettibili di dare luogo al diritto alla legittima difesa[96]. Analogamente, la fornitura di armamenti, nonché l'addestramento e l'assistenza logistica agli insorti operanti nel territorio di un altro Stato, costituiscono un uso della forza vietato ma non, allo stesso tempo, un «attacco armato» ai sensi dell'art. 51 della Carta delle Nazioni Unite[97].

Con riferimento al contesto cibernetico, come opportunamente suggerito da Corten: «*En définitive, il faut rappeler l'absence de précédent dans lequel un Etat aurait officiellement dénoncé une cyber-attaque comme constituant un recours à le force prohibé par l'article 2, par. 4, de la Charte, et a fortiori une agression armée au*

[92] K. Zemanek, *Armed Attack*, in *MPEPIL*, 2013.

[93] La nozione di «attacco armato» non è definita nel testo dell'art. 51 o altrove all'interno della Carta. Oltretutto, il testo francese e quello inglese della disposizione differiscono in quanto impiegano espressioni diverse (*agression armée/armed attack*). In realtà, i concetti di «aggressione» e «attacco armato» sono ben distinti e impiegati nella Carta in due contesti differenti: il primo nell'ambito del sistema di sicurezza collettivo come situazione che legittima il Consiglio di sicurezza ad avvalersi dei poteri conferitigli dal capitolo VII (art. 39), il secondo come circostanza che legittima gli Stati ad invocare il loro diritto alla legittima difesa (art. 51). Come affermato da autorevole dottrina la nozione di «aggressione» pare inclusiva di quella di «attacco armato». Y. Dinstein, *War, Aggression and Self-Defence*, Cambridge, 2011, p. 196 ss.

[94] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, cit., par. 191.

[95] Con il termine «portata» ci si riferisce alla quantità di forza armata utilizzata, inclusa la sua durata, nonché l'estensione dell'area geografica coinvolta, mentre con l'espressione «effetti» si intende l'entità del danno e la quantità delle vittime causate. T. Ruys, *"Armed Attack" and Article 51 of the UN Charter*, Cambridge, 2010, p. 139.

[96] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, cit., par. 195.

[97] C. Gray, *International Law and the Use of Force*, Oxford, 2000, pp. 54-57.

sens de son article 51. A ce stade, on ne peut que spéculer sur diverses hypothèses et renvoyer à une détermination casuistique»[98].

Nella prassi uno dei casi più noti di attacco informatico è quello avvenuto nell'aprile 2007 ai danni dell'Estonia, con effetti assai gravi alle infrastrutture dell'intero Paese (paralisi per diverse settimane del sistema di riscossione delle imposte, di numerosi siti web governativi, ecc.)[99]. Si sospetta che l'operazione sia partita dal territorio della Russia sebbene non vi siano, ad oggi, prove certe del coinvolgimento da parte del governo di Mosca[100], il quale ha più volte negato la propria responsabilità[101].

Ora, se si guarda agli effetti dell'operazione, stando alle fonti disponibili, l'attacco non ha prodotto alcun danno fisico a persone o cose[102]. Ne consegue che, questo non soltanto non ha raggiunto il livello di forza armata richiesto dall'art. 2, par. 4, della Carta, ma non ha neppure integrato una violazione dell'art. 51 della stessa, non configurando, *a fortiori*, un «attacco armato» ai fini della legittima difesa[103].

Ciò trova, peraltro, conferma nel fatto che l'Estonia, all'epoca, si rivolse alla NATO sostenendo di aver subito un vero e proprio «attacco armato» da parte della Russia, e invocando, così, l'attivazione dell'art. 5 del Trattato Nord Atlantico, in base al quale qualora uno Stato parte contraente sia vittima di un «attacco armato» gli altri Stati membri sono in dovere di intervenire con tutti i mezzi a loro disposizione, compresi quelli militari. Tuttavia, come noto, l'Organizzazione rispose ritenendo che si trattasse, in realtà, di un fenomeno di criminalità informatica e non di un «attacco armato»[104].

Ancora, nel 2010, il virus *Stuxnet*, capace di rendere completamente inoperativo un *software Siemens* installato nelle centrifughe nucleari iraniane di Natanz, si diffuse

---

[98] O. Corten, *Cyber-attaques et Jus Contra Bellum*, in M. Grange, A. T. Norodom (Sous la direction de), *Cyberattaques et droit international. Problèmes choisis*, Paris, 2018, p. 212.

[99] R. Ottis, *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, 2007.

[100] I. Traynor, *Russia accused of unleashing cyberwar to disable Estonia*, *The Guardian*, 17 May 2007.

[101] Wire Reports, *Kremlin denies involvement in cyber-attacks on Estonia*, *The Baltic Times*, 18 May 2007.

[102] C. Focarelli, *Self-defence in cyberspace*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., pp. 259-260.

[103] *Ibidem*.

[104] La vicenda è stata oggetto di un diffuso interesse da parte della dottrina. Per una sua più dettagliata ricostruzione si rinvia a: https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007).

rapidamente in Iran, suscitando il sospetto che a crearlo fossero stati Israele e gli Stati Uniti[105]. Si ritiene che il virus abbia causato ingenti danni alle apparecchiature bersagliate[106]. A tale conclusione è giunto anche l'Istituto iraniano per la scienza e la sicurezza nazionale[107], secondo cui il programma malevolo sarebbe stato in grado di modificare la velocità delle centrifughe in misura tale da causarne la distruzione e impedire, di conseguenza, il corretto funzionamento delle centrali nucleari[108].

Per quanto attiene alla qualificazione giuridica dell'operazione, riteniamo, in questo caso, che l'attacco in parola non possa non configurare una violazione dell'art. 2, par. 4, della Carta, poiché il codice *Stuxnet* è stato intenzionalmente progettato per poter essere utilizzato contro un altro Stato e ha cagionato evidenti danni materiali alle infrastrutture critiche presenti sul territorio di quest'ultimo[109]. Ciononostante, ancorché suscettibile di produrre danni fisici tangibili, questo non ha provocato la perdita di vite umane e, per portata, non costituirebbe un «attacco armato» a norma dell'art. 51 della Carta delle Nazioni Unite[110].

Dai casi appena descritti si evince come taluni attacchi cibernetici non risultano così gravi da violare l'art. 2, par. 4, della Carta Onu, né tantomeno da giustificare una reazione in legittima difesa; altri attacchi informatici, invece, sono abbastanza gravi da violare l'art. 2, par. 4, della Carta Onu, ma non al punto di giustificare una risposta in legittima difesa; altri ancora, infine, potrebbero essere, per conseguenze distruttive, talmente gravi che non solo violerebbero l'art. 2, par. 4, della Carta Onu, ma giustificherebbero altresì una risposta in legittima difesa da parte dello Stato colpito.

---

[105] G. Kessler, *New research confirms Iran's nuclear program was target of Stuxnet worm*, *The Washington Post*, 15 November 2010.

[106] Per quanto riguarda la sofisticatezza dell'attacco e le modalità con cui questo è stato predisposto vedi: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010).

[107] P. Hafezi, *Iran admits cyber-attack on nuclear plants*, *Reuters*, 29 November 2010.

[108] Il *report* prodotto dall'Istituto è rinvenibile al seguente sito: https://isis-online.org/.

[109] Deve essere rigettata la tesi secondo cui l'attacco cibernetico in parola non configurerebbe neppure un illecito internazionale. (K. Ziolkowski, *Stuxnet-Legal Considerations*, CCDCOE, 2012, p. 25). Anche qualora si ritenesse che questo non costituisse affatto un uso della forza proibito, esso sarebbe, invero, comunque qualificabile come un atto contrario al divieto di ingerenza negli affari domestici di un altro Stato.

[110] In senso analogo: P. R. Dev, *Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, in *Texas International Law Journal*, 2015, pp. 399-400.

Poiché per quanto concerne la prima tipologia di attacchi, essi non sono mai «usi della forza», mentre per quanto riguarda viceversa gli ultimi, al momento in cui si scrive, essi non sembrano essersi mai verificati, a nostro parere, si può concludere che alcuni attacchi telematici possono sicuramente risultare sufficientemente gravi da rientrare nell'art. 2, par. 4, della Carta Onu, ma non al punto da ammettere una reazione in legittima difesa[111].

5. *Segue:* Attacchi informatici e legittima difesa

Nonostante sia teoricamente possibile, nessun attacco informatico sinora avvenuto pare aver mai raggiunto la soglia di un «attacco armato» idoneo a consentire il ricorso alla legittima difesa ai sensi dell'art. 51 della Carta delle Nazioni Unite[112]. Un attacco cibernetico non coinvolge l'utilizzo della forza fisica (c.d. cinetica) e, come rammentato, gli strumenti impiegati per la sua preparazione ed esecuzione non sono dei mezzi militari in senso tradizionale. Ciononostante, una parte della dottrina ritiene la circostanza secondo cui un simile attacco possa rappresentare un vero e proprio «attacco armato» suscettibile di dar luogo alla legittima difesa, una ipotesi non così remota ed eccezionale[113].

---

[111] La tesi prospettata si pone in contrasto con quanto suggerito dal Manuale di Tallinn secondo cui un attacco informatico potrebbe, per dimensioni ed intensità, ammontare ad un «attacco armato». A proposito del citato Manuale, non ci si può esimere dall'effettuare alcune considerazioni critiche. In particolare, occorre notare che questo non rappresenta un documento ufficiale, ma è il risultato della ricerca di un gruppo di studiosi ed esperti militari. Tale raccolta di norme è priva di efficacia giuridica vincolante. È bene ricordare che i Manuali militari, di norma, non sono mai fonti di diritto, neppure a livello interno, ma semplicemente traducono – sul piano nazionale – quanto convenuto in trattati internazionali spesso di assai difficile interpretazione. Questi, consistenti talvolta in pubblicazioni dei ministeri della difesa contenenti specifiche regole di condotta per i membri delle forze armate, interpretano il diritto internazionale dei conflitti armati alla luce delle riserve apposte dallo Stato o delle dichiarazioni interpretative da questo effettuate al momento della firma o della ratifica delle convenzioni internazionali. Inoltre, delle volte, dettano importanti regole nelle materie in cui lo *ius in bello* appare essere particolarmente lacunoso. Ad ogni modo, tali strumenti normativi non hanno valore giuridico vincolante. C. Garraway, *The Use and Abuse of Military Manuals*, in *Yearbook of International Humanitarian Law*, 2004, pp. 425-440; E. A. Partington, *Manuals on the Law of Armed Conflict*, in *MPEPIL*, 2016.

[112] O. Corten, *Cyber-attaques et Jus Contra Bellum*, cit., p. 212.

[113] Y. Dinstein, *Computer Network Attacks and Self-Defense*, in *International Law Studies*, 2002, p. 99 ss.; H. B. Robertson, *Self-Defense against Computer Network Attack under International Law*, in *International Law Studies*, 2002, p. 121 ss.; D. Delibasis, *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*, in *Peace Conflict and Development: An Interdisciplinary Journal*, 2006, p. 2 ss.; L. Grosswald, *Cyberattack Attribution Matters under*

Tale impostazione non è al riparo da critiche[114]. Laddove si accolga la siffatta tesi, invero, non si può prescindere dall'effettuare alcune considerazioni in merito alle difficoltà che si incontrerebbero nell'applicare al contesto cibernetico le condizioni richieste per ricorrere alla legittima difesa.

L'art. 51 della Carta Onu dispone, come è noto, che: «Nessuna disposizione della presente Carta pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso in cui abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese dai Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo la presente Carta, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quella azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale».

La disposizione – afferente al diritto internazionale consuetudinario[115] – ammette, dunque, tanto la legittima difesa individuale[116], come tale intendendosi quella a cui

---

Article 51 of the U. N. Charter, in *Berkeley Journal of International Law*, 2011, p. 1151 ss.; N. Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, in *Journal of Conflict and Security Law*, 2012, p. 229 ss.; T. D. Gill, *Anticipatory Self-Defense in the Cyber Context*, in *International Law Studies*, 2013, p. 438 ss.

[114] La posizione secondo cui un attacco cibernetico può essere interpretato alla stregua di un «attacco armato» a norma dell'art. 51 della Carta delle Nazioni Unite è rinvenibile anche nel Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica. Il suddetto Manuale ha, tuttavia, un'importanza relativa. Si tratta, infatti, di una mera codificazione privata, adottata su impulso della NATO, che affronta espressamente i problemi connessi alla guerra informatica, ma la cui corrispondenza al diritto internazionale consuetudinario è stata variamente contestata. Questo è, dunque, un atto giuridicamente non vincolante, riferibile unicamente al gruppo di studiosi che lo ha predisposto, provenienti, peraltro, in grandissima parte da taluni Stati occidentali. Per una serie di critiche sulle norme codificate nel predetto Manuale vedi soprattutto: R. Liivoja, T. McCormack, *Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello*, in *Yearbook of International Humanitarian Law*, 2012, p. 45 ss.; L. J. M. Boer, *Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace*, in *Amsterdam Law Forum*, 2013, p. 4 ss.; D. Fleck, *Searching for International Rules Applicable to Cyber Warfare - A Critical First Assessment of the New Tallinn Manual*, in *Journal of Conflict and Security Law*, 2013, p. 331 ss.; J. d'Aspremont, *Cyber Operations and International Law: An Interventionist Legal Thought*, in *Journal of Conflict and Security Law*, 2016, p. 575 ss.

[115] International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), cit., par. 14.

[116] Si noti che la legittima difesa è oggetto di un diritto, non di un obbligo. Ne discende che, lo Stato vittima dell'attacco armato può decidere di non rispondere con la forza e così anche gli Stati terzi, nonostante la richiesta proveniente dallo Stato leso. C. Greenwood, *Self-Defence*, in *MPEPIL*, 2011.

ricorre lo Stato che ha subito l'«attacco armato», quanto la legittima difesa collettiva[117], che è quella, invece, alla quale ricorrono uno o più Stati terzi in soccorso dello Stato attaccato.

Essendo un diritto connaturato con l'esistenza stessa degli Stati, la legittima difesa non necessita di alcuna autorizzazione da parte del Consiglio di sicurezza delle Nazioni Unite[118]. Tuttavia, lo Stato che agisce in legittima difesa ha il dovere di portare a conoscenza del Consiglio le misure adottate[119]. Tale obbligo procedurale, che ha natura convenzionale e non consuetudinaria, ha lo scopo di tenere informato il Consiglio di sicurezza, affinché lo stesso possa verificare la legittimità dell'azione unilaterale intrapresa[120].

Anche se il testo dell'art. 51 non ne fa cenno, la risposta armata giustificata a titolo di legittima difesa è soggetta – nelle sue modalità di svolgimento – ai requisiti della necessità, della proporzionalità e dell'immediatezza[121].

---

[117] Per quanto concerne la legittima difesa collettiva, non è richiesto, come talvolta si è erroneamente sostenuto, che questa sia prevista da un trattato *ad hoc*. Ad ogni modo, nulla esclude che un obbligo specifico di agire in legittima difesa collettiva possa essere assunto attraverso un trattato, bilaterale o multilaterale. Ciò che è necessario, invece, è la richiesta esplicita di intervento *ex post*, oppure il previo consenso da parte dello Stato che ha subito l'attacco armato. In altri termini, gli Stati diversi da quello aggredito non possono – unilateralmente – accertare la sussistenza dell'attacco armato e, conseguentemente, decidere di intervenire. Spetta, quindi, solamente allo Stato aggredito affermare di avere subito un attacco armato. In questo senso si è pronunciata la Corte internazionale di giustizia nella sentenza sulle *Piattaforme petrolifere* del 2003 (International Court of Justice, *Oil Platforms, Islamic Republic of Iran v. United States of America*, *Judgment*, in ICJ *Reports*, 2003, par. 51).

[118] C. Henderson, *The Use of Force and International Law*, Cambridge, 2018, p. 123 ss.

[119] La legittima difesa è soggetta ad un termine finale, nel senso che essa deve cessare non appena il Consiglio di sicurezza delle Nazioni Unite abbia preso tutte le misure necessarie per mantenere o ripristinare la pace e la sicurezza internazionale. Si deve trattare, beninteso, di misure efficaci, cioè tali da rendere superflua la continuazione dell'azione unilaterale intrapresa. Risulta chiara, pertanto, la volontà dei redattori della Carta Onu di attribuire un carattere sussidiario e temporaneo all'azione in legittima difesa dello Stato attaccato rispetto all'azione del Consiglio. L. Zanardi, *La legittima difesa nel diritto internazionale*, Milano, 1972, p. 263.

[120] L'eventuale inadempienza del suindicato obbligo non comporta, si badi, l'illiceità dell'azione in legittima difesa, ma costituisce, comunque, una violazione della Carta Onu (finora mai sanzionata). Ad ogni modo, la circostanza che gli Stati non abbiano adempiuto l'obbligo di portare a conoscenza del Consiglio di sicurezza le misure adottate in legittima difesa potrebbe servire a sostenere che il diritto in parola sia stato invocato in modo pretestuoso. O. Corten, *Le droit contre la guerre*, Paris, 2007, p. 707 ss.

[121] I suindicati criteri appartengono tutti al diritto internazionale consuetudinario. E. Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 2006, p. 4 ss.

In base al requisito della necessità il ricorso alla forza armata non deve oltrepassare lo scopo meramente difensivo per il quale esso è consentito[122]. In altre parole, tale criterio sta ad indicare che lo Stato attaccato non ha avuto, nelle particolari circostanze del caso, altro mezzo a propria disposizione, se non quello di ricorrere alla forza militare per fermare l'attacco armato[123].

Il limite della proporzionalità, viceversa, impone che la forza bellica ammessa sia solamente quella necessaria a respingere l'attacco armato e ripristinare lo *status quo ante*[124]. La regola non richiede però un'identità di contenuto e intensità tra l'attacco subito e l'azione difensiva attuata, quanto piuttosto che quest'ultima non ecceda nello scopo legittimo di fermare e respingere l'attacco armato[125].

Infine, il criterio dell'immediatezza – proposto da Roberto Ago nel corso dei lavori per la codificazione del diritto della responsabilità internazionale – impone che la forza bellica possa essere impiegata solo mentre l'attacco armato si stia verificando o, comunque, entro un lasso di tempo ragionevole dal suo concreto verificarsi[126]. L'importanza del carattere tempestivo della reazione militare risiede nel fatto che una risposta dilazionata nel tempo appare molto più simile ad una rappresaglia che ad un esercizio della legittima difesa[127].

Ora, nel contesto informatico il requisito della necessità sembrerebbe impedire il ricorso alla legittima difesa, la quale assumerebbe, così, un ruolo del tutto residuale. Nella quasi totalità delle ipotesi, infatti, lo Stato vittima dell'operazione potrebbe adottare misure non implicanti l'uso della forza per respingere l'attacco informatico

[122] C. O'Meara, *Necessity and Proportionality and the Right of Self-Defence in International Law*, Oxford, 2021, p. 42 ss.
[123] Due elementi caratterizzano, quindi, la necessità: l'urgenza della situazione e l'assenza di misure alternative pacifiche utili ad ottenere il risultato voluto. J. G. Gardam, *Necessity, Proportionality, and the Use of Force by States*, Cambridge, 2004, p. 4 ss.
[124] E. Cannizzaro, *Il principio della proporzionalità nell'ordinamento internazionale*, Milano, 2000, p. 275 ss.
[125] E. Crawford, *Proportionality*, in *MPEPIL*, 2011.
[126] M. Roscini, *Legittima difesa*, in *Treccani Diritto on line*, 2015.
[127] P. Gargiulo, *Uso della Forza (Diritto internazionale)*, in *Enciclopedia del Diritto*, *Annali V*, Milano, 2012, p. 1407.

in corso. Questo potrebbe, ad esempio, impedire l'accesso alle reti o ai sistemi colpiti attraverso l'adozione di misure di difesa informatica passiva[128].

Per quanto riguarda il limite della proporzionalità, si pone il problema di stabilire se un attacco telematico giustifichi soltanto una reazione cinetica, oppure anche una reazione informatica[129]. A nostro parere, sembra ragionevole supporre che un attacco cibernetico con effetti – ossia con danni a persone o cose – equivalenti a quelli di un attacco armato convenzionale possa giustificare sia una reazione cinetica, che una reazione informatica, pur potendo quest'ultima suscitare non poche perplessità, essendo la legittima difesa per definizione una risposta armata in senso tradizionale. Tuttavia, in mancanza di una prassi degli Stati il problema resta aperto.

Da ultimo, per quanto concerne il requisito dell'immediatezza, anche tale criterio risulta particolarmente inadeguato al contesto cibernetico. Per sua stessa natura un attacco telematico potrebbe, infatti, produrre i propri effetti soltanto dopo un certo periodo di tempo da quando è stato sferrato, oppure al verificarsi di determinate condizioni. Inoltre, sia la verifica delle conseguenze distruttive dell'operazione, che la raccolta delle prove ai fini dell'imputazione del comportamento illecito ad un certo Stato, potrebbero richiedere un *quantum* di tempo più o meno lungo.

In conclusione, come evidenziato da O'Connell "*To date, the problem of Internet security has been the domain of international law scholars with expertise in use of force questions. They have sent the message that the Internet may be protected through military force or the threat of military force, analogizing to Cold War deterrence strategy. Doing so has required strained analogies of cyber-attacks to conventional kinetic attacks. The Internet is now far less secure than before there was a Cyber Command or a NATO CCDCOE. It is time, therefore, to turn to cyber*

[128] Per sicurezza informatica passiva normalmente si intendono quelle tecniche e quegli strumenti informatici di tipo difensivo il cui obiettivo sia quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati aventi natura riservata.

[129] F. Grimal, J. Sundaram, *Cyber Warfare and Autonomous Self-Defense*, *Journal on the Use of Force and International Law*, 2017, p. 329.

dis armament and a focus on peaceful protection of the Internet. The motto should be: a good cyber defence is good cyber defence"[130].

A tale proposito deve essere guardata certamente con favore l'istituzione di *Computer emergency response team* (CERT) in seno alla maggior parte degli Stati della comunità internazionale, quali per esempio lo *Slovenian Computer Emergency Response Team*, il *Singapore Cyber Emergency Response Team*, lo *Hong Kong Computer Emergency Response Team Coordination Center* e il *Cyber Security Center and of Norway*. Si tratta di speciali enti pubblici, costituiti prevalentemente da personale civile e creati allo scopo di tutelare la sicurezza nazionale in ambito informatico principalmente attraverso l'adozione di misure di sicurezza informatica attiva[131].

6. Il possibile ruolo del Consiglio di sicurezza nel mantenimento della pace di fronte alle nuove minacce *cyber*

Alla luce di quanto precede, da ultimo, appare doveroso chiedersi quando un attacco informatico possa costituire una «minaccia alla pace», una «violazione della pace» o, ancora, un «atto di aggressione» ai sensi dell'art. 39 della Carta delle Nazioni Unite, consentendo, pertanto, al Consiglio di sicurezza di intervenire a termini del capitolo VII[132]. In altre parole, ci si domanda se un simile attacco possa, in concreto, configurare una situazione rientrante in una delle tre categorie indicate e, in caso di

[130] M. O'Connell, *Cyber Security without Cyber War*, in *Journal of Conflict and Security Law*, 2012, p. 209.
[131] https://www.oxfordreference.com/.
[132] In merito alle numerose discussioni in tema di cybersecurity avvenute in seno alle Nazioni Unite a partire dalla fine del secolo scorso si rimanda a: C. Henderson, *The United Nations and the Regulation of Cyber-security*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 465 ss.; L. Kello, *Cyber Threats*, in S. Daws, T. G. Weiss (eds.), *The Oxford Handbook on the United Nations*, Oxford, 2018, p. 528 ss.; P. Gargiulo, *Nazioni Unite, cybersecurity e diritto internazionale*, in O. Porchia, M. Vellano (a cura di), *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future. Liber Amicorum in onore di Edoardo Greppi*, Torino, 2023, p. 53 ss.

risposta affermativa, quali misure provvisorie o coercitive possano essere adottate dall'organo in questione al fine di mantenere o ristabilire la pace violata[133].

Nella prassi il Consiglio di sicurezza sinora non ha mai fatto ricorso alla formula «aggressione», neppure quando, come nel caso della guerra di Corea o della prima guerra del Golfo, indubbiamente si trattava di circostanze qualificabili come veri e propri «atti di aggressione»[134]. I riferimenti ad «atti di aggressione» sono contenuti per lo più in risoluzioni non adottate in base al capitolo VII della Carta, nelle quali l'organo in parola si è limitato a condannare certi comportamenti da parte degli Stati e ad evidenziarne la pericolosità per la sicurezza internazionale[135].

La sussistenza di una «violazione della pace»[136] è stata invece accertata, seppur raramente, in occasione del conflitto di Corea nel 1950[137], dell'occupazione militare argentina delle Isole Falkland-Malvinas nel 1982[138], della guerra tra Iran e Iraq nel 1987[139] e, infine, dell'invasione irachena del Kuwait nel 1990[140].

Al contrario, il Consiglio di sicurezza ha considerato in termini di «minaccia alla pace» situazioni assai eterogenee fra loro e sempre più di carattere interno agli Stati (laddove ovviamente suscettibili di avere ripercussioni all'esterno)[141]. Se, in tempi di guerra fredda, il predetto organo è stato assai prudente nel ritenere una

---

[133] Relativamente al concetto di pace contemplato nel testo dell'art. 39, come sostenuto dalla migliore dottrina, si deve intendere l'assoluta assenza di confitti interstatali o interni. B. Conforti, C. Focarelli, Le *Nazioni Unite*, Padova, 2017, p. 232.

[134] In dette ipotesi il Consiglio ha preferito parlare piuttosto di «violazione della pace» e nel caso dell'invasione turca di Cipro del Nord nel 1974 si è, addirittura, limitato a ritenere l'evento una «minaccia alla pace».

[135] Ricordiamo, soprattutto, la risoluzione n. 386 del 1976 che condannava gli atti aggressivi della Rhodesia del Sud contro il Mozambico e la risoluzione n. 527 del 1982 inerente agli atti aggressivi del Sud Africa ai danni del Lesotho.

[136] Con l'espressione «violazione della pace» si è soliti far riferimento ad un conflitto internazionale o non internazionale che, diversamente dalla «minaccia alla pace», è in corso di svolgimento, pur non raggiungendo (ove si tratti di un conflitto fra Stati) il livello più grave dell'atto di aggressione. A tale formula il Consiglio finora non ha mai fatto riferimento in occasione di conflitti armati interni, per i quali ha sempre preferito invocare una «una minaccia alla pace». M. Wood, *Peace, Breach of*, in *MPEPIL*, 2009.

[137] Consiglio di sicurezza, risoluzione n. 82 del 25 giugno 1950.

[138] Consiglio di sicurezza, risoluzione n. 502 del 3 aprile 1982.

[139] Consiglio di sicurezza, risoluzione n. 598 del 20 luglio 1987.

[140] Consiglio di sicurezza, risoluzione n. 660 del 2 agosto 1990.

[141] A differenza dell'«aggressione» e della «violazione della pace», la «minaccia alla pace» non è necessariamente caratterizzata dalla presenza di operazioni militari o di un illecito internazionale. Tale espressione si presta, di conseguenza, ad inquadrare i più disparati comportamenti di uno Stato. P. J. Kooijmans, *The Enlargement of the Concept Threat to the Peace*, in R. J. Dupuy (ed.), *The Development of the Role of the Security Council*, Dordrecht, 1993, pp. 111-121.

determinata situazione come «minaccia alla pace», l'accertamento di «minacce alla pace» da parte dello stesso è divenuto, in seguito, sempre più frequente[142].

Sono state dichiarate come «minaccia alla pace», ad esempio, un'estesa politica di apartheid (Rhodesia del Sud nel 1966 e Sud Africa nel 1977), l'oppressione violenta di una minoranza (come nel caso della repressione irachena dei curdi e degli Sciiti nel 1991), la violazione grave e sistematica dei diritti umani e del diritto umanitario (Albania nel 1997 e Kosovo nel 1999), il genocidio e l'uccisione di civili in Ruanda nel 1994, certe situazioni post-conflittuali (Bosnia 1991), taluni flussi incontrollati di rifugiati (Liberia nel 1993), la commissione di attentati terroristici (Istanbul 2003 e Madrid 2004), la deposizione di un Capo di Stato eletto democraticamente e l'instaurazione di un regime autoritario (Haiti 1994), la mancata protezione della popolazione civile durante un'insurrezione o disordini interni (Libia nel 2011), fenomeni di pirateria (Somalia nel 2008), la proliferazione di armi chimiche (Siria nel 2013) e, più di recente, la diffusione del virus Ebola in Africa occidentale nel 2014[143].

Ora, data la vaghezza e l'elasticità che caratterizzano la nozione di «minaccia alla pace» e tenuto conto, inoltre, dell'ampia discrezionalità di cui gode il Consiglio nell'accertamento di tale condizione, non vi è dubbio che, almeno nei casi più gravi, un attacco cibernetico possa essere qualificato come una «minaccia alla pace»[144] e, di conseguenza, legittimare il suddetto organo ad adottare misure anche armate[145], oppure autorizzare gli Stati membri ad intraprendere una misura armata altrimenti illecita[146].

---

[142] E. de Wet, M. Wood, *Peace, Threat to*, in *MPEPIL*, 2009.

[143] La prassi dimostra l'ampiezza delle situazioni considerate dal Consiglio come una «minaccia alla pace». N. Krisch, *Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression*, *Article 39*, in B. Simma, G. Nolte, A. Paulus (eds.), *The Charter of the United Nations: A Commentary*, vol. II, Oxford, 2012, p. 1332 ss.

[144] C. Woltag, *Cyber Warfare*, cit., p. 193.

[145] E. Kodar, *Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello*, in *Baltic Yearbook of International Law Online*, 2009, pp. 924-927; A. Almutawa, *Designing the Organisational Structure of the UN Cyber Peacekeeping Team*, in *Journal of Conflict and Security Law*, 2020, p. 117 ss.; N. Tsagourias, G. Biggio, *Cyber Peacekeeping Operations and the Regulation of the Use of Lethal Force*, in *International Law Studies*, 2022, p. 36 ss.

[146] M. Roscini, *Cyber Operations and the Use of Force in International Law*, cit., p. 110.

Tuttavia, ad oggi, nessun attacco telematico è stato ritenuto suscettibile di turbare la sicurezza internazionale[147]. Per tale motivo, ci sembra maggiormente plausibile, in presenza di un attacco cibernetico costituente una «minaccia alla pace», fra le molteplici misure che possono essere disposte dal Consiglio di sicurezza al fine di ripristinare la pace violata, soffermarci prevalentemente su quelle non implicanti l'uso della forza bellica.

A tal proposito, il Consiglio potrebbe, in primo luogo, imporre agli Stati membri di adottare sanzioni contro lo Stato autore dell'attacco telematico, quali l'embargo (totale o parziale) sul commercio di specifiche tecnologie informatiche[148]. In secondo luogo, questo potrebbe disporre misure sanzionatorie *ex* art. 41 della Carta nei confronti degli individui o delle entità statali responsabili dell'operazione, a prescindere dalla loro qualità di organi dello Stato e dall'esistenza di un loro collegamento con un apparato governativo[149].

7. Piano del lavoro e linee direttrici

Abbiamo sinora esaminato come e quando le regole internazionali che disciplinano il ricorso alla forza nei rapporti fra Stati (c.d. *ius ad bellum*) possano applicarsi alle operazioni informatiche da essi condotte.

Tali norme giuridiche, contenute nella Carta delle Nazioni Unite, devono essere ben distinte da quelle che disciplinano l'impiego della violenza militare tra i belligeranti (c.d. *ius in bello*), di cui ci occuperemo nei prossimi capitoli.

---

[147] H. H. Dinnis, *Cyber Warfare and the Laws of War*, cit., p. 110.

[148] Le decisioni basate sull'art. 41 sono sempre vincolanti per gli Stati membri, i quali sono, quindi, tenuti ad applicare le misure richieste nei confronti dello Stato sanzionato. S. Marchisio, *L'ONU. Il diritto delle Nazioni Unite*, Bologna, 2012, p. 221.

[149] In tempi recenti, misure non implicanti l'uso della forza sono state emanate principalmente nei confronti di enti non statali nel quadro della c.d. lotta al terrorismo. In argomento, V. Gowlland-Debbas (ed.) *United Nations Sanctions and International Law*, The Hague, 2001; M. P. Malloy, *United States Economic Sanctions: Theory and Practice*, The Hague, 2001; J. M. Farrall, *United Nations Sanctions and the Rule of Law*, Cambridge 2007; V. Lowe and others (eds.), *The United Nations Security Council and War: The Evolution of Thought and Practice since 1945*, Oxford, 2008; A. Tzanakopoulos, *Disobeying the Security Council: Countermeasures against Wrongful Sanctions*, Oxford, 2011.

La presente ricerca si basa, infatti, sulla netta demarcazione tra il settore normativo dello *ius ad bellum* e quello del diritto internazionale dei conflitti armati[150].

Sebbene la dicotomia tra i due gruppi di norme sia stata messa in discussione dalla dottrina maggioritaria[151] a seguito dell'entrata in vigore della Carta delle Nazioni Unite e, talvolta, sia stata ritenuta superata, essa è confermata in talune rilevanti decisioni internazionali[152] e resta tuttora presente nel I Protocollo Aggiuntivo del 1977 sulla protezione delle vittime nei conflitti armati internazionali[153].

A nostro giudizio, pertanto, i suindicati sistemi normativi devono restare autonomi, poiché le loro differenze strutturali persistono tutt'oggi.

Il diritto internazionale umanitario si applica, invero, indistintamente a tutte le parti in lotta, a prescindere dal fatto che la loro condotta sia legittima o meno in base a quanto previsto dalle pertinenti regole dello *ius ad bellum*[154]. Al contrario, sulla base delle norme appartenenti allo *ius contra bellum*, le parti in conflitto assumono inevitabilmente una posizione giuridica diversa, dal momento che una di queste si è resa responsabile della loro violazione.

In altri termini, nel diritto umanitario i belligeranti sono titolari dei medesimi diritti e dei medesimi obblighi, a prescindere dalla loro veste di aggressore o aggredito[155]. Ove i belligeranti non fossero uguali davanti alle leggi della guerra e per gli stessi

---

[150] K. Okimoto, *The Distinction and Relationship between Jus ad Bellum and Jus in Bello*, Oxford, 2011, p. 19 ss.

[151] C. Greenwood, *The Relationship between ius ad bellum and ius in bello*, in *Review of International Studies*, 1983, p. 221 ss.; C. Stahn, *Jus ad bellum, jus in bello, jus post bellum? Rethinking the Conception of the Law of Armed Force*, in *European Journal of International Law*, 2006, p. 921 ss; K. L. Yip, *Separation between jus ad bellum and jus in bello as insulation of results, not scopes, of application*, in *The Military Law and the Law of War Review*, 2020, p. 31 ss.

[152] Vedi Corte internazionale di giustizia, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 105; nonché Ethiopia's Central Front Claim Partial Award, 2004, par. 78.

[153] Protocollo (I) sulla protezione delle vittime nei conflitti armati internazionali, aggiuntivo alle Convenzioni del 12 agosto 1949 (Ginevra, 8 luglio 1977), Preambolo, par. 5.

[154] In altre parole, i civili interessati da un conflitto armato necessitano della massima assistenza, indipendentemente dalla circostanza che i belligeranti combattano in conformità o in contrasto con quanto prescritto dalle disposizioni dello *ius contra bellum*. Il diritto internazionale umanitario è, pertanto, impermeabile alle cause del conflitto bellico. M. Sassòli, *International Humanitarian Law*, Cheltenham, 2019, p. 460.

[155] *Ibidem*.

dovessero valere regole e trattamenti differenti, si finirebbe per minare la solidità di tale articolato *corpus* normativo[156].

In accordo a quanto si è appena detto, il presente lavoro di ricerca si propone, attraverso i capitoli che seguono, di esaminare i problemi giuridici posti dal recente fenomeno degli attacchi informatici in relazione al diritto dei conflitti armati. Se con riferimento allo *ius ad bellum* le peculiarità delle operazioni informatiche sono molto spesso sopravvalutate e «*the danger of a cyberwar is greatly overstated*»[157]; al contrario, la necessità di regolamentare il ricorso alle operazioni informatiche, da parte dei belligeranti, come strumento di guerra non convenzionale, è poco dibattuta dalla dottrina internazionalistica.

[156] Il principio di uguaglianza dei belligeranti è uno dei principi basilari del diritto umanitario. Esso è stato codificato nel preambolo del I Protocollo Aggiuntivo del 1977, dove si afferma che «le disposizioni delle Convenzioni di Ginevra del 12 agosto 1949 e del presente Protocollo devono essere pienamente applicate in ogni circostanza a tutte le persone protette da detti strumenti, senza alcuna distinzione sfavorevole fondata sulla natura o l'origine del conflitto armato, o sulle cause invocate dalle Parti in conflitto, o ad esse attribuite». Per un'analisi storico-giuridica dell'affermarsi di tale principio e del suo contenuto si vedano soprattutto: H. Meyrowitz, *Le principe de l'égalité des belligérants devant le droit de la guerre*, Paris, 1970, p. 33 ss.; C. Rousseau, *Le droit des conflits armés*, Paris, 1983, p. 24 ss.

[157] T. Kliem, *You can't cyber in here, this is the War Room! A rejection of the effects doctrine on cyberwar and the use of force in international law*, in *Journal on the Use of Force and International Law*, 2017, p. 368.

CAPITOLO I

L'applicabilità del diritto dei conflitti armati ai *computer network attacks*

Nei paragrafi precedenti ci siamo domandati, in via preliminare, quando un attacco informatico possa configurare una violazione del divieto della minaccia o dell'uso della forza di cui all'art. 2, par. 4, della Carta delle Nazioni Unite o, addirittura, possa costituire un vero e proprio attacco armato idoneo a consentire il ricorso alla legittima difesa. Successivamente, ci siamo chiesti quando un simile attacco possa rappresentare una «minaccia alla pace», una «violazione della pace» o un «atto di aggressione» ai sensi dell'art. 39 della Carta e consentire al Consiglio di sicurezza di adottare le misure previste dal capitolo VII.

Tali questioni devono essere distinte da quelle, ben più complesse, sollevate dal ricorso a strumenti informatici come mezzi e metodi di guerra non convenzionali. È proprio su queste ultime problematiche che il presente lavoro intende soffermarsi. Il fatto che gli attacchi informatici, nella maggior parte dei casi, si affianchino ad operazioni militari tradizionali non impone agli Stati l'esigenza di confrontarsi con il problema della loro qualificazione giuridica secondo le regole proprie dello *ius ad bellum*, essendosi la violazione del divieto dell'uso della forza già concretizzata attraverso l'utilizzo di mezzi e metodi di combattimento convenzionali.

Di conseguenza, i capitoli che seguono sono volti a verificare, attraverso una loro ricostruzione, in che modo i principi e le norme del diritto internazionale umanitario possano applicarsi nel corso di un conflitto armato innescato da un uso della forza tradizionale, ma caratterizzato allo stesso tempo dal ricorrente utilizzo da parte dei belligeranti di *computer network attacks* con finalità di offesa o di difesa.

1. Attacchi informatici e conflitti armati internazionali

Il diritto umanitario si applica solo in tempo di guerra. Condizione indispensabile ai fini dell'applicazione di tale articolato *corpus* normativo è, dunque, la sussistenza di un conflitto armato internazionale o interno[158].

Nella decisione sulla giurisdizione relativa al caso «*Tadić*» del 1995, la Camera d'appello del Tribunale penale internazionale per la *ex* Iugoslavia ha sostenuto che: «*an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State*»[159].

La nozione – largamente condivisa in dottrina – di conflitto armato internazionale fornita dai giudici internazionali si basa sulla presenza di due requisiti irrinunciabili, il primo avente carattere oggettivo e il secondo avente carattere soggettivo[160].

Per quanto riguarda il profilo oggettivo, è necessario che sia raggiunto un certo livello di intensità nello svolgimento degli scontri armati[161].

Non è richiesto, invece, che il conflitto perduri per un determinato arco di tempo[162]. Nel Commentario del Comitato internazionale della Croce Rossa sui Protocolli addizionali alle Convenzioni di Ginevra del 1949 si è precisato, infatti, che la durata del conflitto bellico è priva di rilievo[163]. In senso analogo il Tribunale penale internazionale per la *ex* Iugoslavia, nella sentenza del 1998 relativa al caso «*Prosecutor v. Mucić*», ha affermato che: «*the existence of armed forces between States is sufficient of itself to trigger the application of international humanitarian*

---

[158] Come osservato da una parte della dottrina, con l'entrata in vigore della Carta delle Nazioni Unite, il termine «conflitto armato» ha progressivamente sostituito il concetto di «guerra». K. J. Partsch, *Armed Conflict*, in *EPIL*, 1992, p. 249 ss.

[159] Tribunale penale internazionale per la *ex* Iugoslavia, Camera d'appello, *Prosecutor v. Duško Tadić*, decisione del 2 ottobre 1995, caso n. IT-94-1, par. 70.

[160] E. Crawford, *Armed Conflict, International*, in *MPEPIL*, 2015.

[161] Non sempre risulta agevole stabilire se si è in presenza di un conflitto armato internazionale quando gli scontri tra gli Stati siano a bassa intensità oppure solo sporadici. Di solito, si esclude che singoli incidenti di frontiera possano dare luogo ad un conflitto armato internazionale. International Law Association, *Final Report on the Meaning of Armed Conflict in International Law*, Report of the Seventy-Fourth Conference, The Hague, 2010, p. 9.

[162] La definizione di «conflitto armato» contenuta nella pronuncia relativa al caso *Tadić* non richiede, infatti, la sussistenza di violenze armate prolungate per i casi di scontri tra Stati.

[163] C. Pilloud, *et al.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva, Norwell, MA, USA, 1987, par. 40.

law» e, di conseguenza, non ha alcun rilievo «*how long conflict lasts or how much slaughter takes place*»[164].

Per quanto concerne le condizioni soggettive imprescindibili ai fini dell'esistenza di un conflitto armato internazionale, è essenziale che questo intercorra tra due o più Stati, ossia fra enti dotati di soggettività internazionale[165]. A tal proposito, assume carattere internazionale non solo un conflitto compiuto da forze armate regolari, ma anche quello in cui uno Stato interviene con gruppi armati che agiscono per suo conto e sotto il suo controllo[166].

Un conflitto armato internazionale ha inizio con l'apertura di fatto delle ostilità, a prescindere che la guerra sia stata dichiarata o meno[167]. È altresì irrilevante che i belligeranti non riconoscano uno stato di guerra ognuno nei confronti dell'altro[168], così come la circostanza che un belligerante non abbia riconosciuto formalmente il nemico come Stato, oppure il suo governo[169]. Affinché, quindi, il diritto umanitario possa applicarsi è sufficiente la sussistenza di un conflitto armato tra due o più Stati, a prescindere se questi si considerino o meno coinvolti in uno stato di guerra[170].

Ora, nelle ipotesi di attacchi telematici effettuati in preparazione o in concomitanza di un attacco convenzionale, come accaduto, ad esempio, durante il conflitto russo-georgiano o, ancora, quello russo-ucraino[171], l'applicabilità del diritto umanitario

---

[164] Tribunale penale internazionale per la *ex* Iugoslavia, decisione del 16 novembre 1998, caso n. IT-96-21-T, *Prosecutor v. Delalić, Mucić, Delić e Landžo*, par. 208.

[165] M. Castellaneta, *Conflitti armati (diritto internazionale)*, in *Enc. dir.*, *Annali V*, 2012, p. 324.

[166] Nella sentenza del 2011 relativa al caso «Gotovina» il Tribunale penale internazionale per la *ex* Iugoslavia ha stabilito che se un gruppo armato organizzato agisce per conto e nell'interesse di un altro Stato il conflitto armato assume carattere internazionale, a patto che lo Stato abbia «*a role in organizing, coordinating or planning the military actions of the organized armed group and that State finances, trains, equips or provides operational support to that group*». Tribunale penale internazionale per la *ex* Iugoslavia, *Prosecutor v. Gotovina, Čermak e Martač, Trial Chamber*, decisione del 15 aprile 2011, caso n. IT-06-90-T, par. 1675.

[167] L'obbligo di dichiarare la guerra si ritiene comunemente venuto meno di fronte alla prassi degli ultimi decenni perlopiù caratterizzata da guerre non dichiarate. Sul punto si veda: M. Mancini, *Stato di guerra e conflitto armato nel diritto internazionale*, Torino, 2009.

[168] L'art. 2 «comune» alle Convenzioni di Ginevra del 1949 dispone, invero, che le «Convenzioni si applicano a tutti i casi di guerra dichiarata o a qualunque altro conflitto armato che possa sorgere tra due o più alte Parti Contraenti, anche quando una delle parti non riconosce lo stato di guerra».

[169] C. Greenwood, *Scope of Application of Humanitarian Law*, in T. Fleck (ed.), *The Handbook of International Humanitarian Law in Armed Conflict*, Oxford, 2013, p. 49.

[170] International Law Association, *Final Report on the Meaning of Armed Conflict in International Law*, cit., p. 10.

[171] La strategia militare russa di far precedere o accompagnare con attacchi cibernetici le proprie operazioni belliche è ampiamente nota. Così è stato, ad esempio, nel caso dell'aggressione contro

appare indiscutibile poiché si è già in presenza di scontri armati originati da un uso della forza bellica tradizionale (c.d. cinetica)[172].

Diverso è il caso in cui non vi sia un conflitto armato preesistente e occorra stabilire se un attacco informatico effettuato da uno Stato nei confronti di un altro costituisca, a tutti gli effetti, un «atto di guerra» facendo, pertanto, scattare l'applicazione delle norme di *ius in bello*.

Come correttamente sostenuto dal Comitato internazionale della Croce Rossa, riteniamo che tale questione «*will probably be determined in a definite manner only through future state practice*»[173].

Di conseguenza, ci occuperemo, nella presente trattazione, soltanto delle operazioni cibernetiche sferrate durante un conflitto armato internazionale già esistente e che abbiano un nesso con lo stesso[174].

Le operazioni cibernetiche effettuate in presenza di concomitanti operazioni militari cinetiche possono essere governate dalle regole consuetudinarie e convenzionali del diritto bellico solamente quando riconducibili alla definizione di «attacco» dettata da tali norme[175]. La nozione di «attacco» prevista dalle disposizioni di *ius in bello*

---

l'Ucraina avvenuta nel febbraio 2022. In un rapporto pubblicato nel giugno dello stesso anno, la multinazionale statunitense Microsoft affermava che diversi servizi di *intelligence* militare e civile russi avevano lanciato numerosi attacchi informatici distruttivi mentre le forze armate russe invadevano il Paese. Microsoft, *An overview of Russia's cyberattack activity in Ukraine*, *Special Report: Ukraine*, 17 April 2022.

[172] N. Melzer, *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research, Geneva, 2011, p. 22.

[173] International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, October 2011, p. 37.

[174] Il nesso con il conflitto armato è una circostanza necessaria ai fini dell'applicazione del diritto internazionale umanitario ad una determinata condotta bellica. Le operazioni cibernetiche sferrate dai belligeranti in mancanza di una qualche forma di collegamento con il conflitto non devono ritenersi parte dello stesso, anche se si verificano durante i combattimenti o nel teatro delle ostilità. Dette operazioni cibernetiche saranno soggette unicamente alle norme internazionali che regolano gli attacchi informatici in tempo di pace, cioè al principio di sovranità statale e a quello di non ingerenza negli affari interni di un altro Stato. T. D. Gill, *International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of "Armed" under the Humanitarian Law of Armed Conflict*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., pp. 366-374.

[175] K. Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, in *International Review of the Red Cross*, 2004, p. 3.

differisce da quella contemplata dall'art. 51 della Carta delle Nazioni Unite e non deve essere, pertanto, confusa con quest'ultima[176].

A ben guardare, le norme del diritto bellico non contemplano l'aggettivo «armato» quando si riferiscono agli attacchi condotti da una parte belligerante nei confronti dell'avversario. Tale assenza ha come conseguenza quella di ampliare il contenuto della nozione di «attacco», facendovi rientrare anche quelle azioni ostili non armate che vanno, comunque, a detrimento della parte avversa. Di conseguenza, per poter qualificare un'azione ostile alla stregua di un «attacco» a norma del diritto bellico l'attenzione andrebbe posta non tanto sul fatto che detta azione ostile sia armata, quanto piuttosto sulle sue conseguenze dannose per il nemico.

Ai sensi dell'art. 49 del I Protocollo addizionale alle Convenzioni di Ginevra del 1949, con l'espressione «attacco» si deve intendere ogni «*act of violence against the adversary, whether in offence or in defence*»[177].

Il termine «attacco» contenuto nel testo della disposizione in parola deve essere interpretato in senso ampio, poiché comprensivo di qualsiasi operazione militare, sia difensiva che offensiva[178]. Di conseguenza, affinché una operazione cibernetica possa essere considerata come un «attacco» secondo il diritto internazionale bellico a nulla rileva il fatto che essa sia compiuta a scopo di difesa o di offesa.

Ciò che conta, invece, sono gli effetti prodotti dalla stessa[179]. Qualsiasi operazione militare condotta nei confronti del nemico, infatti, soggiace all'applicazione delle norme dello *ius in bello* solamente qualora suscettibile di provocare la morte o il ferimento di persone oppure, ancora, la distruzione o il danneggiamento di beni[180].

---

[176] M. N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, in K. Ziolkowski (ed.), *4th International Conference on Cyber Conflict. Proceedings*, NATO CCD COE Publications, Tallinn, 2012, p. 283 ss.

[177] N. Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, in *International Law Studies*, 2013, p. 261.

[178] C. Pilloud, *et al.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, cit., par. 1880.

[179] In definitiva, sono le conseguenze distruttive di un'operazione militare e non la sua natura cinetica a determinare la portata del termine «attacco». L'utilizzo di agenti biologici, chimici, radiologici o batteriologici, ad esempio, costituisce un attacco ai sensi del diritto internazionale umanitario anche se non implica l'impiego di alcuna forza fisica.

[180] M. Bothe, K. J. Partsch, W. A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, The Hague, Boston, London, 1982, p. 289.

Ne consegue che possono essere qualificate come «attacco» ai sensi dell'art. 49 del I Protocollo addizionale solamente quelle operazioni cibernetiche suscettibili di determinare, in concreto, i suindicati effetti distruttivi[181]. Le operazioni cibernetiche che non consistono in veri e propri atti di violenza contro l'avversario – come, per esempio, le attività di spionaggio cibernetico – non costituiscono un «attacco» ai sensi di quanto disposto dall'art. 49 del I Protocollo[182].

Tuttavia, nella maggior parte dei casi, gli attacchi telematici lanciati nel corso di un conflitto armato realizzano un vantaggio militare senza comportare danni materiali a persone o cose[183]. In tali ipotesi, appare piuttosto difficile stabilire se anche tali operazioni cibernetiche possano essere ritenute come un «attacco» secondo quanto prescritto dal diritto dei conflitti armati[184]. Si pensi, a titolo di esempio, agli attacchi informatici che si limitano a interrompere la funzionalità dell'infrastruttura colpita senza causare danni materiali[185].

L'opinione prevalente all'interno del gruppo internazionale di esperti che ha redatto il Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica è quella secondo cui in tali situazioni si è in presenza di un «attacco» soltanto laddove il ripristino della funzionalità dell'infrastruttura bersagliata richieda la sostituzione delle sue componenti fisiche e, dunque, si renda necessaria la sua riparazione[186].

Al contrario, secondo una parte minoritaria degli studiosi coinvolti nella redazione del Manuale, anche le operazioni cibernetiche che determinano un significativo malfunzionamento dell'infrastruttura attaccata, senza allo stesso tempo comportare il suo danneggiamento o la sua distruzione fisica, sarebbero da qualificare come atti

[181] M. N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, in *International Law Studies*, 2002, p. 91.
[182] M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, cit., p. 415.
[183] G. Intoccia, *Communications Technology, Warfare, and the Law: Is the Network a Weapon System?*, in *Houston Journal of International Law*, 2006, p. 467 ss.
[184] M. N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, cit., p. 93.
[185] N. Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, cit., p. 262.
[186] M. N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*, cit., p. 418.

di violenza, in quanto, comunque, arrecano un pregiudizio alla controparte, tale da inficiare il suo sforzo bellico[187].

Tale impostazione si basa sulla constatazione che le parti belligeranti generalmente non si limitano soltanto a distruggere o danneggiare fisicamente gli obiettivi militari dell'avversario al fine di conseguire un determinato vantaggio militare[188].

Un vantaggio militare può essere ottenuto, invero, anche semplicemente catturando o neutralizzando un obiettivo militare del nemico, come riconosciuto dall'art. 52, comma 2, del I Protocollo[189]. La norma in parola statuisce che qualunque «attacco» deve essere strettamente limitato agli obiettivi militari la cui distruzione, cattura o neutralizzazione offra un vantaggio militare, presupponendo, così, che anche la sola neutralizzazione possa configurare un «attacco»[190].

A nostro parere, quest'ultimo orientamento deve essere preferito dal momento che escludere le operazioni cibernetiche che limitano o impediscono la funzionalità dell'infrastruttura colpita dalla definizione di «attacco» contemplata dal diritto dei conflitti armati conduce al risultato secondo cui tali operazioni potrebbero essere intenzionalmente dirette contro persone oppure beni civili, indipendentemente dalla partecipazione diretta di questi ultimi alle ostilità.

In conclusione, la definizione di «attacco» riprodotta nel testo dell'art. 49 del I Protocollo del 1977 abbraccia ogni atto di violenza contro l'avversario, sia esso condotto a scopo di difesa o di offesa. Vi rientrano indubbiamente le operazioni cibernetiche suscettibili di cagionare la morte e il ferimento di persone, nonché la distruzione e il danneggiamento di beni, come nel caso di un attacco informatico alla strumentazione di bordo di un veicolo al fine di farlo precipitare. Vi rientrano, poi, le operazioni cibernetiche volte a causare l'inoperatività prolungata o definitiva

---

[187] *Ivi*, p. 419.

[188] Ad esempio, è stato sostenuto che l'interruzione della funzionalità della rete elettrica ubicata in territorio nemico integri gli estremi di un attacco *ex* art. 49 del I Protocollo anche laddove non si verifichi il suo danneggiamento o la sua distruzione fisica. In tal senso: K. Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks*, cit., p. 4.

[189] Neutralizzare un obiettivo militare significa impedirne l'utilizzo da parte dell'avversario senza ricorrere alla sua distruzione materiale. M. Bothe, K. J. Partsch, W. A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, cit., p. 325.

[190] J. C. Woltag, *Cyber Warfare*, cit., p. 207.

dell'infrastruttura bersagliata. Viceversa, non può essere considerata alla stregua di un «attacco» la mera violazione di sistemi informatici avversari, senza che da tale operazione conseguano effetti distruttivi o impedimenti significativi in ordine al loro funzionamento[191].

Secondo Melzer, anche queste ultime operazioni di disturbo sarebbero idonee a far scattare l'applicazione delle regole di *ius in bello* a condizione però che "*[…] they constitute part of the hostilities within the meaning of IHL*"[192]. Tale impostazione si basa sulla considerazione che numerose norme del diritto umanitario proteggono la popolazione civile nei confronti di qualsiasi operazioni militare, comprese quelle operazioni che non rientrano nella nozione di «attacco» ai sensi del I Protocollo.[193]

A nostro avviso, tuttavia, tale tesi non appare condivisibile in quanto queste ultime operazioni cibernetiche non sono capaci di provocare conseguenze dannose per persone o cose e, quindi, non si traducono in un danno materiale significativo[194].

2. Attacchi informatici e conflitti armati non internazionali

Il diritto internazionale non regola allo stesso modo i conflitti armati internazionali e quelli interni[195]. Questi ultimi trovano la loro disciplina nell'art. 3 «comune» alle

[191] International Law Association (ILA) Study Group, *The Conduct of Hostilities and International Humanitarian Law*, *Challenges of 21st Century Warfare*, Final Report, 2016, p. 12.
[192] N. Melzer, *Cyberwarfare and International Law*, cit., p. 27.
[193] Art. 57, comma 1, I PA; art. 51, comma 3, I PA; art. 48 I PA; art. 37 I PA.
[194] Tali operazioni, peraltro, non alterano il funzionamento delle infrastrutture critiche bersagliate in modo da incidere sulla sicurezza nazionale della parte avversa e sulla fornitura di servizi essenziali alla popolazione civile.
[195] Vi sono, dunque, distinti gruppi di norme che regolano l'una e l'altra tipologia di conflitti. La distinzione tra conflitti armati interni e conflitti armati internazionali appare, così, sufficientemente netta ed evidente. Alla prima tipologia appartengono i conflitti tra Stati, mentre alla seconda quelli che si svolgono in un determinato Stato. Al contrario di quanto accaduto per i conflitti armati internazionali, dove la codificazione è piuttosto risalente nel tempo, solo di recente si è assistito ad una codificazione dei conflitti armati non internazionali. I motivi sono semplici. In passato la guerra civile era considerata una questione rientrante nel dominio riservato degli Stati, i quali potevano sopprimere l'insurrezione senza nessuna ingerenza dall'esterno. È solo con lo sviluppo dei diritti fondamentali dell'uomo che questa concezione è venuta meno. Il rispetto della dignità umana, oggi, ha una importanza tale che il suo riconoscimento non può essere soggetto a limiti o restrizioni in base al tipo di attori impegnati nel conflitto. Sebbene tra conflitti armati internazionali e conflitti armati interni, delle volte, possano esservi delle interferenze, tali tipi di conflitti devono essere tenuti ben distinti tra loro. Il principale elemento caratteristico che distingue la disciplina dei conflitti armati internazionali da quella dei conflitti armati interni risiede nel fatto che coloro i quali partecipano alla prima categoria di conflitti sono normalmente ritenuti «combattenti legittimi», con

quattro Convenzioni di Ginevra del 1949 e nel II Protocollo del 1977 dedicato specificamente alla protezione delle vittime dei conflitti armati non internazionali[196]. Come per i conflitti armati internazionali, si applica, inoltre, il regime dei diritti dell'uomo[197] e quello dei crimini di guerra[198].

L'art. 3 «comune» alle Convenzioni di Ginevra del 1949 viene in rilievo in ogni conflitto armato che non abbia carattere internazionale[199] e detta una "disciplina minima" vincolante tanto il governo legittimo, quanto gli insorti[200]. Tale disciplina, sulla base di quanto sostenuto dalla Corte internazionale di giustizia nell'affare Nicaragua contro Stati Uniti nel 1986, ha natura consuetudinaria[201] e si applica sia per i civili, che per gli individui *hors de combat*[202].

L'art. 3 «comune» alle Convenzioni di Ginevra non precisa però quando si possa effettivamente parlare di conflitto armato interno. Nulla dice, invero, la norma in merito alla soglia di violenza bellica richiesta. Sono stati allora fissati una serie di

---

la conseguenza che non possono essere puniti in nessun caso per gli atti di belligeranza compiuti e nelle ipotesi di cattura devono essere qualificati come prigionieri di guerra. Ciò non può dirsi, viceversa, per coloro che prendono parte alla seconda categoria di conflitti, i quali sono soggetti alla potestà punitiva dello Stato nel rispetto delle regole di carattere umanitario. Un conflitto armato interno può assumere due distinte configurazioni. L'ipotesi classica è costituita dalla contrapposizione tra l'autorità di governo precostituita ed un gruppo di insorti. L'altra ipotesi, meno frequente ma pur sempre riscontrabile, si presenta in quelle situazioni in cui sia venuta meno una qualunque autorità statale di riferimento e si assista ad una contrapposizione fra gruppi armati di varia natura. N. Ronzitti, *Diritto internazionale dei conflitti armati*, Torino, 2017, p. 365.

[196] Si noti come il II Protocollo addizionale del 1977 riceve applicazione soltanto se una delle parti in conflitto appartiene al governo costituito. A differenza dell'art. 3 «comune», il II Protocollo non si applica qualora il conflitto bellico abbia luogo tra varie fazioni armate, ma non coinvolga il governo costituito. N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 365.

[197] Occorre tener conto anche per i conflitti armati non internazionali dei diritti dell'uomo. Questi trovano applicazione tanto nei conflitti armati internazionale, quanto in quelli interni.

[198] Nella decisione interlocutoria sul caso «*Tadic*» del 1995, il Tribunale penale internazionale per la *ex* Iugoslavia ha precisato che le gravi violazioni delle norme che disciplinano i conflitti armati interni possono, a certe condizioni, costituire crimini di guerra. Tribunale internazionale penale per la *ex* Iugoslavia, *Tadic c. Procuratore*, decisione della Camera d'Appello del 2 ottobre 1995, cit., par. 117.

[199] Nel novero dei conflitti armati non compresi nella norma vi sono, oltre a quelli fra Stati, le guerre di liberazione nazionale.

[200] La disposizione presuppone la soggettività giuridica non soltanto del governo legittimo, ma anche degli insorti, anch'essi titolari di situazioni giuridiche soggettive e tenuti al rispetto delle norme umanitarie.

[201] International Court of Justice, *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, cit., par. 114.

[202] S. Sivakumaran, *The Law of Non-International Armed Conflict*, Oxford, 2012, p. 255.

indicatori diretti a statuire un certo grado di intensità degli scontri armati e di organizzazione relativamente alle formazioni coinvolte nel conflitto[203].

La Camera di appello del Tribunale internazionale penale per la *ex* Iugoslavia, nel citato caso «*Tadic*», ha dichiarato che esiste un conflitto armato interno quando ha luogo una violenza armata protratta tra autorità governative e gruppi armati organizzati, oppure fra gruppi armati organizzati all'interno del territorio del medesimo Stato[204]. Non si può parlare di conflitto armato interno, quindi, in presenza di semplici disordini o tensioni interne, quali sommosse o atti sporadici di violenza, come si deduce, del resto, anche dal II Protocollo, il quale parla di «operazioni militari concertate e prolungate».

Occorre, pertanto, che gli scontri armati non siano solamente intensi, bensì anche prolungati[205]. È quanto richiesto, appunto, dal II Protocollo Aggiuntivo del 1977, il quale – a differenza della disciplina convenzionale del 1949 – trova applicazione allorquando la guerra civile abbia raggiunto una intensità ed una continuità tale da poter essere equiparata, a tutti gli effetti, ad uno scontro tra eserciti convenzionali[206].

Il riferimento all'arco temporale dei combattimenti è contenuto anche nello Statuto della Corte penale internazionale. In base all'art. 8, par. 2, lett. *f*), dello stesso, la punizione dei crimini di guerra deve avere luogo nel caso di «un conflitto bellico prolungato tra forze governative e gruppi armati organizzati o fra detti gruppi»[207].

Allo scopo di facilitare la valutazione circa l'esistenza di una violenza prolungata, il Tribunale internazionale penale per la *ex* Iugoslavia ha indicato diversi criteri quali la gravità degli attacchi sferrati, la loro ricorrenza ed il numero delle vittime da essi causato[208].

---

[203] L. Moir, *The Law of Internal Armed Conflict*, Cambridge, 2002, p. 34.
[204] Tribunale internazionale penale per la *ex* Iugoslavia, Camera di Appello, caso *Tadic*, 2 ottobre 1995, par. 70.
[205] Corte penale internazionale, *The Prosecutor v. Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06, sentenza del 14 marzo 2012, par. 234.
[206] T. Marauhn, Z. F. Ntouband, *Armed Conflict, Non-International*, in *MPEPIL*, 2016.
[207] Rispetto all'art. 3 «comune», lo Statuto della Corte penale internazionale, oltre a formalizzare il carattere organizzato delle fazioni in lotta, aggiunge quello prolungato del conflitto.
[208] Tribunale penale internazionale per la *ex* Iugoslavia, *Prosecutor v. Slobodan Milošević*, *Trial Chamber*, Decision, Case No. IT-02-54-T, 16 giugno 2004, par. 28.

L'art. 3 «comune» alle Convenzioni di Ginevra del 1949 trova applicazione ogni qual volta si riscontrino fenomeni di violenza bellica nel territorio di uno Stato, quale che sia la natura delle formazioni in conflitto: è necessario però che tali formazioni abbiano natura organizzata[209].

Affinché un gruppo armato non statale possa ritenersi sufficientemente organizzato, esso deve possedere un centro di comando e l'accertata capacità di procurarsi armi e di comunicare in modo ufficiale con l'esterno[210]. Viceversa, non è necessario che esso disponga di una struttura militare simile a quella di uno Stato, né che sia capace di controllare effettivamente una parte del territorio[211].

Secondo il Rapporto del 2008 del Comitato per l'uso della forza creato in seno all'*International Law Association* (ILA), i suindicati criteri sono tra loro correlati e devono, pertanto, considerarsi congiuntamente al fine classificare una determinata situazione come conflitto armato non internazionale[212].

Alla luce di quanto precede, per poter stabilire se una operazione cibernetica possa configurare un vero e proprio «atto di guerra» idoneo a far sorgere un conflitto armato non internazionale soggetto alle regole del diritto internazionale umanitario, occorre valutare se e, in caso affermativo in quali circostanze, i requisiti della soglia di violenza armata richiesta e del grado di organizzazione relativamente ai gruppi armati che sono coinvolti nel conflitto siano presenti e determinanti[213].

Per quanto concerne la prima condizione fondamentale, nessun attacco informatico pare aver mai raggiunto sinora, in termini di intensità e portata, il livello di violenza necessario affinché si possa discorrere di un conflitto armato non internazionale. Di conseguenza, l'inizio di un conflitto armato di questo genere dovuto ad attacchi di natura informatica appare uno scenario, al momento, alquanto improbabile[214]. In

---

[209] Y. Dinstein, *Non-International Armed Conflicts in International Law*, Cambridge, 2014, p. 30.
[210] Tribunale internazionale penale per la *ex* Iugoslavia, *Prosecutor v. Limaj, Bala e Musliu*, Case No. IT-03- 66-T, 30 novembre 2005, par. 129.
[211] *Ivi*, par. 89.
[212] International Law Association, Committee on the Use of Force, *Initial Report on the Meaning of Armed Conflict in International Law*, 2008, par. 22.
[213] M. N. Schmitt, *Classification of Cyber Conflict*, in *Journal of Conflict and Security Law*, 2012, p. 256.
[214] In senso opposto, sempre Schmitt, *Ivi*, p. 255.

particolare, come opportunamente osservato, gli attori non statali dispongono attualmente di capacità militari piuttosto limitate nello spazio cibernetico[215].

Diverso è il caso dell'impiego di tecnologie informatiche nel corso di un conflitto armato non internazionale già in svolgimento e combattuto prevalentemente con mezzi e metodi di combattimento convenzionali. In queste ipotesi, la suesposta normativa internazionale in tema di conflitti armati non internazionali trova senz'altro applicazione.

Tuttavia, le operazioni cibernetiche effettuate da singoli individui non appartenenti a nessuna delle fazioni armate in lotta ricadono nella sfera di applicazione del diritto penale interno dello Stato coinvolto nel conflitto[216].

Allo stesso modo, è da escludere che gruppi di *hackers* privi di infrastrutture fisiche o di punti di incontro reali, quali ad esempio sedi centrali, e composti da individui provenienti da numerosi Stati diversi da quello impegnato nel conflitto, possano qualificarsi alla stregua di «gruppi armati organizzati»[217].

In primo luogo, sarebbe impossibile determinare con certezza l'appartenenza di un individuo ad un simile gruppo[218]. In secondo luogo, manca certamente un grado di organizzazione tale da poter qualificare siffatti gruppi "virtuali" come gruppi armati organizzati.

Il Consiglio per i diritti umani delle Nazioni Unite, nel rapporto della Commissione internazionale di inchiesta chiamata a indagare sulle presunte violazioni dei diritti umani in Libia, ha sottolineato, infatti, che per poter ritenere sussistente un conflitto armato interno deve essere valutata, in aggiunta alla intensità degli scontri armati, anche la natura dei gruppi armati che si oppongono al Governo[219]. Riguardo a questi

---

[215] R. Geiss, *Cyber Warfare: Implications for Non-international Armed Conflicts*, in *International Law Studies*, 2013, pp. 633-634.
[216] *Ivi*, pp. 635-636.
[217] L. Arimastu, *Classifying cyber warfare*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 338.
[218] *Ivi*, p. 389.
[219] Consiglio per i diritti umani, rapporto della Commissione internazionale di inchiesta sulla Libia, 1° giugno 2011, doc. n. A/HRC/17/44, par. 64.

ultimi, ha assoluto rilievo il carattere gerarchico della loro struttura di comando, il sistema di disciplina e la logistica[220].

3. La regolamentazione dei mezzi e dei metodi di combattimento

Sebbene – in mancanza di una connessione con ostilità "tradizionali" – gli attacchi informatici non possono di pe sé portare all'applicazione delle norme di *ius in bello*, tali attacchi sono però assoggettati alle regole del diritto internazionale umanitario qualora effettuati in un conflitto nel quale sono già in svolgimento scontri armati tra i belligeranti.

Le parti in lotta non hanno un diritto illimitato nella scelta dei mezzi e metodi di guerra[221] a cui ricorrere per nuocere al nemico[222] e non possono avvalersi di armi capaci di causare mali superflui o sofferenze non necessarie[223].

Il diritto dei conflitti armati si applica a tutti i mezzi e metodi di combattimento, compresi quelli cibernetici[224]. La mancata regolamentazione di una condotta bellica non vuol dire, infatti, che questa sia ammessa.

---

[220] P. Margulies, *Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"*, in *International Law Studies*, 2013, pp. 56-65.

[221] L'espressione «mezzi di combattimento» viene impiegata, in genere, con riferimento a qualunque strumento di cui i belligeranti materialmente si avvalgono ai fini dell'esercizio della violenza bellica. Con l'espressione «metodi di combattimento» si intende, invece, qualunque tattica, strategia o procedura militare usata dagli stessi, nel corso delle ostilità, per cercare di imporsi sull'avversario. Y. Dinstein, *Warfare, Methods and Means*, in *MPEPIL*, 2015.

[222] Art. 22, Regolamento Annesso alla IV Convenzione dell'Aia del 1907 concernente le leggi e gli usi della guerra terrestre.

[223] In altre parole, un obiettivo legittimo non può essere colpito mediante armi che provochino sofferenze inutili o mali superflui. L'art. 35 del I Protocollo Aggiuntivo del 1977 impedisce, invero, ai belligeranti di ricorrere all'utilizzo di mezzi e metodi di conduzione delle ostilità suscettibili di cagionare all'avversario sofferenze maggiori di quanto necessario per realizzare il vantaggio militare che ci si attende di ottenere con l'operazione. Quanto ai parametri attraverso cui deve essere valutata l'eventuale superfluità di un'arma, l'interpretazione prevalente fa riferimento ai criteri della necessità e della proporzionalità. Ne scaturisce che, un'arma sarà automaticamente vietata qualora arrechi mali non necessari o, comunque, non proporzionali rispetto ai vantaggi militari che possono conseguire dal suo impiego. Occorre aggiungere che il divieto dell'utilizzo di armi che arrecano sofferenze inutili non tiene conto del fattore intenzionalità ed è volto a proteggere solo i combattenti, poiché – come si vedrà – la popolazione civile è protetta da altri principi applicabili ai conflitti armati. W. H. Boothby, *Weapons and the Law of Armed Conflict*, Oxford, 2009, p. 62.

[224] J. Döge, *Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime*, in *Archiv des Völkerrechts*, 2010, p. 489.

In altri termini, il fatto che la *cyber warfare* non sia disciplinata dalle norme dello *ius in bello* non ne esclude a priori la loro applicabilità e, come sottolineato da Döge, non significa affatto che durante un conflitto armato "*[…] cyber-attacks can be launched without any restrictions […]*"[225].

Sono numerose le previsioni del diritto umanitario che depongono in questo senso. La Dichiarazione di San Pietroburgo del novembre 1868 afferma, ad esempio, che: «*The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established, and to conciliate the necessities of war with the laws of humanity*»[226].

Ancora, la clausola Martens – incorporata nel terz'ultimo paragrafo del preambolo della IV Convenzione dell'Aia del 1907 relativa alle leggi e agli usi della guerra terrestre – dispone quanto segue: «*Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity and the dictates of public conscience*»[227].

---

[225] *Ibidem*.

[226] La Dichiarazione di San Pietroburgo del 1868 è il risultato di una conferenza internazionale tenutasi tra numerosi Stati europei di allora e promossa dallo Zar Alessandro II con lo scopo di limitare la violenza bellica, sottoponendola a nuovi e più stringenti restrizioni. W. H. Boothby, *Weapons and the Law of Armed Conflict*, cit., p. 57.

[227] La clausola Martens è ripetuta nelle quattro Convenzioni di Ginevra del 1949 e nel testo dell'art. 1, par. 2, del I Protocollo del 1977, il quale dispone: «Nei casi non previsti nel presente Protocollo o in altri accordi internazionali, le persone civili ed i combattenti restano sotto la protezione e l'imperio dei principi del diritto delle genti, quali risultano dagli usi stabiliti, dai principi di umanità e dai precetti della pubblica coscienza». Per effetto di tale clausola, regole in origine metagiuridiche, come quelle discendenti dai dettami della coscienza pubblica, si traducono in vere e proprie norme giuridiche internazionali. In argomento, H. Strebel, *Martens Clause*, in *EPIL*, 1982, p. 252 ss.; V. V. Pustogarov, *The Martens Clause in International Law*, in *Journal of the History of International Law*, 1999, p. 125 ss.; A. Cassese, *The Martens Clause: Half a Loaf or Simply Pie in the Sky?*, in *European Journal of International Law*, 2000, p. 187 ss.; T. Meron, *The Martens Clause, Principles of Humanity, and Dictates of Public Conscience*, in *American Journal of International Law*, 2000, p. 78 ss.; M. Salter, *Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause*, in *Journal of Conflict and Security Law*, 2012, p. 403 ss.

Tale clausola ha una portata generale e appare sostanzialmente diretta a colmare eventuali lacune presenti nella codificazione del diritto umanitario o, comunque, ad assicurare una disciplina ove le parti in lotta denuncino le convenzioni di diritto bellico[228]. Essa svolge, pertanto, una funzione essenziale ai fini della valutazione circa la liceità dei mezzi e dei metodi di guerra non specificatamente disciplinati dal diritto dei conflitti armati, impedendo così quella deplorevole interpretazione secondo cui sarebbe permesso tutto ciò che non risulti espressamente proibito[229]. Nel parere consultivo concernente la *liceità delle armi atomiche*, la Corte internazionale di giustizia ha conferito alla clausola in parola rango consuetudinario[230].

Il principio di umanità – richiamato dalla clausola Martens – impone, poi, a tutte le parti in lotta l'obbligo fondamentale di garantire a qualsiasi persona coinvolta nel conflitto, sia essa un civile o un combattente, un trattamento umano[231]. Tale principio riceve piena applicazione, come dichiarato dal Tribunale penale internazionale per la *ex* Iugoslavia, sia nei conflitti internazionali, che in quelli non internazionali[232]. Il principio in commento permea l'insieme delle norme di *ius in bello*, fungendo da contraltare al principio della necessità militare[233]. A ben

---

[228] J. von Bernstorff, *Martens Clause*, in *MPEPIL*, 2009.

[229] Come esempi di applicazione della clausola Martens, il Tribunale penale internazionale per la *ex* Iugoslavia ha citato il caso di attacchi che provochino danni incidentali alla popolazione civile, ma che in sé considerati non sono contrari al principio di proporzionalità. Secondo i giudici l'effetto cumulativo di attacchi ripetuti può dare luogo ad una violazione della regola della proporzionalità, poiché si finisce per arrecare un pregiudizio eccessivo alla popolazione civile e ai suoi beni, in contrasto con le esigenze di umanità. Tribunale penale internazionale per la *ex* Iugoslavia, *Kupreskic*, Judgment, Case No: IT-95-16-T, 14 January 2000, par. 1 ss.

[230] Corte internazionale di giustizia, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 78.

[231] G. S. Corn, *Humanity, Principle of*, in *MPEPIL*, 2013.

[232] Tribunale penale internazionale per la *ex* Iugoslavia, *Tadic (Interlocutory Appeal)*, cit., par. 119.

[233] Nell'economia del diritto dei conflitti armati la necessità militare o necessità bellica funge da clausola di salvaguardia, giustificando la commissione di atti altrimenti vietati. Nella sua accezione più ampia, elaborata dalla dottrina militare tedesca del secolo scorso, questa veniva invocata come limite generale all'applicazione delle norme di diritto internazionale bellico, finendo, di fatto, per mettere completamente in discussione il carattere cogente di tale *corpus* normativo. Tale visione non trova spazio però nella prassi internazionale successiva al Secondo conflitto mondiale. Oggi, infatti, la necessità militare può essere invocata come giustificazione di una condotta altrimenti proibita solo quando ciò sia espressamente consentito da una norma di diritto bellico. È il caso, ad esempio, dell'art. 17 del II Protocollo, il cui testo vieta il trasferimento della popolazione civile per motivi connessi al conflitto, a meno che non lo esigano ragioni militari imperiose o la sicurezza dei civili stessi. Ancora, risponde alla logica della necessità militare il divieto di attaccare città e località indifese, contenuto nell'art. 25 del Regolamento dell'Aia del 1907 relativo alle leggi e agli usi della guerra terrestre. Non vi è, infatti, nessuna esigenza militare nel bombardare, con qualsiasi mezzo,

guardare, invero, tutte le norme umanitarie non sono che il risultato di un continuo bilanciamento fra questi due principi, nel tentativo di fissare un punto di equilibrio fra l'esigenza degli Stati di ricorrere alla violenza bellica e quella di limitare le sofferenze inflitte agli individui a qualsiasi titolo coinvolti nel conflitto[234].

La Corte internazionale di giustizia, nel citato parere consultivo sulla *liceità delle armi nucleari*, ha sostenuto, inoltre, come segue: «*the entire law of armed conflict applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future*»[235].

Infine, in favore dell'applicazione del diritto internazionale umanitario nel caso di attacchi cibernetici condotti durante un conflitto armato preesistente si è espressa altresì la maggioranza degli Stati in seno all'Assemblea generale delle Nazioni Unite[236].

---

un luogo che può essere attraversato dal belligerante senza incontrare alcuna resistenza armata. Quando richiamata dalla norma primaria pertinente, la necessità militare giustifica l'adozione di una condotta altrimenti proibita soltanto se funzionale al conseguimento di un vantaggio militare nei confronti dell'altra parte in conflitto. Tale clausola di salvaguardia non può, quindi, essere invocata per giustificare atti finalizzati a perseguire obiettivi politici o soddisfare bisogni o interessi della popolazione civile dello Stato belligerante. Secondo una parte della dottrina, la necessità militare, nel moderno diritto bellico, dovrebbe essere intesa anche in un secondo significato, completamente opposto a quello precedente. A parere di taluni autori questa – lungi dal costituire una causa di giustificazione per un'azione altrimenti vietata – rappresenterebbe in realtà un limite generale all'azione bellica, nel senso che il belligerante dovrebbe impiegare solo la quantità di forza armata necessaria per sconfiggere il nemico, come è precisato nell'art. 5.2 del Manuale della Marina USA e nell'art. 2.2 del Manuale militare del Regno Unito. Se inteso in questo significato, il principio della necessità militare non si pone in conflitto con quello di umanità, ma semmai lo corrobora. La stessa regola che proibisce il ricorso a mezzi e metodi di combattimento capaci di cagionare mali superflui e sofferenze inutili può, invero, essere considerata come espressione dell'uno o dell'altro principio. La violazione del principio della necessità militare costituisce un crimine di guerra ai sensi dell'art. 8, par. 2 (*a*) (iv), dello Statuto della Corte penale internazionale. Il Tribunale internazionale penale per la *ex* Iugoslavia, nella sentenza riguardante il caso «*Prosecutor v. Rajić*», resa nel 2006, ha ritenuto l'imputato colpevole di aver distrutto un villaggio della Bosnia Erzegovina senza che la devastazione fosse necessaria a soggiogare il nemico. I giudici hanno sottolineato come non era stata provata alcuna giustificazione fondata sulla necessità militare e il comportamento era stato realizzato con intenzionalità. (Tribunale internazionale penale per la *ex* Iugoslavia, *Prosecutor v. Rajić*, 8 maggio 2006, IT-95-12-S, par. 54). Per una trattazione più ampia sulla necessità militare si rimanda a: G. Venturini, *Necessity in the Law of Armed Conflict and in International Criminal Law*, in *Netherlands Yearbook of International Law*, 2010, p. 45 ss.; Y. Dinstein, *Military Necessity*, in *MPEPIL*, 2015; L. Salvadego, *Struttura e funzioni della necessità militare nel diritto internazionale*, Torino, 2016; N. Hayashi, *Military Necessity: The Art, Morality and Law of War*, Cambridge, 2020.

[234] A. Annoni, F. Salerno, *La tutela della persona umana nei conflitti armati*, Bari, 2019, p. 125.

[235] Corte internazionale di giustizia, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 86.

[236] Assemblea generale delle Nazioni Unite, risoluzione n. 73/266, 13 luglio 2021.

In conclusione, non esiste attualmente alcun accordo internazionale che vieti o limiti il ricorso all'utilizzo di attacchi informatici nel corso di un conflitto armato da parte dei belligeranti[237]. In assenza di una specifica regolamentazione, tali attacchi sono soggetti ai principi e alle norme del diritto internazionale umanitario come qualsiasi altro strumento bellico convenzionale[238]. In altri termini, tutte le operazioni militari, comprese quelle condotte mediante strumenti informatici, sono vincolate alle regole del diritto dei conflitti armati[239].

Ai sensi dell'art. 36 del I Protocollo Aggiuntivo del 1977: «Nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra, un'Alta Parte contraente ha l'obbligo di stabilire se il suo impiego non sia vietato, in talune circostanze o in qualunque circostanza, dalle disposizioni del presente Protocollo o da qualsiasi altra regola del diritto internazionale applicabile a detta Alta Parte contraente»[240].

Ne discende che, come per i mezzi bellici convenzionali, gli Stati hanno l'obbligo di valutare la liceità delle tecnologie informatiche destinate a scopi militari sia nella fase di sviluppo delle stesse, che nella fase della loro adozione o acquisizione, da uno Stato terzo o da un privato[241].

Come affermato da Boothby, rientra fra le tecnologie informatiche ad uso militare: "*any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects*"[242].

---

[237] H. H. Dinnis, *Cyber Warfare and the Laws of War*, cit., p. 258.

[238] W. H. Boothby, *Methods and Means of Cyber Warfare*, in *International Law Studies*, 2013, p. 391.

[239] In tal senso si è pronunciata anche la maggioranza della dottrina internazionalistica: J. Beckett, *New War, Old Law: Can the Geneva Paradigm Comprehend Computers?*, in *Leiden Journal of International Law*, 2000, p. 33 ss.; W. Church, *Information warfare*, in *International Review of the Red Cross*, 2000, p. 205 ss.; E. Haslam, *Information Warfare: Technological Changes and International Law*, in *Journal of Conflict and Security Law*, 2000, p. 157 ss.

[240] W. H. Parks, *Conventional Weapons and Weapons Reviews*, in *Yearbook of International Humanitarian Law*, 2005, p. 55 ss.; M. Castellaneta, *New weapons, old crimes?*, in F. Pocar, M. Pedrazzi, M. Frulli (eds.), *War Crimes and the Conduct of Hostilities. Challenges to Adjudication and Investigation*, Cheltenham, 2013, pp. 197-199; N. Jevglevskaja, *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict*, Cambridge, 2021.

[241] P. J. Blount, *The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons*, in *Northern Kentucky Law Review*, 2012, pp. 213-214.

[242] W. H. Boothby, *Methods and Means of Cyber Warfare*, cit., p. 389.

4. La disciplina delle *cyber operations* in tempo di *occupatio bellica*

Affinché un determinato territorio possa dirsi, in tutto o in parte, occupato occorre, come recita l'art. 42 del Regolamento dell'Aia del 1907, che esso sia posto di fatto sotto l'autorità dell'esercito avversario[243]. La disposizione in commento subordina l'applicazione del regime giuridico dell'*occupatio bellica* alla sussistenza di una situazione meramente fattuale: la sottoposizione del territorio e della popolazione ivi residente al controllo effettivo e stabile dello Stato nemico[244].

La nozione di controllo effettivo implica il concreto esercizio, da parte dell'Autorità occupante, del proprio potere di governo per un arco di tempo più o meno lungo[245]. La Potenza occupante può svolgere tale potestà di governo in maniera diretta, ossia attraverso un'apposita struttura militare o civile, oppure indirettamente, ovvero affidando la gestione del territorio oggetto di occupazione ad un governo fantoccio, la cui condotta sarà comunque ad essa riconducibile[246].

L'occupazione belligerante è disciplinata dagli articoli 42-56 del Regolamento annesso alla IV Convenzione dell'Aia del 1907, dagli articoli 27-33 e 47-48 della IV Convenzione di Ginevra del 1949 e, infine, dagli articoli 72-79 del I Protocollo del 1977[247]. Vengono, inoltre, in considerazione le norme sui diritti dell'uomo e il

---

[243] A. Roberts, *What is military occupations?*, in *British Yearbook of International Law*, 1984, p. 249.

[244] Occorre distinguere l'occupazione bellica dalla semplice invasione o incursione, la quale non dà luogo ad un insediamento stabile dell'Autorità occupante in territorio occupato. L'invasione è, di regola, prodromica all'occupazione e rende applicabili le norme sull'occupazione militare solamente nei casi in cui il belligerante controlli effettivamente e stabilmente il territorio in cui è penetrato. E. Benvenisti, *Occupation, Belligerent*, in *MPEPIL*, 2009.

[245] L'occupazione bellica, indipendentemente dall'intento che l'ha motivata, presuppone sempre che il conflitto armato sia ancora in corso di svolgimento, cioè che nessuno dei belligeranti abbia ancora vinto e, conseguentemente, non determina in nessun modo l'acquisto della sovranità sul territorio occupato. M. Bothe, *Occupation, Belligerent*, in *EPIL*, 1997, p. 763.

[246] Al potere di governo della Potenza occupante deve corrispondere la cessazione della potestà di governo dello Stato occupato. L'esercizio delle funzioni di governo da parte dell'occupante non deve necessariamente essere esclusivo. Può accadere, infatti, specie nei casi di occupazione prolungata, che la Potenza occupante consenta alle autorità locali di svolgere talune funzioni di governo in modo sostanzialmente autonomo. Il concetto di controllo effettivo prescinde altresì dalla presenza fisica delle truppe nemiche sul territorio occupato. Vi possono essere, invero, situazioni in cui lo Stato occupante riesca ad esercitare la propria autorità in modo esclusivo anche mantenendosi all'interno dei propri confini. A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 177.

[247] Tali norme, in genere ritenute corrispondenti al diritto internazionale consuetudinario, regolano specificamente – a partire dal momento in cui l'occupazione ha inizio e per il tutto il tempo in cui

principio di autodeterminazione dei popoli, come rilevato dalla Corte internazionale di giustizia nel parere consultivo del 2004 concernente le conseguenze giuridiche derivanti dalla costruzione di un *Muro in Palestina*[248].

Non avendo nessun titolo di sovranità sul territorio occupato, l'Autorità occupante non può procedere alla sua annessione *pendente bello* o al suo smembramento per stabilirvi entità statali più o meno indipendenti[249]. Essa può svolgere, pertanto, i soli poteri che il diritto internazionale le conferisce per realizzare le proprie esigenze militari e garantire, allo stesso tempo, lo svolgimento della ordinaria vita civile[250].

A tale proposito, la Potenza occupante – avendo sostituito la propria autorità a quella del precedente governo del territorio occupato – ha, anzitutto, l'obbligo di assicurare e, eventualmente, ripristinare l'ordine e la sicurezza pubblica[251], nonché l'obbligo di provvedere al benessere e al sostentamento della popolazione locale[252]. Nell'adempiere tali obblighi essa è tenuta, salvo impedimento assoluto, a rispettare le leggi previgenti[253] e mantenere l'apparato organizzativo preesistente[254]. Da ultimo, lo Stato occupante non può procedere al trasferimento di una parte della propria popolazione all'interno del territorio occupato, alla luce del divieto della pratica degli insediamenti (art. 49 della IV Convenzione di Ginevra del 1949)[255] e

---

questa si protrae, nei limiti della porzione di territorio che si trova sotto il controllo esclusivo delle forze armate avversarie – i soli rapporti tra lo Stato occupante e lo Stato occupato o gli abitanti del territorio occupato. Non si applicano, invece, ai cittadini della Potenza occupante. Ai cittadini di Stati terzi che eventualmente si trovino nel territorio occupato si applicano, viceversa, le norme sul trattamento degli stranieri e quelle sui diritti dell'uomo. C. Curti Gialdino, *Occupazione bellica*, in *Enc. dir.*, Vol. XXIX, 1979, p. 720.

[248] Corte internazionale di giustizia, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, cit., par. 106 e par. 113.

[249] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 277.

[250] Lo Stato occupante deve, pertanto, amministrare il territorio soggetto ad occupazione non soltanto nell'interesse proprio, ma anche nell'interesse degli abitanti ivi residenti, con la conseguenza che ad esso spetteranno sia diritti che doveri.

[251] M. Sassòli, *Legislation and Maintenance of Public Order and Civil Life by Occupying Powers*, in *European Journal of International Law*, 2005, p. 661 ss.

[252] S. Vité, *L'articulation du droit de l'occupation et des droits économiques, sociaux et culturels: les exemples de l'alimentation, de la santé et de la propriété*, in *International Review of the Red Cross*, 2008, p. 1 ss.

[253] R. Kolb, S. Vité, *Le droit de l'occupation militaire. Perspectives historiques et enjeux juridiques actuelles*, Bruxelles, 2009, p. 187.

[254] C. Greenwood, *The Administration of Occupied Territory in International Law*, in E. Playfair (ed.), *International Law and the Administration of Occupied Territories. Two Decades of Israel Occupation of the West Bank and Gaza Strip*, Oxford, 1992, p. 241 ss.

[255] M. Castellaneta, *Conflitti Armati (diritto internazionale)*, cit., p. 331.

deve, poi, astenersi dall'infliggere punizioni collettive per fatti commessi da singoli individui (art. 33 della IV Convenzione di Ginevra).

Ora, con riferimento all'istituto dell'occupazione militare, il Manuale di Tallinn 2.0 sul diritto internazionale applicabile alla guerra cibernetica, alla regola 147, dispone quanto segue: «*To the extent the law of occupation permits the confiscation or requisition of property, taking control of cyber infrastructure or systems is likewise permitte*d»[256].

La citata regola si basa, a ben guardare, sulla disciplina dettata dagli articoli 46, 52, 53, 55 e 56 del Regolamento dell'Aia del 1907 e dall'art. 55 della IV Convenzione di Ginevra del 1949. Tali disposizioni, descrivendo i poteri dell'Autorità occupante sulla proprietà ubicata nel territorio occupato, dettano una disciplina differenziata sulla base di due criteri di fondo: la natura mobile o immobile del bene e quella pubblica o privata dello stesso.

Per quanto concerne il trattamento da riservare ai beni mobili pubblici, ai sensi dell'art. 53, par. 1, del Regolamento dell'Aia del 1907, la Potenza occupante ha la facoltà di appropriarsi, in maniera definitiva, di tutti i beni mobili di proprietà dello Stato occupato suscettibili di utilizzo militare e di disporne come meglio crede, fermo restando la necessità di evitare un impoverimento eccessivo del territorio occupato, capace di compromettere tanto il benessere della popolazione civile, quanto il rapido ripristino dello *status quo ante*, una volta cessata l'occupazione[257].

Il trattamento dei beni immobili di proprietà dello Stato occupato è disciplinato, invece, dall'art. 55 del Regolamento dell'Aia del 1907, il quale considera lo Stato occupante come «amministratore» e «usufruttuario» delle proprietà immobili pubbliche situate nel territorio occupato. La norma impone all'Autorità occupante di salvaguardare il capitale di tali proprietà e di amministrarlo conformemente alle regole dell'usufrutto[258].

---

[256] *Tallinn Manual 2.0*, p. 549.

[257] A. Annoni, *L'occupazione ostile nel diritto internazionale contemporaneo*, Torino, 2012, p. 211,

[258] A ben vedere, i poteri dell'occupante sono più estesi per quanto attiene alla proprietà mobile pubblica, mentre la proprietà immobile pubblica è tutelata in modo più ampio.

Diversamente, per quanto riguarda le proprietà mobili e immobili private, le norme sull'occupazione, in termini complessivi, riservano ad esse un trattamento più garantista rispetto a quello riconosciuto ai beni pubblici[259].

Il principio fondamentale è la totale esclusione della confisca[260]. Sono al contrario possibili, ove funzionali al soddisfacimento dell'esercito occupante, requisizioni della proprietà privata mobile dietro pagamento e requisizioni temporanee della proprietà privata immobile[261].

Alla luce del suesposto articolato quadro normativo, relativamente ai beni aventi carattere mobile, lo Stato occupante non può procedere al sequestro dei dispositivi elettronici (computers, *memory devices*, ecc.) appartenenti alla popolazione civile, mentre può impossessarsi degli stessi qualora essi rientrino nel novero dei beni di proprietà dello Stato occupato e presentino una qualche utilità militare [art. 53 del Regolamento dell'Aia del 1907]. Ad ogni modo, ai sensi dell'art. 53 della IV Convenzione di Ginevra del 1949, l'Autorità occupante ha la facoltà di distruggere le predette apparecchiature, quando le operazioni militari lo rendano assolutamente necessario[262].

La natura pubblica-privata o mobile-immobile del bene deve essere individuata con riferimento alle caratteristiche fisiche dello stesso, oppure, ancora, in base alla sua classificazione nell'ordinamento giuridico del territorio occupato[263].

In ragione delle loro caratteristiche fisiche, nonché del loro statuto giuridico negli ordinamenti interni di molti Stati della comunità internazionale, le infrastrutture di reti pubbliche di comunicazione – quali torri, tralicci, impianti radio-trasmittenti, ripetitori di servizi di comunicazione elettronica – si iscriveranno certamente nella categoria dei beni immobili presenti nel territorio occupato[264]. Tale inquadramento

---

[259] A. Annoni, *L'occupazione ostile nel diritto internazionale contemporaneo*, cit., p. 187.
[260] Art. 46 del Regolamento dell'Aia del 1907.
[261] M. Pertile, *La relazione tra risorse naturale e conflitti armati nel diritto internazionale*, Padova, 2012, p. 173.
[262] Deve trattarsi, quindi, di beni suscettibili di essere, in qualche modo, utilizzati nelle operazioni militari contro le truppe di occupazione.
[263] M. Pertile, *La relazione tra risorse naturale e conflitti armati nel diritto internazionale*, cit., p. 176.
[264] Nell'ordinamento giuridico italiano, le infrastrutture di reti pubbliche di comunicazione e le opere civili realizzate per l'installazione di infrastrutture di comunicazione elettronica ad uso pubblico

giuridico riveste assoluta importanza poiché esclude il sequestro delle installazioni in parola da parte dell'Autorità occupante[265]. La misura del sequestro è, invero, sempre ammessa per la proprietà mobile – sia questa privata o pubblica – che rientri nell'ambito dei mezzi di comunicazione della Potenza occupata [art. 53, par. 2, Regolamento dell'Aia del 1907].

Come si è detto, anche in contesti di occupazione militare si applicano le norme internazionali sulla protezione della persona umana[266]. Ne consegue per lo Stato occupante l'obbligo di garantire il diritto di accesso ad Internet in tutto il territorio occupato. L'accesso ad Internet è, oggi, ritenuto non soltanto essenziale per il rafforzamento ed il godimento dei diritti umani in genere (si pensi, a titolo di esempio, alla libertà di espressione e di informazione, che si estende a tutti i mezzi

sono qualificate come beni immobili ai sensi degli artt. 87 e 88 del Codice delle comunicazioni elettroniche (CCE).

[265] Appare ammissibile la demolizione delle costruzioni in commento qualora esse appartengano a privati e siano impiegate dal nemico per scopi militari, sempreché la sicurezza dell'occupante non possa essere garantita in altra maniera. Qualora, invece, tali opere rientrino nella categoria dei beni immobili statali, in base a quanto statuito dall'art. 55 del Regolamento dell'Aia del 1907, la Potenza occupante non può procedere alla loro alienazione. Qualora sorgano dubbi sul carattere privato o pubblico di tali costruzioni, deve sempre presumersi che esse siano di proprietà dello Stato, a meno che la loro natura privata non risulti evidente.

[266] La Corte internazionale di giustizia, nel parere consultivo sulle conseguenze giuridiche derivanti dalla costruzione di un «Muro» nei territori palestinesi occupati, reso nel 2004, ha sancito l'obbligo per Israele di applicare il Patto Onu sui diritti civili e politici in qualità di Potenza occupante che ha il controllo effettivo sul territorio del nemico. Secondo la Corte la costruzione del «Muro» violava non solo il diritto internazionale umanitario, bensì anche una pluralità di altre norme internazionali poste a protezione dei diritti umani. (International Court of Justice, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, cit., par. 112). Nella sentenza relativa al caso *Al-Skeini c. Regno Unito*, resa dalla Grande Camera nel 2011, la Corte europea dei diritti dell'uomo ha analizzato il complesso rapporto tra Convenzione europea dei diritti dell'uomo e diritto umanitario ed ha riconosciuto l'applicabilità della Convenzione rispetto alla condotta delle forze di occupazione inglesi presenti in Iraq. Secondo la Corte il Regno Unito, in quanto Potenza occupante di una zona dell'Iraq, era certamente tenuto al rispetto della Convenzione. (Corte europea dei diritti dell'uomo *Al Skeini and Others c. United Kingdom*, sentenza del 7 luglio 2011, Grande Camera, ricorso n. 55721/07, in ECHR *Reports*, par. 86). In dottrina, sulla tesi dell'applicabilità delle norme sui diritti umani durante un'occupazione, si rinvia soprattutto a: M. Dennis, *Application of Human Rights Treaties Extraterritorially in Times of Armed Conflict and Military Occupation*, in *American Journal of International Law*, 2005, p. 119 ss.; D. Campanelli, *The Law of Military Occupation Put to the Test of Human Rights Law*, in *International Review of the Red Cross*, 2008, p. 653 ss.

di comunicazione elettronica)[267], ma è anche considerato un vero e proprio diritto umano a sé stante[268].

[267] Nella sentenza *Yildirm c. Turchia* del 2012 la Corte europea dei diritti dell'uomo ha affermato che il blocco all'accesso a Google deciso dalle autorità giudiziarie turche per impedire l'accesso al sito di un docente che aveva diffuso testi offensivi (secondo i giudici turchi) della memoria di Ataturk era in chiaro contrasto con l'art. 10 della Convenzione. Secondo la Corte «Internet è ormai divenuto lo strumento principale con il quale poter esercitare la libertà di espressione e di informazione e risulta, pertanto, senz'altro protetto dall'art. 10, tenendo conto in particolare che il diritto alla libertà di espressione si applica senza riguardo alle frontiere». Corte europea dei diritti dell'uomo, *Yildirm c. Turchia*, sentenza del 18 dicembre 2012, ric. 3111/10, par. 54. Con riguardo, invece, al sistema delle Nazioni Unite, il Consiglio Onu per i diritti umani ha sollecitato gli Stati ad emanare misure dirette ad assicurare l'accesso alle nuove tecnologie di comunicazione, dal momento che dette tecnologie rappresentano, a tutti gli effetti, mezzi di attuazione della libertà di espressione. Nel suo rapporto del 2011 il relatore speciale del Consiglio Onu per i diritti umani – nel sancire il diritto di accesso ad Internet come specifico aspetto alla libertà di espressione – ha, peraltro, sottolineato il ruolo cruciale che Internet può svolgere nella lotta al razzismo, alle discriminazioni e alla xenofobia, e ha affermato che misure restrittive di accesso alla rete sono ammesse solamente quando sussistono le condizioni previste dai trattati.

[268] La questione se il diritto di accesso ad Internet abbia assunto i connotati di un diritto fondamentale autonomo è piuttosto controversa in dottrina. A nostro giudizio, ciò non può escludersi a priori. Il diritto in commento è contenuto sia nella Dichiarazione del Millennio Onu, che nella Dichiarazione di principi del *World Summit on the Information Society*, tenutosi a Ginevra nel 2003, dove è stato associato al diritto allo sviluppo, in quanto strumento idoneo a integrare tutti gli Stati, in particolare quelli più poveri, nell'economia internazionale. Sempre con riferimento al diritto allo sviluppo, l'Assemblea generale dell'Onu ha ribadito la rilevanza dell'accesso alla rete, evidenziando come le tecnologie dell'informazione possano effettivamente contribuire a favorire una crescita economica più sostenibile ed inclusiva. Il diritto di avvalersi delle reti internazionali di comunicazione è sancito, peraltro, nel testo dell'art. 3.4 dei Regolamenti dell'Unione Internazionale delle Telecomunicazioni, e nell'art. 33 della Costituzione ITU, la quale consente agli Stati di adottare limitazioni ai servizi internazionali di telecomunicazione solo al fine di tutelare interessi di rilevanza superiore, come, ad esempio, la sicurezza nazionale. Un richiamo al diritto in commento è, inoltre, rinvenibile nella Convenzione Onu sui diritti delle persone con disabilità e nella Dichiarazione Onu sui diritti dei popoli indigeni. La Convenzione, adottata il 13 dicembre 2006, promuove l'accesso alle tecnologie dell'informazione in favore delle persone disabili. La Dichiarazione, approvata dall'Assemblea generale il 13 settembre 2007, dispone, invece, il diritto delle popolazioni indigene ad avere accesso a tutte le forme mediatiche esistenti, senza subire discriminazioni. Per quanto concerne, viceversa, le fonti di *soft law* vigenti in materia di accesso al Web, può ricordarsi la raccomandazione UNESCO del 15 ottobre 2003 riguardante l'utilizzo di contenuti e sistemi multilingue nella dimensione del ciberspazio. Tale dichiarazione, sebbene non abbia valore giuridico vincolante, risulta di particolare rilievo poiché ha per oggetto la facilitazione dell'accesso alle reti ed ai servizi informatici. Infine, relativamente alle normative nazionali, non mancano misure dirette a introdurre il diritto in parola nelle Costituzioni statali. Nel luglio 2010, ad esempio, il Parlamento della Finlandia ha riconosciuto il diritto di accesso a banda larga a Internet a tutti i suoi cittadini, inclusi quelli che vivono in località remote. Durante lo stesso anno, lo Stato di Panama ha ritenuto di dover estendere l'accesso alla rete istituendo sul suo territorio ben 214 punti pubblici di connessione. Anche l'art. 16 della Costituzione dell'Ecuador dispone un diritto di accesso generale alle tecnologie dell'informazione, mentre il successivo art. 17 impone una serie di obblighi correlativi allo Stato. Sul diritto di accesso al Web vedi: S. Tully, *A Human Right to Access the Internet? Problems and Prospects*, in *Human Rights Law Review*, 2014, pp. 175-195; O. Pollicino, *The Right to Internet Access. Quid Iuris?*, in A. von Arnauld, K. von der Decken, M. Susi (eds.), *The Cambridge Handbook of New Human Rights Recognition, Novelty, Rhetoric*, Cambridge, 2020, pp. 263-275.

Di conseguenza, le misure con cui Israele ha disposto l'interruzione totale delle comunicazioni e il blocco all'accesso alla rete in tutti i territori della Striscia di Gaza, nel corso della sua risposta armata – a nostro giudizio del tutto in contrasto con principi dello *ius in bello* – agli attacchi condotti dalle forze di Hamas il 7 ottobre 2023[269], devono ritenersi certamente contrari tanto all'art. 15 del Patto delle Nazioni Unite sui diritti economici, sociali e culturali (il quale stabilisce il diritto a usufruire dei benefici del progresso scientifico e delle sue applicazioni, fra le quali deve essere annoverato anche Internet); quanto all'art. 19 del Patto delle Nazioni Unite sui diritti civili e politici (che tutela tutte le forme e le modalità di espressione elettronica, compresa, per l'appunto, quella basata su Internet).

5. La rilevanza dei diritti dell'uomo nella condotta delle operazioni cibernetiche in tempo di guerra

A differenza di quanto accaduto per i sistemi d'arma autonomi[270], poco si è discusso in dottrina in merito alle problematiche che gli attacchi telematici, condotti in tempo di guerra, potrebbero sollevare sul piano del diritto internazionale dei diritti umani[271].

Accertata l'applicabilità del diritto internazionale umanitario a tutte le operazioni informatiche equivalenti ad un attacco ai sensi dell'art. 49, par. 1, del I Protocollo Aggiuntivo del 1977, occorre ora chiedersi se, ai fini della regolamentazione di tali operazioni, possano venire in rilievo anche gli obblighi assunti dai belligeranti in materia di diritti umani.

---

[269] R. Carroll, *Gaza in communications blackout as Israel intensifies siege*, *The Guardian*, 27 October 2023.

[270] P. Asaro, *On Banning Autonomous Weapons Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision Making*, in *International Review of the Red Cross*, 2012, p. 687 ss.; D. Mauri, *Autonomous Weapons Systems and the Protection of the Human Person: An International Law Analysis*, Cheltenham, 2022.

[271] H. Lin, *Cyber Conflict and International Humanitarian Law*, in *International Review of the Red Cross*, 2012, pp. 527-528; D. P. Fidler, *Cyberattacks and International Human Rights Law*, in S. Casey-Maslen (ed.), *Weapons under International Human Rights Law*, Cambridge, 2014, pp. 304-305.

Secondo una parte della dottrina internazionalistica, risalente oramai a molti anni addietro, le norme sui diritti umani si applicherebbero solamente in tempo di pace[272]. Anche a detta di taluni Stati, come ad esempio Israele, il diritto internazionale umanitario avrebbe carattere esclusivo, nel senso che nel corso di un conflitto bellico andrebbero applicate soltanto le regole (meno garantiste) sulla tutela della persona umana previste da questo regime normativo.

Tuttavia, una simile impostazione non appare per nulla condivisibile alla luce del diritto internazionale contemporaneo. Essa non tiene conto, infatti, del processo di modifica strutturale che ha investito l'intero ordinamento internazionale a partire dagli ultimi sessant'anni, con il graduale affermarsi della teoria dei diritti umani[273]. La netta dicotomia fra regole proprie del tempo di pace e norme applicabili in tempo di guerra, che un tempo caratterizzava l'impianto normativo internazionale, non è oggi più riscontrabile[274]. Le norme internazionali consuetudinarie, specialmente se

---

[272] J. Pictet, *Le droit humanitaire et la protection des victimes de la guerre*, Leiden, 1973, p. 13; A. Migliazza, *L'évolution de la réglementation de la guerre à la lumière de la sauvegarde des droits de l'homme*, in *RdC*, 1972, p. 143 ss.

[273] T. Meron, *The Humanization of International Law*, The Hague, 2006, in specie pp. 91-187; R. Pisillo Mazzeschi, *Diritto internazionale dei diritti umani. Teoria e prassi*, Torino, 2020, pp. 13-28.

[274] L'applicabilità dei trattati sui diritti umani in caso di conflitto armato pone il problema del rapporto tra le regole di diritto umanitario e la normativa internazionale sui diritti umani. Tale relazione, in assenza di una gerarchia, viene considerata, di solito, come un rapporto tra *lex generalis* (diritti umani) e *lex specialis* (diritto umanitario), con la consequenziale prevalenza di quest'ultimo nelle ipotesi di contrasto normativo. Qualora il criterio di specialità non possa però venire in rilievo, occorrerà fare ricorso al principio del *favor*, in virtù del quale, in caso di antinomia fra due norme protettive del medesimo diritto individuale, sarà quella in concreto più favorevole per l'interessato a dover essere preferita. Per quanto concerne le molteplici differenze tra diritto umanitario e diritto dei diritti umani, se si assume il criterio temporale, si constata che il primo *corpus* normativo risale alla Conferenza diplomatica del 1864, mentre la normativa internazionale sui diritti umani prende avvio con la Dichiarazione universale del 1948. Anche sotto il profilo dell'organizzazione da cui i due sistemi normativi promanano è possibile individuare la differenza. Il diritto umanitario è riconducibile all'impulso offerto da quella entità che va convenzionalmente sotto il nome di "Croce Rossa Internazionale", mentre il diritto dei diritti umani è stato sviluppato in seno alle Nazioni Unite. I due complessi normativi si differenziano, quindi, altresì quanto all'ente che ne ha promosso e presieduto il sorgere e lo sviluppo. La differenziazione tocca, inoltre, l'ambito di applicazione. Il diritto umanitario, infatti, è applicabile nella sfera circoscritta dei conflitti armati, laddove i diritti umani hanno applicazione soprattutto in tempo di pace, rientrando nel contesto del diritto internazionale "*tout court*". Quanto ai soggetti, il diritto dei diritti umani investe, in primo luogo, i rapporti che intercorrono tra lo Stato ed i suoi cittadini, mentre le regole di diritto umanitario abbracciano una sfera più estesa di rapporti, ricomprendendo anche i rapporti fra lo Stato in conflitto ed i cittadini nemici. Infine, il diritto umanitario è radicato intorno al concetto di reciprocità: esso risponde all'interesse di ciascuno Stato di fare in modo che alla propria popolazione civile vengano risparmiati gli orrori della guerra. Il diritto dei diritti umani è, invece, più incentrato sulla tutela di interessi rilevanti per la comunità internazionale intesa nel suo insieme, dal momento che ha come interesse primario quello di proteggere l'essere umano in quanto tale, vale a dire indipendentemente

cogenti[275], nonché molti trattati internazionali conclusi in tempo di pace aventi ad oggetto la protezione dei diritti umani conservano, invero, la propria efficacia anche in fase di conflitto armato[276].

Sono numerosi i dati della prassi che depongono proprio in questo senso. La piena applicabilità delle norme sui diritti umani in contesti di conflitto armato è stata più volte ribadita, in ambito Onu, dall'Assemblea generale[277], dal Consiglio di sicurezza[278] (ancorché meno frequentemente rispetto all'Assemblea), dal Segretario

dalla sua nazionalità o da altre forme di appartenenza o fedeltà ad uno Stato. Dopo la Seconda guerra mondiale, i due ambiti normativi considerati hanno percorso vie differenti ma parallele. A partire dagli anni Sessanta, tuttavia, si è fatta strada, nella comunità internazionale, la constatazione della similarità e della confluenza del diritto umanitario e di quello dei diritti umani. Di conseguenza, gli anzidetti settori normativi si presentano oggi, ancorché distinti, come strettamente correlati, con ampie zone di sovrapposizione. Di qui, la necessità di operare una connessione e ritenere i due regimi normativi – dall'originaria divergenza – come complementari. E. Greppi, *Diritto internazionale umanitario dei conflitti armati e diritti umani: profili di una convergenza*, in *La Comunità internazionale*, 1996, p. 473 ss.; G. Venturini, *Diritto umanitario e diritti dell'uomo: rispettivi ambiti di intervento e punti di confluenza*, in *Rivista internazionale dei diritti dell'uomo*, 2001, p. 101 ss.; F. Lattanzi, *Il confine fra diritto internazionale umanitario e diritti dell'uomo*, in *Studi in Onore di Gaetano Arangio Ruiz*, Vol. III, Napoli, 2004, p. 1985 ss.;

[275] A. Bianchi, *Human Rights and the Magic of Jus Cogens*, in *European Journal of International Law*, 2008, p. 491 ss.

[276] Tale posizione è condivisa dalla gran parte della dottrina internazionalistica. Si veda: L. Doswald-Beck, S. Vité, *International Humanitarian Law and Human Rights Law*, in *International Review of the Red Cross*, 1993, p. 94 ss.; H. J. Heintze, *On the Relationship between Human Rights Law Protection and International Humanitarian Law*, in *International Review of the Red Cross*, 2004, p. 789 ss.; N. Lubell, *Challenges in Applying Human Rights Law to Armed Conflict*, in *International Review of the Red Cross*, 2005, p. 737 ss.; A. Cassimatis, *International Humanitarian Law, International Human Rights Law, and Fragmentation of International Law*, in *International and Comparative Law Quarterly*, 2007, p. 623 ss.; C. Droege, *Elective Affinities? Human Rights and Humanitarian Law*, in *International Review of the Red Cross*, 2008, p. 501 ss; F. J. Hampson, *The Relationship between International Humanitarian Law and Human Rights Law from the Perspective of a Human Rights Treaty Body*, in *International Review of the Red Cross*, 2008, p. 549 ss; A. Orakhelashvili, *The Interaction between Human Rights and Humanitarian Law: Fragmentation, Conflict, Parallelism, or Convergence?*, in *European Journal of International Law*, 2008, p. 161 ss.; C. Tomuschat, *Human Rights and International Humanitarian Law*, in *European Journal of International Law*, 2010, p. 15 ss.

[277] Nella risoluzione n. 2675 (XXV) del 9 dicembre 1970, l'Assemblea generale dell'Onu dichiarava che i "*fundamental human rights, as accepted in international law and laid in international instruments, continue to apply fully in situations of armed conflict*". Assemblea generale delle Nazioni Unite, risoluzione n. 2675 (XXV) del 9 dicembre 1970, par. 1.

[278] Nella risoluzione n. 237 del 14 giugno 1967, il Consiglio di sicurezza dell'Onu dichiarava che: "*essential and inalienable human rights should be respected even during the vicissitudes of war*". Consiglio di sicurezza delle Nazioni Unite, risoluzione n. 237 del 14 giugno 1967, preambolo.

generale[279], dal Comitato sui diritti civili e politici[280], nonché, ancora, dal Comitato sui diritti economici, sociali e culturali[281]. La Commissione di diritto internazionale ha inserito, poi, i trattati sui diritti umani fra quelle categorie di convenzioni che, in virtù del loro oggetto e del loro scopo, devono ritenersi perfettamente applicabili anche in situazioni di guerra[282]. In favore della consolidata tendenza a riconoscere l'osservanza degli obblighi sui diritti umani in luogo di conflitto armato si sono espresse, inoltre, la Corte internazionale di giustizia[283], la Corte europea dei diritti

[279] Nel 1969 il Segretario generale dell'Onu pubblicò un rapporto sull'applicabilità delle norme a tutela dei diritti umani durante un conflitto armato, nel quale dichiarava espressamente che: "*United Nations instruments already in force and those which still require ratifications in order to become fully operative may be invoked to protect human rights at all times and everywhere and thus complete in certain respects and lend support to the international instruments especially applicable in condition of war or armed conflicts*". Segretario generale delle Nazioni Unite, *Respect For Human Rights in Armed Conflicts*, 20 novembre 1969, UN Doc. A/7720, par. 16.

[280] Nelle sue osservazioni conclusive pubblicate nel 2003 e riguardanti lo Stato di Israele, il Comitato dei diritti dell'uomo dichiarava – con ciò definitivamente rigettando l'opinione contraria di Israele – che il Patto internazionale sui diritti civili e politici è perfettamente applicabile anche in fase di conflitto armato e nei territori occupati militarmente. Comitato delle Nazioni Unite per i diritti civili e politici, *Concluding Observation: Israel*, 21 agosto 2003, UN. Doc. CCPR/C/79/Add. 93, par. 11.

[281] La questione della rilevanza del Patto delle Nazioni Unite sui diritti economici, sociali e culturali in caso di conflitto armato, si è posta all'attenzione nel 2003, di fronte alle reticenze dello Stato di Israele, il quale non riteneva di dover fornire informazioni circa la situazione dei territori palestinesi occupati. In tale occasione, pertanto, il Comitato sui diritti economici, sociali e culturali si è pronunciato in favore della concomitante e complementare applicazione del diritto umanitario e dei diritti umani in contesti di guerra o di occupazione belligerante. Comitato delle Nazioni Unite per i diritti economici sociali e culturali, *Concluding Observation: Israel*, 23 maggio 2003, UN. Doc. CRC/C/15/Add. 90, par. 31.

[282] L'allegato al Progetto di articoli sugli effetti dei conflitti armati sui trattati, adottato in seconda lettura dalla Commissione del diritto internazionale nel 2011, propone un elenco di categorie di convenzioni che – alla luce del loro oggetto e del loro scopo – devono ritenersi indubbiamente applicabili anche nel corso di un conflitto armato. All'interno di tale lista (non esaustiva) figurano anche e, soprattutto, i trattati in materia di diritti umani. International Law Commission, *Draft Articles on the Effects of Armed Conflicts on Treaties*, in *Yearbook of the International Law Commission*, 2011, vol. II, part II.

[283] Nel parere consultivo inerente alla liceità della minaccia o dell'utilizzo dell'arma nucleare, la Corte internazionale di giustizia ha affermato, con riferimento al Patto delle Nazioni Unite sui diritti civili e politici del 1966, che le garanzie in esso contenute non cessano in tempo di guerra, a meno che non si invochi l'art. 4 dello stesso, secondo cui talune norme possono essere derogate in caso di emergenza nazionale. International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 25.

dell'uomo[284], la Corte interamericana dei diritti dell'uomo[285], la Commissione dei reclami tra Eritrea ed Etiopia[286], il Tribunale penale per la *ex* Iugoslavia[287] e, non da ultimo, il Comitato internazionale della Croce Rossa[288].

Alla luce di quanto precede, appare evidente come, durante un conflitto armato, devono essere applicate tanto le norme umanitarie, quanto quelle sui diritti umani. Queste ultime vincolano i belligeranti sia in caso di attacchi convenzionali, che nelle ipotesi di attacchi informatici.

6. Attacchi informatici e rapporto di neutralità

Con l'entrata in vigore della Carta delle Nazioni Unite e l'affermarsi del divieto di aggressione, l'istituto della neutralità ha perso gran parte della sua importanza, dal momento che agli Stati membri dell'Organizzazione non si richiede più di rimanere imparziali ed equidistanti dalle parti belligeranti, bensì si permette loro di assistere lo Stato aggredito ed eventualmente di intervenire contro quello aggressore[289].

---

[284] La Corte europea dei diritti dell'uomo, con decisione del 2021, ha dichiarato la Russia colpevole di aver violato diverse disposizioni della Convenzione a causa degli attacchi indiscriminati contro la popolazione civile della Georgia, respingendo, di fatto, le eccezioni della Russia secondo cui la Convenzione europea dei diritti dell'uomo non era applicabile perché, all'epoca dei fatti, era in corso un conflitto armato internazionale. Corte europea dei diritti dell'uomo, *Georgia c. Russia*, ricorso n. 38263/08, 21 gennaio 2021.

[285] La Commissione interamericana dei diritti dell'uomo nel rapporto n. 109/99, relativa al caso «*Coard et al. c. United States*» del 1999, ha sottolineato che l'applicazione del diritto umanitario non esclude affatto quella dei diritti umani, che rilevano, dunque, anche in luogo di conflitto armato. Commissione interamericana dei diritti dell'uomo, *Coard et al. v. United States*, ricorso n. 10.951, 29 settembre 1999, par. 39.

[286] Anche secondo la Commissione Eritrea-Etiopia il diritto umanitario non rappresenta di per sé un limite o, comunque, un impedimento alla concorrente applicazione delle norme in materia di diritti umani in situazioni di conflitto armato. EECC, *Partial Award*, *Eritrea's Claims 15,16, 2327-32*, 17 December 2004, para. 5.

[287] Il Tribunale penale internazionale per la *ex* Iugoslavia, nella sentenza del 2001 riguardante il caso «*Prosecutor v. Kunarac*», ha affermato che l'attuazione delle regole applicabili in tempo di pace a tutela dei diritti umani non può essere esclusa nei conflitti armati. Tribunale penale internazionale per la *ex* Iugoslavia, *Prosecutor v. Kunarac, Kovač e Vuković*, caso n. IT-96-23/1-T, sentenza del 22 febbraio 2001, par. 467.

[288] Anche nello studio del Comitato internazionale della Croce Rossa sul carattere consuetudinario del diritto umanitario è stata sostenuta l'applicabilità congiunta del diritto umanitario e dei diritti umani durante i conflitti armati. J. M. Henckaerts, L. Doswald-Beck (eds.), *Customary International Humanitarian Law*, *Vol. 1: Rules*, cit., p. 115 ss.

[289] M. Gavouneli, *Neutrality - A Survivor?*, in *European Journal of International Law*, 2012, pp. 267-273.

Tuttavia, con l'avvento di Internet e la creazione del cyberspazio, può osservarsi come la neutralità abbia assunto una dimensione tutt'altro che residuale e marginale nel diritto internazionale contemporaneo[290].

I sistemi informatici situati nel territorio di uno Stato neutrale potrebbero, infatti, essere utilizzati, da ciascuno dei belligeranti, nel corso di un conflitto armato internazionale, per sferrare un attacco informatico contro lo Stato nemico. Si pone, così, il problema riguardante l'integrità territoriale e la neutralità degli Stati terzi al conflitto.

La neutralità è uno *status* che comporta specifici diritti e doveri per i soggetti che si trovino in tale situazione[291]. La condizione dello Stato neutrale si caratterizza per la sua terzietà al conflitto armato e la sua equidistanza rispetto ad ambedue le parti in lotta[292]. Deve definirsi neutrale, dunque, lo Stato che non prende parte alle ostilità[293].

Quanto al momento in cui la neutralità ha inizio, la condizione necessaria per il suo sorgere è l'effettiva sussistenza di un rapporto bellico tra due o più Stati. Non ogni conflitto armato internazionale rende però applicabile la neutralità. L'applicazione del diritto di neutralità dipende, infatti, dalla soglia di violenza del conflitto bellico, implicando, pertanto, la sussistenza di scontri armati di una certa intensità. In altri termini, un semplice incidente di frontiera non fa scattare il meccanismo della neutralità[294]. Non sono richieste, invece, né una dichiarazione di neutralità da parte

---

[290] P. G. K. Walker, *Information Warfare and Neutrality*, in *Vanderbilt Journal of Transnational Law*, 2000, pp. 1995-2002.

[291] E. Castren, *The Present Law of War and Neutrality*, Helsinki, 1954; L. Oppenheim, *International law*, *Vol. II, War and Neutrality*, 1981, Ney York, pp. 300-398; A. Spring, *The International Law Concept of Neutrality in the 21 Century*, Zurich, 2014; J. Upcher, *Neutrality in Contemporary International Law*, Oxford, 2015.

[292] La neutralità è la posizione giuridica di uno Stato che non partecipa ad un conflitto armato in corso fra altri Stati. Questa non trova, quindi, applicazione nei conflitti armati interni (o guerre civili).

[293] Si tratta di una condotta volontaria, nel senso che lo Stato può successivamente decidere di prendere parte al conflitto bellico (ma finché resta neutrale esso è obbligato, beninteso, ad osservare le norme del diritto di neutralità). Al contrario, la neutralità rappresenta una condotta dovuta per quegli Stati che, come Malta, seguono una politica di neutralità permanente, cioè per gli Stati che sono obbligati a comportarsi da neutrali sulla base di un trattato internazionale, di regola, concluso in tempo di pace.

[294] N. Ronzitti, *Neutralità*, in S. Cassese (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, p. 6.

dello Stato che non intende prendere parte al conflitto armato, né l'esistenza formale di uno stato di guerra[295].

La condizione di neutralità termina con la cessazione delle ostilità, confermata da un trattato di pace, da un armistizio di natura permanente, dal Consiglio di sicurezza delle Nazioni Unite, oppure, ancora, quando lo Stato neutrale interviene a fianco del belligerante[296].

Per descrivere sinteticamente gli obblighi della neutralità, si afferma che il neutrale è obbligato a conformarsi a tre doveri fondamentali nei confronti dei belligeranti: astensione, prevenzione ed imparzialità[297].

Il principale obbligo dello Stato neutrale è quello di non permettere che il suo territorio diventi una base per lo svolgimento delle operazioni militari di taluno dei belligeranti[298]. Di conseguenza, il neutrale non può consentire che all'interno del suo territorio vengano formati corpi di combattimento o uffici di arruolamento[299].

Lo Stato neutrale dovrà pure interdire il passaggio dal suo territorio di ogni tipo di materiale bellico o di truppe, qualora tale passaggio avvenga per scopi militari[300].

Dovendo mantenere la propria imparzialità nei confronti dei belligeranti, il neutrale deve inoltre esimersi dal fornire aiuti militari all'uno o a all'altro Stato impegnato nel conflitto[301].

Infine, la Potenza neutrale deve astenersi dal compiere atti di ostilità nei confronti dell'uno o dell'altro belligerante. Tuttavia, ai sensi dell'art. 10 della V Convenzione

---

[295] *Ibidem*.

[296] M. Bothe, *The Law of Neutrality*, in D. Fleck (ed.), *The Handbook of International Humanitarian Law*, cit., p. 571 ss.

[297] La condizione di neutralità, si badi, non può essere invocata per sottrarsi agli obblighi solidali imposti dal diritto internazionale umanitario. Lo Stato neutrale ha invero il diritto di fornire supporto umanitario e apprestare aiuto ai feriti, ai malati ed ai prigionieri di guerra.

[298] I cittadini del belligerante possono soggiornare in territorio neutrale senza però compromettere la neutralità dello Stato che li ospita, ovvero senza compiere atti di ostilità contro l'altro belligerante. Parimenti, la neutralità non è compromessa se il neutrale concede rifugio a disertori appartenenti ai belligeranti.

[299] L'art. 4 della V Convenzione dell'Aia del 1907 prescrive che il neutrale non possa tollerare tali attività, che devono, quindi, essere impedite. Non costituisce, invece, una violazione della neutralità il fatto che cittadini dello Stato neutrale si arruolino isolatamente nell'esercito dell'uno o dell'altro belligerante.

[300] Tale transito è ammissibile solo come misura richiesta dal Consiglio di sicurezza (art. 43, par. 1 della Carta delle Nazioni Unite). P. Seger, *The Law of Neutrality*, in P. Gaeta, A. Clapham (eds.), *The Oxford Handbook of International Law in Armed Conflict*, Oxford, 2014, p. 248 ss.

[301] *Ibidem*.

dell'Aia sulla neutralità nella guerra terrestre del 1907, il neutrale ha il diritto di respingere, anche con la forza, eventuali attacchi provenienti dalle parti belligeranti che rappresentino un concreto attentato alla propria neutralità.

Non esiste alcuna norma internazionale che vieti il commercio tra Stati neutrali e Stati belligeranti, tranne che tale commercio non sia impedito da una decisione del Consiglio di sicurezza delle Nazioni Unite. Dalla regola generale testé enunciata si discosta però la disciplina del traffico di armi. A tal fine, si distingue, in dottrina, tra commercio statale e commercio privato. Lo Stato neutrale non può mai trasferire armi ai belligeranti, pena la violazione del diritto di neutralità. Esso non è, tuttavia, obbligato ad impedire che i suoi cittadini o le sue imprese vendano armi alle parti in conflitto[302]. L'art. 7 della V Convenzione dell'Aia, infatti, statuisce che una Potenza neutrale non è tenuta ad impedire la vendita o il transito, per conto dei belligeranti, di armi, munizioni e, in genere, tutto ciò che può essere utile ad un esercito o una flotta.

Le regole relative al trasferimento di armi possono essere applicate, *mutatis mutandis*, anche alle tecnologie informatiche destinate ad un uso militare. La loro concessione da parte dello Stato neutrale, in favore di uno dei belligeranti, comporta inevitabilmente una violazione del dovere di neutralità. Ma il neutrale non è tenuto ad impedirne la vendita da parte di privati.

A loro volta, i belligeranti hanno l'obbligo di rispettare il territorio del neutrale. L'art. 1 della V Convenzione dell'Aia del 1907 dispone, invero, che «il territorio delle Potenze neutrali è inviolabile».

La proibizione ha per oggetto tanto la conduzione di ostilità in territorio neutrale, quanto l'impiego di armi che possono causare effetti al di là delle frontiere[303]. Tale principio è stato ribadito dalla Corte internazionale di giustizia nel parere consultivo riguardante la liceità delle armi nucleari ed è, oggi, ritenuto appartenente al diritto consuetudinario[304].

---

[302] Ovviamente lo Stato neutrale può impedire la fornitura di armi da parte dei privati. Ma se agisce in questo modo, esso deve proibire il traffico di armi nei confronti di tutti i belligeranti, altrimenti commetterebbe una violazione del dovere di imparzialità.

[303] M. Bothe, *The Law of Neutrality*, cit., p. 571 ss.

[304] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 88.

Il Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica, con riferimento all'istituto giuridico della neutralità, stabilisce che il belligerante non può sferrare attacchi informatici diretti contro le infrastrutture critiche dello Stato neutrale (art. 91) e non può effettuare operazioni cibernetiche nel territorio di quest'ultimo (art. 92). Al contempo, la Potenza neutrale ha il dovere di impedire ai belligeranti l'uso delle strutture cibernetiche presenti all'interno del suo territorio (art. 93).

Il Manuale, seppur implicitamente, richiama l'obbligo assoluto imposto agli Stati belligeranti di rispettare il territorio neutrale e, in secondo luogo, il dovere dello Stato neutrale non soltanto di astenersi dal compiere atti ostili nei confronti dell'uno o dell'altro belligerante, ma anche di impedire che il suo territorio venga utilizzato, pure solo indirettamente, da uno di questi a proprio vantaggio[305].

Tuttavia, l'attuazione delle regole contenute nel Manuale di Tallinn presume un livello di controllo da parte delle Potenze belligeranti sulle strutture cibernetiche presenti in territorio neutrale che appare, a dire il vero, poco realistico. A causa delle peculiari caratteristiche dello strumento telematico e delle modalità con cui avviene il Traffico Internet, può rivelarsi, invero, particolarmente difficile per le parti impegnate nel conflitto armato, al momento di compiere atti ostili di natura informatica, astenersi dall'utilizzare le infrastrutture cibernetiche di proprietà dello Stato neutrale.

Allo stesso tempo, per quest'ultimo è quasi impossibile impedire che il belligerante si avvalga anche dei sistemi informatici presenti nel suo territorio, al fine di effettuare un attacco telematico contro l'avversario.

Gli attacchi informatici, di solito, coinvolgono un traffico transfrontaliero di dati[306]. Limitare o respingere detto flusso transfrontaliero di dati richiede, in pratica, un monitoraggio costante, da parte del neutrale, dell'intera attività di rete[307]. Un simile

[305] C. Antonopoulos, *Non-Participation in Armed Conflict: Continuity and Modern Challenges to the Law of Neutrality*, Cambridge, 2022, p. 216.
[306] J. C. Woltag, *Cyber Warfare*, in *MPEPIL*, 2012.
[307] W. H. Von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013, p. 141 ss.

obbligo, gravante sullo Stato neutrale, sarebbe per questi particolarmente difficile da adempiere[308].

Al contrario di quanto sostenuto da taluni autori, il flusso di dati attraverso cui un attacco informatico può realizzarsi non va equiparato al movimento di munizioni o, ancora, alla circolazione di truppe in territorio neutrale[309]. Per tale motivo, secondo chi scrive, l'eventuale utilizzo delle infrastrutture informatiche poste in territorio neutrale, allo scopo di lanciare un attacco telematico contro l'avversario, da parte di taluno dei belligeranti, non comporta una violazione degli obblighi e dei doveri di neutralità.

Ciò trova conferma tanto nell'art. 8 della V Convenzione dell'Aia, secondo cui: «Una Potenza neutrale non è tenuta a proibire o a restringere l'uso, da parte dei belligeranti, dei cavi telegrafici o telefonici e degli apparecchi di telegrafia senza filo, siano essi di sua proprietà, oppure proprietà di compagnie o di privati», quanto nella disciplina dettata dal Manuale di Harvard sul diritto internazionale applicabile alla guerra aerea, il quale, alla regola 168 (*b*), afferma testualmente che: «*However, when Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality*»[310].

Quanto detto, tuttavia, vale soltanto per gli attacchi informatici che, originati nel territorio del belligerante, attraversano successivamente le strutture cibernetiche dello Stato neutrale prima di aver raggiunto e colpito l'obiettivo[311]. Diversa, invece, è la situazione in cui gli attacchi telematici contro la Potenza avversaria vengono generati direttamente mediante le strutture informatiche presenti nel territorio del neutrale[312].

---

[308] *Ibidem*.
[309] J. T. G. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, in *Michigan Law Review*, 2008, pp. 1443-1445.
[310] Program on Humanitarian Policy and Conflict Research at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare*, Bern, 2009, Section X, Rule 168 (b).
[311] M. Roscini, *Cyber Operations and the Use of Force in International Law*, cit., pp. 259-261.
[312] Occorre, in altri termini, distinguere tra «Stato di lancio» e «Sato di transito» dell'operazione informatica.

In tali ipotesi, viceversa, l'utilizzo dei sistemi informatici situati nel territorio del neutrale deve ritenersi certamente vietato e sorge in capo alla Potenza neutrale l'obbligo di prevenire, impedire o far cessare, con tutti i mezzi a sua disposizione, l'attacco cibernetico sferrato[313].

Nel 2008, prima dell'inizio del conflitto armato russo-georgiano, la Georgia subì gravi danni alle proprie infrastrutture, compresi i servizi di telecomunicazione[314]. Un certo numero di siti web governativi, incluso quello della Presidenza, del Parlamento e del ministero degli Affari esteri, fu preso di mira da numerosi attacchi telematici provenienti dal territorio della Federazione Russa[315]. Tali attacchi ebbero come effetto principale quello di impedire le comunicazioni da parte del governo georgiano ai suoi cittadini nei momenti in cui la Russia effettuò l'attacco armato convenzionale[316].

Di conseguenza, diversi *servers* di Google ubicati nel territorio della California vennero impiegati da remoto al fine ristabilire e consentire provvisoriamente le comunicazioni[317].

Ora, secondo taluni autori, il ripristino delle funzionalità della rete Internet georgiana, attraverso l'utilizzo dei predetti *servers* ubicati nel territorio degli Stati Uniti, avrebbe costituito una violazione della legge sulla neutralità[318].

A nostro parere, viceversa, deve escludersi che lo Stato neutrale sia costretto ad impedire l'uso dei propri sistemi informatici alle Potenze belligeranti per la sola

---

[313] Si tratta, a ben guardare, di un obbligo giuridico di dovuta diligenza. J. M, Lemnitzer, *Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace*, in *European Journal of International Law*, 2022, p. 789 ss.

[314] B. Rohan, *Georgia says Russian hackers block govt websites*, *Reuters*, 11 August 2008.

[315] Le autorità russe hanno sempre respinto la loro responsabilità in merito all'attacco in commento. Ciononostante, diversi esperti informatici hanno affermato che l'operazione era stata effettuata da un gruppo di individui meglio noto come "*Russian Business Network*", il quale avrebbe avuto stretti rapporti con il governo russo. Vedi: S. Gorman, *Georgia States Computers Hit By Cyberattack*, *The Wall Street Journal*, 12 August 2008; J. Markoff, *Before the gunfire, cyberattacks*, *The New York Times*, 12 August 2008; L. Swanson, *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict*, in *Loyola of Los Angeles International and Comparative Law Review*, 2010, p. 303 ss.

[316] J. Swaine, *Georgia: Russia "conducting cyber war"*, *The Telegraph*, 11 August 2008.

[317] K. Hart, *Longtime Battle Lines are Recast in Russia and Georgia's Cyberwar*, *The Washington Post*, 14 August 2008.

[318] J. E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, in *AFL Review*, 2009, pp. 57-64.

eventuale trasmissione di notizie riguardanti le operazioni belliche o, ancora, per la trasmissione di informazioni di carattere non militare rivolte alla propria popolazione civile[319].

Vi è, infatti, una notevole differenza tra l'uso, da parte delle Potenze belligeranti, delle infrastrutture cibernetiche neutrali volto a condurre attacchi informatici contro l'avversario e l'impiego delle siffatte strutture per trasmettere comunicazioni alla popolazione civile coinvolta nel conflitto.

[319] Ad ogni modo, è fatto divieto alle Potenze belligeranti di utilizzare il territorio del neutrale per installarvi apparecchi di comunicazione (art. 3 della V Convenzione dell'Aia del 1907 sui diritti e i doveri delle potenze neutrali nella guerra terrestre).

CAPITOLO II

Le norme e i principi che regolano la condotta dei belligeranti

Le infrastrutture statali oggetto di attacco informatico difficilmente assolvono solo ed esclusivamente una funzione di carattere militare. Un attacco telematico diretto contro una di esse si traduce, pertanto, nella maggior parte dei casi, anche in un attacco contro un obiettivo di tipo civile, circostanza che può facilmente configurare una violazione dei principi di proporzionalità, distinzione e precauzione.

Tali principi cardine sono alla base dell'insieme delle norme – consuetudinarie e convenzionali – del diritto internazionale applicabile ai conflitti armati e modellano il contenuto e l'applicazione di tali norme giuridiche anche, come vedremo, nei casi di attacchi di natura informatica[320].

Il teatro in cui i combattimenti si svolgono è, invero, del tutto irrilevante e il diritto internazionale umanitario si applica ovunque un conflitto armato si verifichi[321]. L'art. 1 «comune» alle quattro Convenzioni di Ginevra del 1949, come è noto, impone alle parti contraenti l'obbligo di rispettare il diritto umanitario in tutte le circostanze. Ciò porta a ritenere che tutti i tipi di conflitto armato, compresi quelli del futuro combattuti con mezzi e metodi di guerra non convenzionali, siano ricompresi in questo obbligo. Poiché l'obiettivo della norma è quello di proporre una migliore e più efficace tutela della popolazione civile e dei beni di carattere civile, è chiaro che tale obiettivo non potrebbe essere raggiunto, in tutto o in parte, se non si adottasse un'interpretazione evolutiva della norma stessa, tale da includere nel suo campo di applicazione anche le operazioni militari nello spazio cibernetico.

---

[320] Tali principi, per la loro natura consuetudinaria e la loro portata generale, si applicano a tutti i tipi di conflitto armato e ad ogni forma di violenza bellica, inclusa quella in qualsiasi modo collegata allo spazio cibernetico.

[321] Come è noto, il diritto internazionale regola i rapporti fra Stati. Da ciò consegue la sua applicabilità a tutti gli spazi nei quali essi possono agire, compreso quello cibernetico. M. C. Vitucci, *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino*, in *La Comunità internazionale*, 2023, p. 7.

1. La regola della proporzionalità

La regola della proporzionalità trova la propria *ratio* nella constatazione che nel corso di un attacco contro un obiettivo militare legittimo possono essere causati danni collaterali alla popolazione civile o ai beni ad essa appartenenti[322]. Per un verso, le necessità della guerra implicano che si debba comunque procedere con l'attacco; per altro verso, si vuole impedire che i danni collaterali siano sproporzionati rispetto al vantaggio militare conseguito[323]. Partendo, pertanto, dal presupposto che nessun metodo o mezzo di conduzione delle ostilità, per quanto sofisticato, possa evitare del tutto il rischio di danni collaterali, si pretende che i danni inflitti ai civili o ai loro beni siano commisurati (o in ogni caso non eccessivi rispetto) allo specifico vantaggio militare che il belligerante si attende di ottenere mediante l'attacco[324].

Il principio di proporzionalità svolge, così, un ruolo essenziale nel limitare i danni provocati dal conflitto armato nei confronti della popolazione civile[325]. Esso è, oggi, codificato nell'art. 51, par. 5, lett. *b*), del I Protocollo Aggiuntivo del 1977, il quale impone ai belligeranti il divieto di condurre attacchi suscettibili di produrre morti e feriti fra la popolazione civile, danni ai beni di carattere civile o, ancora, una combinazione di perdite di vite umane e di danni, che risulterebbero eccessivi rispetto al vantaggio militare previsto. La disposizione – incorporata in numerosi manuali militari[326] ed appartenente al diritto consuetudinario[327] – è applicabile anche ai conflitti armati non internazionali[328].

Il I Protocollo non detta una formula matematica per misurare la proporzione tra vantaggio militare e danni collaterali alla popolazione o ai beni di natura civile, ma

---

[322] J. van den Boogaard, *Proportionality in International Humanitarian Law. Refocusing the Balance in Practice*, Cambridge, 2023, p. 13 ss.
[323] G. Venturini, *Necessità e proporzionalità nell'uso della forza militare in diritto internazionale*, Milano, 1988, p. 130.
[324] A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 129.
[325] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 272.
[326] UK Ministry of Defence, *The Manual of the Law of Armed Conflict*, Oxford, 2004, p. 86.
[327] W. H. von Heinegg, *Proportionality and Collateral Damage*, in *MPEPIL*, 2015.
[328] ICRC, *International Humanitarian Law Database*, Rule 14.

si fonda soltanto sulla nozione di danno collaterale "eccessivo", con la conseguenza che la proporzionalità sarà del tutto assente quando i danni collaterali risulteranno "eccessivi" rispetto al vantaggio militare perseguito.

Nel configurare l'entità del vantaggio militare, secondo la dottrina maggioritaria, occorre fare riferimento ai soli effetti diretti e concreti della condotta bellica, non potendo entrare nel calcolo – ai fini dell'applicazione della regola – né i vantaggi militari indiretti, né quelli concretamente non misurabili, come per esempio le conseguenze di natura psicologica[329]. Secondo una parte minoritaria della dottrina, viceversa, un'operazione il cui scopo principale sia di natura psicologica o i cui vantaggi militari siano soltanto indiretti risulta di dubbia legittimità[330].

Quello previsto dal testo dell'art. 51, par. 5, lett. *b*), del I Protocollo del 1977 è un giudizio di bilanciamento prognostico, da effettuarsi sulla base delle informazioni disponibili al momento in cui si assume la decisione di procedere all'attacco[331]. Il vantaggio militare, invero, può essere previsto dall'attaccante durante la fase di preparazione dell'operazione, ma la sua effettiva portata può essere valutata solo *a posteriori*, cioè dopo la consumazione dell'attacco[332].

Non è chiaro se, ai fini della misurazione del vantaggio militare, debba essere preso in considerazione ogni singolo attacco su un determinato obiettivo, più attacchi rientranti in un'unica operazione o, ancora, l'intero arco di tempo in cui si svolge il conflitto. Secondo Ronzitti, si potrà prendere in considerazione, come termine di misurazione, un'intera operazione complessiva di più attacchi, ma non l'intero conflitto[333]. Tale posizione è sostenuta anche da molti Stati NATO[334]. Il Regno Unito, ad esempio, ha dichiarato che il vantaggio militare previsto deve riguardare

[329] W. H. von Heinegg, *Proportionality and Collateral Damage*, in *MPEPIL*, 2015.
[330] S. Knuckey, A. Moorehead, A. McCalley, A. Brown, *The Proportionality Rule and Mental Harm in War*, in C. Kress, R. Lawless (eds.), *Necessity and Proportionality in International Peace and Security Law*, Oxford, 2021, pp. 407-408.
[331] A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 130.
[332] G. Venturini, *Necessità e proporzionalità nell'uso della forza militare in diritto internazionale*, cit., p. 131.
[333] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 273.
[334] A. Roberts, R. Guelff, *Documents on the Law of War*, Oxford, 2000, p. 511.

quello conseguente all'attacco complessivamente considerato e non solamente quello che discende da parti specifiche dell'operazione[335].

Diversamente, a nostro parere, il calcolo del vantaggio militare a cui fa espresso riferimento la disposizione andrebbe effettuato con riferimento ad ogni singolo obiettivo oggetto di attacco e non all'insieme degli obiettivi rientranti in un'unica operazione. Ciò è sostenuto anche dal Comitato internazionale della Croce Rossa[336] e dal Parlamento svizzero che, con riferimento all'uso di droni in luogo di conflitto armato, ha espressamente dichiarato che: «*In armed conflicts, strikes carried out with armed drones must respect the rules of the conduct of hostilities as stipulated by international humanitarian law, including the principle of proportionality. For each strike, it is thus necessary to verify that this principle was respected*»[337].

Da non condividere sarebbe, quindi, l'assunto della Commissione dei reclami Eritrea-Etiopia secondo cui il vantaggio militare previsto dall'operazione deve essere rapportato al conflitto armato nella sua interezza e non ad ogni specifico attacco[338]. La tesi sostenuta dalla Eritrea-Ethiopia Claims Commission (EECC) non sembra trovare, in effetti, alcun fondamento nella prassi.

Anche la posizione dei civili e dei beni civili può determinare una differenza di calcolo[339]. È ovvio che l'applicazione del principio di proporzionalità comporta non pochi problemi quando le operazioni belliche abbiano luogo in un'area densamente popolata e, in particolare, in un contesto urbano[340].

In ogni caso, il vantaggio militare e l'entità dei danni collaterali sono i soli fattori che le parti in conflitto devono tenere in considerazione ai fini del giudizio di

---

[335] *Ibidem*.

[336] ICRC, Statement at the UN Diplomatic Conference of Plenipotentiaries on the Establishment of an International Criminal Court, 8 July 1998, UN Doc. A/CONF.183/INF/10, 13 July 1998, p. 1, par. 2

[337] Switzerland, *Answer by the Federal Council to interpellation 13.3245 in Parliament regarding the use of drones*, 29 May 2013.

[338] EECC, 19 December 2005, *Partial Award, Western Front, Aerial Bombardment and Related Claims – Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 & 26 between the State of Eritrea and the Federal Democratic Republic of Ethiopia*, *Partial Award*, par. 113.

[339] M. Sossai, *The Place of Cities in the Evolution of International Humanitarian Law*, in *Italian Yearbook of International Law*, 2021, pp. 237-242.

[340] *Ibidem*.

proporzionalità, a nulla rilevando il rischio a cui la scelta di un certo mezzo o metodo di combattimento al posto di un altro esporrebbe le proprie forze armate[341]. La violazione del principio in discorso costituisce un grave crimine di guerra. L'art. 8, par. 2, lett. *b)* (iv), dello Statuto della Corte penale internazionale rende, infatti, punibile colui che abbia deliberatamente sferrato un attacco sapendo che tale attacco avrebbe cagionato danni accidentali alla popolazione civile o ai suoi beni chiaramente eccessivi rispetto al concreto e diretto vantaggio militare che ci si attendeva dall'operazione.

Le parti belligeranti hanno l'obbligo di risarcire le vittime di un attacco che risulti sproporzionato, in conformità con quanto stabilito dall'art. 91 del I Protocollo Aggiuntivo. Queste devono anche istituire procedimenti penali laddove vi siano elementi sufficienti per ritenere che l'attacco sproporzionato sia stato sferrato intenzionalmente, oppure sia il frutto di grave negligenza[342].

Nella prassi, il principio di proporzionalità è stato affermato, ad esempio, dalla Commissione d'inchiesta sul conflitto tra Israele e Libano, la quale ha stabilito, nel rapporto del 23 novembre 2006, che l'attacco dell'esercito israeliano nei confronti delle truppe di Hezbollah aveva comportato un utilizzo eccessivo, indiscriminato e sproporzionato della forza armata[343].

Ora, sembra non residuino dubbi sul fatto che il principio in oggetto regoli tutte quelle *cyber operations*, in concreto, suscettibili di costituire un attacco ai sensi del diritto internazionale umanitario[344]. Come osservato da Roscini: "*The question is not if, but how the principle of proportionality applies to cyber operations*"[345].

---

[341] Di conseguenza, da un lato, se il mezzo o metodo di guerra prescelto consente di contenere il danno collaterale entro limiti accettabili, il belligerante non è tenuto a scegliere un mezzo o metodo di combattimento alternativo, che comporti un rischio maggiore per le proprie truppe, ma minore per i civili ed i beni civili. Dall'altro lato, laddove i danni collaterali possano essere ridotti entro i limiti della proporzionalità solamente adottando un mezzo o metodo di guerra più rischioso per le forze armate impegnate nell'operazione, il belligerante non avrà altra scelta se non accettare tali rischi o desistere dall'attacco. A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 130.

[342] In argomento, A. Gattini, *Le riparazioni di guerra nel diritto internazionale*, Padova, 2003.

[343] Human Rights Council, *Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council resolution S-2/1*, 23 November 2006, doc. n. A/HRC/3/2.

[344] H. H. Koh, *International Law in Cyberspace*, in *Harvard International Law Journal*, 2012, p. 5.

[345] M. Roscini, *Cyber Operations and the Use of Force in International Law*, cit., p. 220.

La concreta applicazione del principio di proporzionalità, nel contesto informatico, si può rivelare, invero, di difficile realizzazione. Due sono, in particolare, i piani dove tale difficoltà può manifestarsi: il primo riguarda la complessa qualificazione del danno alla luce della assai frequente doppia natura degli obiettivi tipici di un attacco telematico, mentre il secondo concerne l'altrettanto delicata questione dell'identificazione del vantaggio militare nel quadro delle *cyber operations*.

Cominciando dalla prima questione, relativa all'ampiezza del concetto di danno collaterale ai sensi del diritto internazionale umanitario, le conseguenze dannose di un attacco cibernetico si rivelano principalmente sul piano degli effetti indiretti[346]. Più precisamente, gli effetti prodotti da un attacco di tipo cibernetico possono essere distinti in tre differenti sotto-categorie: in primo luogo vi sono quelli direttamente causati ai dati ed al sistema informatico colpito dal cyber attacco (c.d. effetti diretti o primari); in secondo luogo vi sono quelli prodotti alla infrastruttura fisica gestita dal sistema informatico oggetto dell'attacco cyber (c.d. effetti indiretti secondari); da ultimo, devono essere annoverati gli effetti incidentali che si ripercuotono, solo in un secondo momento, sulla popolazione civile interessata dalla distruzione oppure dal malfunzionamento del sistema informatico della infrastruttura bersagliata (c.d. effetti indiretti terziari)[347].

Tali effetti rientrano tutti nella nozione di danno collaterale qualora previsti come conseguenza – diretta o indiretta – dell'attacco informatico al momento della sua pianificazione, approvazione o esecuzione[348]. Così, come affermato da Dinstein: "*As far as a Computer Network Attack is concerned, if – while disrupting some military electronic systems in a minor way – it causes irreparable damage to the civilian infrastructure (e.g. water management, research centres, banking systems, stock exchanges), this should be adjudged excessive*"[349].

---

[346] R. G. Wedgwood, *Proportionality, Cyberwar, and the Law of War*, in *International Law Studies*, 2002, p. 228.
[347] N. C. Rowe, *Distinctive Ethical Challenges of Cyberweapons*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., pp. 316-324.
[348] B. T. O'Donnell, J. C. Kraska, *International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement*, in *International Law Studies*, 2002, pp. 412-413.
[349] Y. Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, in *Journal of Conflict and Security Law*, 2012, p. 272.

Passando ora all'esame della seconda questione precedentemente evocata relativa all'identificazione del vantaggio militare, come sottolineato da Doyle, allo scopo di limitare l'entità dei danni incidentali cagionati da un attacco telematico appare di fondamentale importanza un'accurata mappature delle rete Internet avversaria, nonché la presenza di esperti informatici tra i membri delle forze armate dello Stato attaccante, considerate le conoscenze tecniche che risultano necessarie per un corretto esercizio di ponderazione nel momento in cui si decide di procedere con l'operazione[350].

Infine, a nostro giudizio, sarebbe conforme alla finalità umanitaria delle norme di *ius in bello* che le parti in lotta sottopongano la propria condotta ad una procedura di accertamento, in caso di controversia successiva all'attacco cibernetico lanciato. In particolare, il belligerante che ha effettuato l'attacco informatico, cui in seguito si contesti di aver provocato perdite collaterali sproporzionate, dovrebbe fornire ad un organismo internazionale imparziale ed indipendente (o ad ogni altro organismo competente), nel corso del conflitto o al termine di questo, tutti gli elementi di cui era in possesso – al momento dell'attacco – suscettibili di provare la sussistenza del vantaggio militare atteso.

2. Il principio di distinzione e il problema della qualificazione giuridica dei dati informatici

L'utilizzo di *computer network attacks*, nel corso di un conflitto armato, rende particolarmente complessa l'applicazione del principio di distinzione poiché non è affatto raro che ad essere oggetto di attacchi informatici siano infrastrutture – quali, ad esempio, dighe, raffinerie, oleodotti, installazioni petrolifere, impianti nucleari, centrali destinate alla produzione di energia elettrica – che quasi sempre assolvono una doppia funzione civile e militare.

Oggi codificato nell'art. 48 del I Protocollo Aggiuntivo del 1977, il principio di distinzione costituisce una delle regole fondamentali del diritto dei conflitti

[350] J. H. Doyle, *Computer Networks, Proportionality, and Military Operations*, in *International Law Studies*, 2002, p. 159.

armati[351]. Esso impone, a carico di ciascuna delle parti belligeranti, l'obbligo di dirigere la propria violenza bellica solamente verso obiettivi militari e combattenti, vietando, dunque, gli attacchi contro la popolazione civile e i suoi beni[352].

Il mancato rispetto del principio in commento costituisce un crimine di guerra tanto nei conflitti armati internazionale[353], quanto in quelli non internazionali[354]. Sebbene non incorporato nel II Protocollo Aggiuntivo del 1977, il divieto di attaccare i civili e i loro beni rileva, invero, anche nei conflitti armati interni[355].

Non sempre risulta facile distinguere, in concreto, tra beni civili e obiettivi militari. A tal proposito, l'art. 52, par. 1, del I Protocollo Aggiuntivo del 1977 dispone che: «*Civilian objects shall not be the object of attack or of reprisals. Civilian objects are all objects which are not military objectives as defined in paragraph two*». La norma, a ben guardare, non fornisce né una definizione, né una elencazione di beni di carattere civile, limitandosi a considerare tali tutti i beni non qualificabili come obiettivi militari ai sensi del suo secondo paragrafo.

Ora, secondo una parte della dottrina, il significato dell'espressione «*civilian objects*», contenuto nel testo inglese della citata disposizione, si è evoluto nel tempo, sino ad includere anche i beni immateriali e intangibili, come ad esempio i dati informatici[356].

La tesi si basa sostanzialmente sulla considerazione che le disposizioni del I Protocollo del 1977 debbano essere lette alla luce dell'oggetto e dello scopo del trattato (c.d. interpretazione teleologica), nonché nel senso di dare ai termini in esso presenti un significato ed un contenuto suscettibili di evolvere nel tempo (c.d. interpretazione evolutiva)[357].

---

[351] Corte internazionale di giustizia, *Nuclear Weapons Case*, cit., par. 79.
[352] N. Melzer, *Targeted Killing in International Law*, Oxford, 2008, p. 300.
[353] Art. 8, par. 2, lett. (b) (i) dello Statuto della Corte penale internazionale.
[354] Art. 8, par. 2, lett. (*e*) (i) dello Statuto della Corte penale internazionale.
[355] Tribunale penale internazionale per la *ex* Iugoslavia, *Prosecutor v Tadić*, Appeals Chamber, Decision, Case no. IT-94-1-A, 2 October 1995, para. 126. In dottrina si veda: N. Melzer, *Targeted Killing in International Law*, cit., p. 311.
[356] K. Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, in *Israel Law Review*, 2015, p. 55 ss.
[357] *Ivi*, pp. 68-80.

Taluni autori, diversamente, hanno rifiutato una simile lettura della disposizione, ritenendo che con l'espressione «*civilian objects*» si debba e possa intendere soltanto un oggetto avente carattere tangibile e materiale[358]. Alla luce di questa impostazione, il Protocollo deve essere interpretato nel suo significato ordinario (c.d. interpretazione testuale) e non si possono legittimare risultati interpretativi che vadano oltre la volontà delle parti resa palese nel testo del trattato[359]. Tale posizione è ribadita altresì nel Commentario ai due Protocolli Aggiuntivi del 1977, secondo cui: «*an object is characterized as something visible and tangible*»[360] e trova, peraltro, conferma nel Manuale di Tallinn alla regola 38[361].

Infine, in base ad un terzo orientamento, spetta agli Stati, in futuro, stabilire se i dati elettronici rientrino o meno nella nozione di bene civile dettata dalla norma[362].

Dinnis, a sua volta, distingue due differenti categorie di dati: a) quelli denominati "*données de contenu*", la cui cancellazione può comportare il malfunzionamento del sistema informatico colpito e, ancora, b) i cosiddetti metadati, la cui alterazione o definitiva eliminazione non determina, invece, la distruzione o il danneggiamento del sistema informatico bersagliato[363]. Di conseguenza, secondo l'autore, solo i primi sarebbero meritevoli di protezione, mentre per quanto riguarda la seconda tipologia di dati, questi ultimi costituirebbero un obiettivo militare legittimo e sarebbero passibili di attacco telematico[364].

A parere di chi scrive, escludere i dati dall'ambito di applicazione del principio di distinzione lascerebbe automaticamente senza protezione un'ampia serie di dati

---

[358] O. Pomson, *"Objects"? The Legal Status of Computer Data under International Humanitarian Law*, in *Journal of Conflict and Security Law*, 2023, p. 349 ss.
[359] *Ibidem*.
[360] Y. Sandoz, *et al.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, cit., para. 2007-08.
[361] Secondo il Manuale di Tallinn 1.0 sul diritto internazionale applicabile alla guerra cibernetica: «*Civilian objects are all objects that are not military objectives. Military objectives are those objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Military objectives may include computers, computer networks, and cyber infrastructure*». *Tallinn Manual* 1.0, p. 125.
[362] T. McCormack, *International Humanitarian Law and the Targeting of Data*, *in International Law Studies*, 2018, p. 222 ss.
[363] H. H. Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, in *Israel Law Review*, 2015, p. 54.
[364] *Ibidem*.

informatici appartenenti alla popolazione civile. Ciò è stato sottolineato anche dal Comitato internazionale della Croce Rossa, secondo il quale: "*destroying essential civilian data can quickly bring government services and private businesses to a complete standstill and thus cause more harm to civilians than the destruction of physical objects*"[365].

Per tale ragione, riteniamo che il principio di distinzione debba necessariamente tutelare anche i dati elettronici civili, a prescindere dal loro carattere intangibile e immateriale[366]. Tali dati non potranno, pertanto, essere fatti oggetto di attacchi informatici a meno che non siano impiegati per finalità militari. Del resto, come dichiarato, con lungimiranza, da autorevole dottrina: "*in the dynamic circumstances of armed conflict, objects which may have been military objectives yesterday may no longer be such today and vice versa*"[367].

In conclusione, la sempre maggiore dipendenza della società dai dati e dalle reti informatiche giustifica una reinterpretazione dell'art. 52, apr. 1, del I Protocollo, che consenta di includere nel suo campo di applicazione anche i dati elettronici.

3. *Segue:* La nozione di obiettivo militare e la questione dei beni a duplice uso

Abbiamo visto come, in base al principio di distinzione, siano vietati gli attacchi contro i civili e i beni civili, nonché gli attacchi indiscriminati contro persone e beni civili ed obiettivi di tipo militare[368]. L'art. 52, par. 2, del I Protocollo Aggiuntivo del 1977, qualifica come obiettivi militari, per quanto concerne le cose, tutti quei

---

[365] ICRC, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, Geneva, 2020, p. 490.

[366] In questo senso si sono espressi diversi autori, tra cui McKenzie, per il quale: "*In IHL and in the corresponding war crime provisions within the ICC Statute, civilian data should be considered as part of protected objects and property. […] Data is always embedded in tangible, physical systems that are unequivocally protected by the rules of international law discussed in this article. […] A narrower interpretation would result in a lacuna of civilian protection against a wide array of cyber operations*". S. McKenzie, *Cyber Operations against Civilian Data, Revisiting War Crimes against Protected Objects and Property in the Rome Statute*, in *Journal of International Criminal Justice*, 2021, p. 1192.

[367] M. Bothe, K. J. Partsch, W. A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, cit., p. 326.

[368] K. Obradovic, *La protection de la population civile dans les conflits armés internationaux*, in A. Cassese (ed.), *The New Humanitarian Law of Armed Conflict*, Vol. I, Napoli, 1979, p. 128 ss.

beni che «per loro natura, ubicazione, destinazione o impiego» contribuiscono in modo efficace all'azione militare dell'avversario e la cui completa distruzione, conquista o neutralizzazione offrono, nelle circostanze del momento, un vantaggio militare preciso.

In altri termini, ai sensi della disposizione, un oggetto, per poter essere considerato un obiettivo militare, deve soddisfare due condizioni. In primo luogo, deve trattarsi di un bene che «per via della sua natura, ubicazione, destinazione o impiego» contribuisca efficacemente all'azione militare e, in secondo luogo, la sua totale o parziale distruzione, conquista o neutralizzazione deve offrire, nel caso concreto, uno vantaggio militare specifico[369].

È ammissibile sostenere che tale definizione di obiettivo militare abbia oggi assunto natura consuetudinaria[370] e, conseguentemente, si imponga anche a quei Paesi che non sono parti del I Protocollo Aggiuntivo, come, ad esempio, gli Stati Uniti.

Rientrano nella definizione di obiettivo militare dettata dalla norma tutti quei beni – sia civili che militari – direttamente utilizzati al fine di alimentare lo sforzo bellico dell'avversario, quali armi, depositi di munizioni, equipaggiamenti, laboratori per lo sviluppo di armamenti ed altro materiale bellico, centri di comando e controllo, nonché edifici occupati dalle forze armate nemiche e dai loro vertici militari[371].

Più complessa, invece, è la qualificazione come obiettivo militare dei cosiddetti beni «*dual use*», quali ponti ed altre vie di comunicazione destinate ai trasporti sia civili che militari, centrali elettriche, raffinerie di petrolio, fabbriche ed altri edifici adibiti alla produzione di beni destinati sia alle forze armate che al mercato civile[372]. Tale qualificazione assume assoluta rilevanza in relazione agli attacchi telematici, dal momento che la maggior parte delle tecnologie informatiche rientrano proprio in questa categoria di beni[373].

---

[369] La definizione di obiettivo militare contenuta in questa disposizione è stata ripresa in molti strumenti convenzionali successivi, quali il II ed il III Protocollo alla Convenzione del 1980 sulle armi convenzionali e, ancora, il II Protocollo del 1999 alla Convenzione dell'Aia sulla protezione dei beni culturali in caso di conflitto armato.

[370] Corte internazionale di giustizia, *Nuclear Weapons Case*, cit., par. 79.

[371] M. Sassòli, *Military Objectives*, in *MPEPIL*, 2015.

[372] K. Banellier, *Is the Principle of Distinction Still Relevant in Cyberwarfare?*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 360.

[373] *Ibidem*.

Se i dispositivi elettronici e le infrastrutture cibernetiche impiegate in via esclusiva per scopi militari – come, ad esempio, quelle che consentono il funzionamento dei sistemi d'arma – costituiscono naturalmente un obiettivo militare legittimo[374], in quanto tale passibile di attacco, il problema si pone per quelle apparecchiature e infrastrutture informatiche che hanno uso duale, che sono cioè utilizzate anche per finalità civili[375].

In questi casi, andrà valutato con particolare attenzione il contributo che il bene offre effettivamente all'azione militare del nemico, nonché il vantaggio militare che conseguirebbe dalla sua completa distruzione, conquista o neutralizzazione[376]. In caso di dubbio, si deve sempre presumere che il bene sia destinato al mercato civile e non offra alcun contributo effettivo all'azione militare avversaria[377]. Ciò in base a quanto statuito dall'art. 52, par. 3, del I Protocollo Aggiuntivo, secondo cui: «In caso di dubbio, un bene che è normalmente destinato ad un uso civile, quale un luogo di culto, una casa, un altro tipo di abitazione o una scuola, si presumerà che non sia utilizzato per contribuire efficacemente all'azione militare».

Ci si è domandati se le compagnie private (come, ad esempio, la società statunitense Microsoft) che sviluppano le tecnologie informatiche impiegate dai belligeranti nel corso delle ostilità per alimentare il proprio sforzo bellico possano essere equiparate alle fabbriche di munizioni e, di conseguenza, essere attaccate in quanto obiettivi militari legittimi ai sensi dell'art. 52, par. 2, del I Protocollo[378].

La risposta parrebbe senz'altro essere negativa. Come precisato infatti, sul punto, da Droege: "*In cyber warfare, where the temptation to target civilian infrastructure is possibly higher than in traditional warfare, it is important to keep in mind that for a civilian object to become a military objective its contribution to military action must be directed towards the actual war-fighting capabilities of a party to the*

---

[374] M. N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, in *International Review of the Red Cross*, 2002, p. 380.
[375] *Ivi*, pp. 384-385.
[376] International Law Association (ILA) Study Group, *The Conduct of Hostilities and International Humanitarian Law*, *Challenges of 21st Century Warfare*, Final Report, 2016, p. 12.
[377] *Ibidem*.
[378] *Tallinn Manual 1.0*, Rule 39, cit., p. 134.

conflict. If an object merely contributes to the war-sustaining capability of a party to the conflict (its general war effort), it does not qualify as a military objective"[379]. Se nel caso di obiettivi militari vige una presunzione a favore del belligerante che sferra l'attacco, nelle ipotesi di beni civili impiegati per finalità militari, come per l'appunto la maggior parte delle tecnologie informatiche utilizzate per fini bellici, detta presunzione viene meno e l'onere della prova è su colui che effettua l'attacco contro questi beni[380]. È quanto affermato dalla Corte internazionale di giustizia nella sentenza relativa all'affare sulle *piattaforme petrolifere*, resa nel 2003, in cui i giudici dell'Aia hanno considerato chiaramente contrario al diritto internazionale l'attacco compiuto dagli Stati Uniti nei confronti di alcune piattaforme petrolifere iraniane in risposta ad alcuni missili lanciati dall'Iran verso navi statunitensi, dal momento che gli Stati Uniti non avevano dimostrato la necessità dell'attacco attraverso la prova dell'utilizzo delle piattaforme a scopi militari[381].

Spetta, inoltre, alla parte che intende sferrare l'attacco verificare che, alla luce delle circostanze del momento, colpire un certo obiettivo offra un preciso vantaggio militare[382].

La nozione di vantaggio militare deve essere intesa in senso restrittivo. Essa si riferisce all'impatto concreto che la (totale o parziale) distruzione, conquista o

---

[379] In altre parole, secondo l'autore: "*The example shows that the parallel with munitions factories should not be overstretched. The relevant criterion of Article 52(2) of Additional Protocol I is that the object must by its use make an effective contribution to military action. First, corporations as such are not physical objects, but legal entities, and so the question would instead be whether any of their locations (that is, buildings) have become military objectives. Second, there is a difference between weapons and IT tools. Weapons are by their nature military objectives, while generic IT systems are not. Thus, one might have to differentiate between factories that actually develop what might be called cyber weapons, that is specific codes/protocols that will be used for a specific computer network attack (so, for instance, the location where a specific virus like Stuxnet is being developed), and those that just provide the military with generic IT supplies, which are not so different from, say, food supplies*". C. Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, in *International Review of the Red Cross*, 2012, pp. 566-567.

[380] M. Castellaneta, *Conflitti armati (diritto internazionale)*, cit., p. 342.

[381] Corte internazionale di giustizia, 6 novembre 2003, *Repubblica islamica d'Iran c. Stati Uniti d'America*, in ICJ *Reports*, 2003, par. 76.

[382] R. Kolb, *Military Objectives in International Humanitarian Law*, in *Leiden Journal of International Law*, 2015, p. 962 ss.

neutralizzazione dell'obiettivo colpito può avere sulla capacità dello Stato nemico di condurre operazioni belliche offensive o difensive[383].

Deve, peraltro, trattarsi di un vantaggio militare certo e non meramente ipotetico[384]. Il Comitato internazionale della Croce Rossa ha, peraltro, messo in luce che un vantaggio militare specifico deve sussistere per ogni obiettivo che viene colpito[385]. Secondo taluni Paesi, come gli Stati Uniti, è da ritenersi legittima la distruzione di beni che "indirettamente" ma "efficacemente" contribuiscono allo sforzo bellico[386]. Tale tesi – che amplia notevolmente la nozione di vantaggio militare – potrebbe essere perfettamente adattata alla guerra cibernetica, dal momento che il collasso delle infrastrutture critiche nemiche causato da un attacco informatico renderebbe, di fatto, impossibile al belligerante continuare le operazioni militari su larga scala. Come affermato da Ronzitti, si tratta di dottrine che, a prescindere dalla durata del conflitto, non hanno nessun fondamento nel diritto internazionale umanitario e sono difficilmente compatibili con le prescrizioni di cui all'art. 52, par. 2, del I Protocollo Aggiuntivo del 1977[387].

4. Il divieto di condurre attacchi indiscriminati

Dal principio di distinzione discende il divieto assoluto di attacchi indiscriminati[388]. Sono ritenuti tali gli attacchi non diretti contro un obiettivo militare specifico, quelli che impiegano mezzi e metodi di combattimento che non possono essere indirizzati con precisione contro un obiettivo militare determinato e, infine, quelli realizzati con mezzi e metodi di guerra i cui effetti, non potendo essere circoscritti, rischiano di provocare danni sproporzionati fra i civili e i beni di natura civile[389].

---

[383] D. Steiger, *Civilian Objects*, in *MPEPIL*, 2011.
[384] M. Bothe, K. J. Partsch, W. A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, cit., p. 326.
[385] https://casebook.icrc.org/law/principle-distinction.
[386] Department of Defence Office of General Counsel, *An Assessment of International Legal Issues in Information Operations*, May 1999, p. 7.
[387] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 266.
[388] Art. 51, par. 4., Protocollo (I) sulla protezione delle vittime dei conflitti armati internazionali, aggiuntivo alle Convenzioni di Ginevra del 12 agosto 1949 (Ginevra, 8 giugno 1977).
[389] ICRC*, International Humanitarian Law Databases*, Rule 12.

In tali casi, l'attaccante non intende danneggiare direttamente la popolazione, ma colpisce indistintamente sia obiettivi militari che civili e beni di carattere civile, non preoccupandosi di provocare possibili danni collaterali[390].

Il divieto di condurre attacchi indiscriminati ha origine nel principio di distinzione e la sua violazione costituisce un grave crimine di guerra[391]. Esso riceve applicazione tanto nei conflitti armati internazionali, quanto in quelli non internazionali ed è oggi considerato sicura espressione del diritto internazionale consuetudinario[392].

Come esempi tipici di attacchi indiscriminati vengono indicati i bombardamenti a tappeto, cioè quei bombardamenti che trattano come unico obiettivo militare più obiettivi militari distanziati fra loro e collocati in luoghi densamente popolati e, ancora, gli attacchi rivolti contro obiettivi militari la cui distruzione comporta un numero di vittime o di danni del tutto sproporzionato rispetto al vantaggio militare concreto e diretto previsto[393].

Il Tribunale internazionale penale per la *ex* Iugoslavia, nel caso *Martìc* del 2007, ha ritenuto il lancio di missili Orkan in una zona densamente popolata della città di Zagabria, avvenuto nel maggio 1995, un chiaro esempio di attacco indiscriminato[394].

A ben guardare, mentre le armi convenzionali non sono di per sé indiscriminate, quelle cibernetiche, al pari delle armi atomiche, chimiche e biologiche, possono delle volte produrre effetti indiscriminati. Ancorché spesso in grado di scegliere accuratamente l'obiettivo militare, non sempre queste sono programmate affinché i propri effetti distruttivi restino limitati al sistema informatico bersagliato[395].

---

[390] Y. Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict*, Cambridge, 2016, p. 127.
[391] K. Dörmann, *Elements of War Crimes under the Rome Statute of the International Criminal Court: Sources and Commentary*, Cambridge, 2003, pp. 161-177.
[392] C. Bell, J. Pfeiffer, *Indiscriminate Attack*, in *MPEPIL*, 2011.
[393] *Ibidem*.
[394] Tribunale internazionale penale per la *ex* Jugoslavia, *Prosecutor v. Martìc*, Judgment, ICTY-95-11, 12 June 2007, par. 463.
[395] C. Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law and the Protection of Civilians*, cit., p. 571.

Il divieto di compiere attacchi indiscriminati assume, pertanto, centrale importanza ai fini della presente analisi. Come sostenuto da Dinstein: "*A CNA may surely constitute an indiscriminate attack. Thus, should a CNA be launched against all enemy computers – without any effort being made to differentiate between them on the basis of military or civilian nature, use, purpose or location (and assuming that harm or injury to civilian persons or more than nominal damage to civilian physical property is caused by the attack) – this may qualify as a violation of the principle of distinction*"[396].

In base al divieto in parola, sulle parti in lotta grava, dunque, un duplice onere.

In primo luogo, esse non possono avvalersi di strumenti cibernetici suscettibili di produrre effetti indiscriminati, come virus e worm capaci di riprodursi – senza alcuna possibilità di controllo – dal computer militare colpito ad un numero consistente di dispositivi elettronici civili connessi in rete con quest'ultimo[397]. In altri termini, è proibito l'utilizzo di qualunque virus o worm che, una volta installato all'intero dell'apparecchiatura militare bersagliata, si diffonde rapidamente in un numero non esiguo di computer civili.

In secondo luogo, i belligeranti devono verificare, sulla base delle circostanze del caso concreto, che l'attacco informatico è (o può essere) indirizzato con precisione contro un obiettivo militare definito[398]. Così, costituisce, ad esempio, un attacco indiscriminato un attacco telematico effettuato allo scopo di mettere fuori uso o impedire il corretto funzionamento del traffico aereo nemico, qualora l'attacco avesse come conseguenza incidenti che coinvolgessero tanto gli aerei militari, quanto quelli civili.

A partire da giugno 2007, una serie di operazioni telematiche denominate *NotPeya* hanno colpito i sistemi informatici ucraini e di altri Paesi del mondo, causando un

[396] Y. Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, cit., p. 267.
[397] L. Dervan, *Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown*, in *Göttingen Journal of International Law*, 2011, p. 388.
[398] *Ivi*, p. 389.

danno economico che, secondo alcune stime, raggiungerebbe l'ammontare di undici miliardi di dollari[399].

Taluni Paesi, quali Stati Uniti, Australia, Nuova Zelanda e Regno Unito, hanno ritenuto la Russia responsabile dell'operazione, senonché, ad oggi, l'attribuzione della condotta illecita si è fermata sul piano politico[400].

A nostro giudizio, l'attacco informatico non rappresenta un attacco indiscriminato poiché, non potendo con certezza essere attribuito giuridicamente alla Federazione Russa, non si configura come un atto di guerra da parte di quest'ultima.

Alla stessa conclusione è giunta la Corte superiore del New Jersey, la quale ha condannato, nel 2022, la compagnia assicurativa *Ace American Insurance Company* al versamento di un risarcimento in favore dell'azienda statunitense Merck per i danni – dell'ammontare di circa un miliardo di dollari – subiti da quest'ultima a seguito dell'operazione telematica in commento[401]. La società assicurativa aveva in precedenza rigettato la richiesta di pagamento, sulla base di una clausola secondo cui è precluso qualsiasi premio assicurativo nelle ipotesi di danni causati da un atto (nel nostro caso un attacco informatico) qualificabile come atto di guerra da parte di uno Stato[402].

5. L'odierna rilevanza dei cavi sottomarini per la comunità internazionale e i rischi per la loro sicurezza in caso di conflitto armato

Il principio di proporzionalità e quello di distinzione svolgono un ruolo essenziale, in tempo di guerra, ai fini della tutela delle condotte e dei cavi sottomarini impiegati per le telecomunicazioni (c.d. *submarine cables*)[403].

---

[399] E. Rosen, *Manufacturers Remain Slow to Recognize Cybersecurity Risks*, *The New York Times*, 21 November 2018.

[400] F. Rampini, *Hacker, Usa e Gb accusano la Russia per il cyber-attacco NotPetya: "Pagherà conseguenze"*, *la Repubblica*, 18 febbraio 2018.

[401] *Merck Ransomware Judgement: New Jersey Superior Court grants partial judgment in favour of Merck*, in *Cyber Economics*, 10 February 2022.

[402] D. Cummings, A. Moss, *Lessons from Merck v. Ace: A cyberattack does not amount to an "act of war"*, *The Policyholder Perspective*, 11 February 2022.

[403] I cavi sottomarini utilizzati per le comunicazioni devono essere distinti da quelli impiegati per il trasporto di energia elettrica e, ancora, dalle condotte posate sul fondo del mare e destinate al

La concezione che Internet sia uno spazio "virtuale", libero da costrizioni fisiche è largamente diffusa ma inesatta[404]. Internet funziona, infatti, principalmente per via di cavi transnazionali che consentono la connessione[405]. La maggior parte di tali cavi, prodotti in fibra ottica, sono posati sul fondo del mare[406]. Tra il 95 e il 99 % delle comunicazioni internazionali avviene, oggi, per via di tali sofisticate costruzioni[407]. Esse rientrano, pertanto, tra le infrastrutture essenziali di ogni Stato e sono, per tale ragione, di vitale importanza per la sua sicurezza nazionale[408].

Tutta questa rete di cavi è oggetto di diverse norme giuridiche internazionali, tra le quali spiccano gli articoli 58, 79, e 112-115 della Convenzione di Montego Bay del 1982 sul diritto del mare[409]. Tuttavia, la predetta Convenzione non trova applicazione in tempo di guerra, come attestato dagli articoli 88 (utilizzazione

---

trasporto di importanti risorse naturali, quali soprattutto petrolio greggio e gas naturale (c.d. *submarine pipelines*). R. Lagoni, *Pipelines*, in *MPEPIL*, 2011.

[404] A. Gili, *Geoeconomia dei cavi sottomarini*, in *ISPI Online*, 28 gennaio 2022.

[405] Sulla disciplina delle condotte e dei cavi sottomarini in tempo di pace si rimanda a: A. Pearce Higgins, *Submarine Cables and International Law*, in *British Yearbook of International Law*, 1921-1922, p. 27 ss.; J. Soubeyrol, *La condition juridique des pipelines en droit international*, in *Annuaire Français de Droit International*, 1958, p. 157 ss.; L. D. M. Nelson, *Submarine Cables and Pipelines*, in R. J. Dupuy and others (eds.), *A Handbook on the New Law of the Sea*, Dordrecht, 1991, vol. 2, p. 977 ss.; W. H. Von Heinegg, *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law*, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, cit., p. 291 ss.; D. Shvets, *Submarine Cables as an Object of Legal Regulation under International Law*, in *Spanish Yearbook of International Law*, 2021, p. 119 ss.; G. Gallo, *I cavi sottomarini e il diritto internazionale: quale protezione per le cosiddette "arterie" della globalizzazione?*, in *La Comunità Internazionale*, 2022, p. 393 ss.

[406] Secondo gli studi più recenti, i cavi attualmente posati sul fondo del mare sono circa trecento e collegano tra loro più di centotrenta Stati. La maggiore concentrazione di tali infrastrutture fisiche si trova nell'Oceano Atlantico. Per una mappa mondiale delle condotte e dei cavi sottomarini vedi: http://www.submarinecablemap.com.

[407] Ne deriva che, una loro eventuale lesione, rottura o danneggiamento – come opportunamente sottolineato anche dall'Assemblea generale delle Nazioni Unite – provocherebbe effetti di non poco conto sul commercio e, di conseguenza, sull'intera economia internazionale. Assemblea generale, *Oceans and the Law of the Sea*, UN Doc. A/65/37 del 7 dicembre 2010, p. 121.

[408] L'attuale rilevanza delle infrastrutture in oggetto trova, peraltro, conferma nella costituzione, in seno all'*International Law Association* (ILA), di un comitato appositamente incaricato di esaminare e definire lo *status* delle condotte e dei cavi sottomarini nel sistema giuridico internazionale. International Law Association, *Submarine Cables and Pipelines under International Law* - Interim Report 2020 (ILA Interim Report), par. 3.

[409] In sintesi, in base a quanto sancito dalla predetta Convenzione tutti gli Stati godono della libertà di posa di condotte e cavi sottomarini nella loro zona economica esclusiva nonché, nel rispetto di determinate condizioni, nella piattaforma continentale e, infine, nell'alto mare.

dell'alto mare per scopi pacifici) e 95 (immunità delle navi da guerra in alto mare)[410].

La questione della salvaguardia delle condotte e dei cavi sottomarini durante un conflitto armato internazionale o interno assume, di conseguenza, assoluta rilevanza[411].

Ora, poiché le regole del diritto umanitario non contengono, a ben guardare, alcun riferimento significativo a tali particolari costruzioni, allo scopo di stabilire quale trattamento debba essere loro riservato nel corso di un conflitto bellico, pare utile ricorrere a quanto disposto dai principali manuali militari di riferimento.

A tale proposito, in virtù di quanto previsto dal Manuale di Oxford sulla guerra navale del 1913, possono essere attaccati, da taluno dei belligeranti, sia i cavi che collegano il suo territorio con quello dell'avversario, sia i cavi che congiungono i territori degli Stati nemici, nonché, da ultimo, i cavi che connettono il territorio dell'avversario con quello di uno Stato neutrale [art. 54][412]. In caso di distruzione di cavi che collegano il territorio del nemico con quello di uno Stato neutrale, è dovuto a quest'ultimo un equo indennizzo, una volta cessati i combattimenti[413]. I cavi che congiungono i territori delle Potenze neutrali sono, invece, inviolabili[414].

---

[410] Il diritto bellico si applica, come noto, a titolo di *lex specialis*, sulla disciplina complessiva dettata dalla Convenzione.

[411] Nelle ultime due guerre mondiali le Potenze belligeranti provvidero a tagliare i cavi sottomarini collegati con la Potenza avversaria, ed effettuarono tale operazione militare anche in luoghi dove difettava ogni loro sovranità, come in alto mare, e persino allorché i suddetti cavi risultavano essere di proprietà di uno Stato neutrale e, quindi, sottratti a ogni loro autorità territoriale.

[412] L'art. 54 del Manuale di Oxford del 1913 trova applicazione, in virtù di quanto sancito dalla stessa norma, a prescindere dalla circostanza che proprietario del cavo sia lo stesso Stato belligerante o, viceversa, singole entità private a quest'ultimo riconducibili. A ben guardare, il Manuale di Oxford sulla guerra navale richiama, quasi per intero, quanto già precedentemente sancito nella risoluzione dell'Institut de Droit International, adottata a Bruxelles nel 1902, e concernente lo *status* giuridico dei cavi sottomarini in tempo di guerra. La risoluzione in commento propone, infatti, la regola secondo cui «*that cables connecting two belligerents or two parts of the territory of a belligerent can be cut anywhere except in neutral waters*», mentre, al contrario, «*that cables connecting two neutral territories are inviolable*». Institut de Droit International, *Câbles Sous-Marins en Temps de Guerre*, Resolution, Brussels Session, 23 settembre 1902.

[413] Quando, in passato, i cavi sottomarini appartenenti alle Potenze neutrali sono stati distrutti, le Potenze belligeranti hanno provveduto talvolta a risarcirli e altre volte a riattivarli al termine delle ostilità. La regola, in questi casi, appare essere nel senso che il belligerante può, per le necessità della guerra, compiere atti che sarebbero altrimenti vietati ed illeciti anche secondo le norme comuni della neutralità e che si giustificano solo eccezionalmente per la impellente necessità militare che li genera, ma deve risarcire alla Potenza neutrale il danno così arrecato. G. Cansacchi, *Nozioni di diritto internazionale bellico*, Torino, 1968, p. 127.

[414] Manual of the Laws of Naval War, Oxford, 9 agosto 1913, art. 54.

Ancora, secondo quanto prescritto dal Manuale di San Remo sul diritto internazionale applicabile alla guerra marittima del 1995, i combattenti sono tenuti a prendere tutte le misure necessarie a prevenire, nonché evitare possibili danni alle condotte e ai cavi sottomarini il cui utilizzo non sia riservato ai soli belligeranti[415].
Le condotte e i cavi sottomarini il cui utilizzo sia destinato ai soli belligeranti, alla luce di quanto contemplato dal Manuale di Oslo del 2020, costituirebbero, invece, degli obiettivi militari legittimi[416]. Con la conseguenza che, in qualsiasi momento, potrebbero essere attaccati e distrutti[417]. L'operazione militare, si badi, deve però essere giustificata da una oggettiva necessità militare e, soprattutto, deve essere condotta nel pieno rispetto dei principi del diritto internazionale umanitario.
In altre parole, per valutare la liceità di un attacco condotto contro condotte o cavi sottomarini, non possono non venire in considerazione, in particolare, i principi di distinzione e di proporzionalità.
In forza del principio di distinzione, trattandosi di infrastrutture a doppio uso civile e militare, il belligerante prima di attaccare una condotta o un cavo sottomarino deve valutare con particolare attenzione il contributo che la struttura offre all'azione militare dello Stato nemico, nonché il vantaggio militare concreto e diretto che conseguirebbe dalla sua distruzione[418]. La stima del vantaggio militare conseguente all'operazione va effettuata in concreto, alla luce delle circostanze esistenti nel momento in cui l'attacco viene eseguito.
Tuttavia, come taluni autori hanno osservato: "*network cables are certainly not used only to facilitate military objectives; they are primarily used for civilian purposes. As a technical matter, the interconnectedness and resilience of cable networks means that any attack on cables that contribute to specific military systems or communications would likely have indiscriminate effects for civilian systems and*

[415] L. Doswald-Beck (ed.), *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, Cambridge, 1995, art. 37.
[416] Y. Dinstein (ed.), *Oslo Manual on Select Topics of the Law of Armed Conflict. Rules and Commentary*, Cham, 2020, art. 68.
[417] I cavi sottomarini non possono essere però attaccati se situati in acque neutrali. Ciò in conformità con quanto previsto dalle norme sulla neutralità, le quali impongono a carico dello Stato belligerante l'obbligo di rispettare il territorio delle Potenze neutrali.
[418] S. Ryan, *Submarine Communication Cables and Belligerent Rights in Armed Conflict*, in *Ocean Yearbook Online*, 2024, p. 29.

uses"[419]. È proprio per tale motivo che il Comitato internazionale della Croce Rossa ha affermato che: "*an attack against undersea cables would raise concerns under the prohibition of indiscriminate attacks*"[420].

Per quanto attiene al principio di proporzionalità alcuni autori hanno sottolineato che: "*the volume of civilian data and likelihood of damage spreading beyond the targeted state to neutral states, will always render the military advantage less than the anticipated collateral damage and incidental injury to civilian objects and civilians; that is, it would fail the proportionality test*"[421]. Di conseguenza: "*it is near impossible for an attack on a military objective submarine data cable to be considered proportionate as regards the widespread and anticipated damage that would occur to civilians, including civilians in third neutral states*"[422].

In conclusione, in tempo di guerra, sulla base dei manuali militari indicati, più che sulla base della normativa convenzionale relativa ai conflitti armati internazionali, risulta che le condotte e i cavi sottomarini configurano, a tutti gli effetti, degli obiettivi militari legittimi. Tali infrastrutture, invero, non rientrano tra le categorie di beni oggetto di particolare protezione durante un conflitto armato.

Tuttavia, da un lato, la loro rilevanza per la comunità internazionale e, dall'altro, il fatto che le loro caratteristiche tecniche potrebbero incidere sulla normale applicazione dei principi del diritto dei conflitti armati, ci inducono a pensare che forse le condotte e i cavi sottomarini utilizzati per le comunicazioni debbano sempre essere qualificati come beni civili e, conseguentemente, non possano essere fatti oggetto di attacco (informatico o convenzionale) da parte dei belligeranti nel corso delle ostilità.

---

[419] *Ivi*, p. 30.
[420] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Geneva, December 2015, p. 43.
[421] R. McLaughlin, T. P. Paige, D. Guilfoyle, *Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization*, in *Journal of Conflict and Security Law*, 2022, p. 42.
[422] *Ibidem*.

6. Le misure di precauzione

Il principio di precauzione svolge una funzione servente rispetto alle suesposte regole di diritto internazionale umanitario[423]. Esso impone, a carico di ciascuna parte belligerante, l'obbligo di risparmiare i civili ed i loro beni, adottando tutte quelle precauzioni volte a prevenire o, quantomeno, ridurre il rischio di danni collaterali derivanti da un attacco, assicurando, di conseguenza, il rispetto dei principi di distinzione e di proporzionalità[424].

Sebbene non formalmente richiamato nel testo dell'art. 3 «comune» alle quattro Convenzioni di Ginevra del 1949 e nel II Protocollo a queste Aggiuntivo del 1977, il principio in oggetto trova applicazione anche durante i conflitti armati interni[425] ed ha carattere consuetudinario[426]. La sua violazione può comportare un grave crimine di guerra, quando viene effettuato un attacco indiscriminato, nella consapevolezza che tale attacco provocherà morti, feriti o distruzioni di beni civili eccessivi rispetto al vantaggio militare atteso dall'operazione[427].

Il principio di precauzione viene in rilievo nel corso di qualsiasi attività militare, sia difensiva, che offensiva[428]. Occorre, quindi, che questo venga rispettato anche allorquando si conducono operazioni cibernetiche soltanto a scopo di difesa, oppure operazioni cibernetiche che, pur non costituendo un vero e proprio «attacco» ai sensi del diritto internazionale umanitario, rientrano comunque nell'ambito delle attività militari intraprese. Non sembrerebbe residuino dubbi, invero, sul fatto che

---

[423] T. D. Gill, *International Humanitarian Law Applied to Cyber-Warfare: Precautions, proportionality and the Notion of "Armed" under the Humanitarian Law of Armed Conflict*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., p. 375.

[424] A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 130.

[425] Tribunale penale internazionale per la ex Iugoslavia, *The Prosecutor v. Kupreskic*, Judgment, 14 April 2022, (IT-95-16), par. 524.

[426] J. M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, *Vol. 1: Rules*, cit., p. 51 ss.

[427] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p 271.

[428] J. M. Henckaerts, L. Doswald-Beck, *Customary International Humanitarian Law*, *Vol. 1: Rules*, cit., p. 51 ss.

il suddetto principio debba essere pienamente osservato anche in caso di attacchi di natura telematica [429].

L'art. 57 del I Protocollo Aggiuntivo del 1977 specifica quali misure di precauzione devono essere poste in essere dallo Stato belligerante che intende sferrare un attacco, tanto nella fase di pianificazione, quanto in quella di esecuzione dello stesso (cosiddette misure di precauzione attiva)[430].

Ai sensi della citata norma le tre regole fondamentali che devono essere eseguite in materia di attacchi sono le seguenti:

a) occorre accertare che gli obiettivi da attaccare siano effettivamente obiettivi militari;
b) occorre rispettare il principio di proporzionalità, cioè non bisogna realizzare attacchi che potrebbero determinare danni e perdite di vite umane eccessive rispetto al vantaggio militare diretto e concreto previsto;
c) occorre impiegare mezzi e metodi di combattimento che riducano al minimo i danni collaterali ai civili e ai loro beni. La fattibilità di eventuali soluzioni alternative che consentono di diminuire il rischio di danni collaterali deve essere valutata alla luce del diverso impatto che queste potrebbero avere sul successo dell'operazione militare, nonché tenendo conto dell'eventuale maggiore pericolo a cui le forze armate dell'attaccante potrebbero essere esposte[431].

Al rispetto delle elencate regole sono tenuti non solamente coloro che preparano o decidono un attacco, ma anche gli esecutori dello stesso poiché l'art. 57 del I Protocollo Aggiuntivo impone l'immediata interruzione dell'attacco quando, una volta cominciata l'operazione bellica, appare chiaro che questa sia contraria alla regola della proporzionalità[432].

La disposizione pone, inoltre, a carico delle parti in conflitto l'obbligo di avvertire in tempo utile e con mezzi efficaci (ad esempio attraverso il lancio preventivo di

[429] J. M. Conde, *The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law*, in *Tilburg Law Review*, 2010, pp. 84-85.
[430] ICRC, *International Humanitarian Law Databases*, Rule 122.
[431] W. H. von Heinegg, *Precautions in Attack*, in *MPEPIL*, 2015.
[432] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p 272.

volantini o, ancora, mediante tempestivi annunci telefonici, radiofonici o televisivi) la popolazione civile, allorquando l'attacco è suscettibile di colpire incidentalmente quest'ultima. Tuttavia, l'obbligo in commento, che potrebbe impedire il vantaggio dalla sorpresa, viene meno quando le circostanze lo impediscano[433].

Gli obblighi di precauzione attiva non sono assoluti[434]. Il belligerante è, invero, tenuto ad adempierli in modo diligente, assumendo cioè le proprie decisioni sulla base delle informazioni di cui dispone al momento dell'attacco[435].

Ora, le suindicate misure di precauzione attiva rivestono un'importanza centrale nel contesto in esame. Il crescente ricorso all'intelligenza artificiale, in situazioni di conflitto armato, ha notevolmente ridimensionato, infatti, il ruolo dei combattenti nel processo decisionale di un attacco[436].

In forza di detti obblighi di precauzione attiva, la Potenza belligerante – prima di sferrare l'operazione cibernetica – dovrà, dunque, anzitutto, verificare la legittimità dell'obiettivo che intende colpire, accertandosi che questo non sia un civile o un bene civile e non benefici, ad ogni modo, di una protezione speciale [art. 57, par. 2, lett. *a*) (i) I PA].

In secondo luogo, ove vi siano armi più precise, tra quelle disponibili e lecite, la scelta dei mezzi e metodi di guerra da utilizzare andrà effettuata in favore di queste ultime [art. 57, par. 2, lett. *a*) (ii) I PA].

In terzo luogo, il belligerante dovrà procedere al giudizio prognostico circa l'entità dei possibili danni collaterali e del vantaggio militare atteso e, laddove i danni ai civili o ai loro beni si annunciassero sproporzionati, l'attacco informatico non potrà essere ordinato [art. 57, par. 2, lett. *a*) (iii) I PA].

Qualora vi siano due o più obiettivi militari che consentono di ottenere un vantaggio militare equivalente, la scelta dovrà ricadere sull'obiettivo che presenti il minor rischio di danni collaterali [art. 57, par. 3, I PA].

---

[433] A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 131.

[434] J. Quéguiner, *Precautions under the Law Governing the Conduct of Hostilities*, in *International Review of the Red Cross*, 2006, p. 793 ss.

[435] W. H. von Heinegg, *Precautions in Attack*, in *MPEPIL*, 2015.

[436] J. M. Beard, *Law and War in the Virtual Era*, in *American Journal of International Law*, 2009, p. 440.

Infine, qualora le condizioni dovessero cambiare dopo l'approvazione dell'attacco informatico, o nuove informazioni a disposizione del belligerante modifichino il suo giudizio in merito al carattere militare dell'obiettivo o sulla proporzionalità dell'operazione, questa dovrà essere annullata o sospesa [art. 57, par. 2, lett. *b*) I PA]. L'obbligo in parola vincola ovviamente tutti i livelli della catena di comando, incluso l'esecutore materiale dell'attacco telematico.

Pertanto, qualora si intenda infettare con un virus un computer militare, andranno adottati tutti gli accorgimenti necessari a minimizzare il rischio di danni collaterali che potrebbero discendere dal contagio delle apparecchiature civili connesse in rete con il dispositivo oggetto dell'attacco. Si potrà, ad esempio, prevedere che il virus si attivi solo laddove sul dispositivo colpito sia installato un particolare *software* ad uso militare, ovvero che esso si disattivi automaticamente entro una certa data, oppure che operi unicamente durante le ore notturne, in cui il numero dei computer civili connessi in rete è presumibilmente inferiore.

Come affermato da Ronzitti, l'obbligo di precauzione negli attacchi, al pari della maggior parte degli obblighi internazionali contemplati dalle norme di *ius in bello*[437], è un obbligo di condotta e non un obbligo di risultato[438]. Di conseguenza, riteniamo che l'impiego di personale militare non debitamente addestrato nella conduzione di operazioni cibernetiche con finalità di offesa potrebbe concretizzare, in astratto, una violazione del principio in questione.

L'obbligo di precauzione investe tutte le parti in conflitto, tanto sul fronte offensivo, quanto sul fronte difensivo (cosiddetta precauzione passiva)[439]. In altre parole, le precauzioni relative agli attacchi devono essere prese non solamente dallo Stato attaccante, ma anche dallo Stato vittima di attacchi informatici.

---

[437] Da un'attenta analisi dei principi di proporzionalità e di precauzione si desume l'inesistenza di un obbligo di risultato, atto ad evitare in maniera assoluta danni a persone o cose estranei alla condotta militare. Tale obbligo sarebbe, allo stato attuale di sviluppo del diritto bellico, del tutto irrealistico. Sul punto vedi: E. Cannizzaro, *Il principio della proporzionalità nell'ordinamento internazionale*, cit., p. 306.

[438] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 272.

[439] E. T. Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, in *International Law Studies*, 2013, p. 212.

L'art. 58 del I Protocollo Aggiuntivo del 1977 richiede al belligerante, per quanto possibile, di evitare di collocare obiettivi militari all'interno o in prossimità di zone densamente popolate, di compiere ogni sforzo per allontanare la popolazione civile, nel caso in cui questa sia stanziata vicino ad obiettivi militari costruiti in tempo di pace e, ancora, di prendere ogni altra precauzione necessaria per proteggere i civili ed i beni civili che si trovano sotto il suo controllo, contro i pericoli scaturenti dalle operazioni militari[440]. Si tratta, anche in queste ipotesi, di obblighi di *due diligence*, che il belligerante è tenuto ad adempiere nei limiti delle proprie capacità[441].

Come osservato da Jensen, le informazioni militari si diffondono principalmente tramite reti e infrastrutture per le comunicazioni ad uso civile, quali satelliti e cavi in fibra ottica sottomarini[442]. Distinguere o separare tali infrastrutture civili dalle reti e infrastrutture per le comunicazioni ad uso militari, avvalendosi – nel corso delle ostilità – soltanto di queste ultime, al fine di rispettare, in maniera adeguata, il predetto obbligo di precauzione passiva, non sembra essere né praticamente né, tanto meno, economicamente possibile per gli Stati belligeranti[443]. Oltretutto, un obbligo in tal senso non appare neppure ricavabile, in via interpretativa, dalla lettura dell'art. 58 PA[444].

Come suggerito dall'autore, ben più plausibile sarebbe che le parti in lotta adottino altri accorgimenti ed idonee misure precauzionali finalizzate a limitare i molteplici danni collaterali che potrebbero discendere da un attacco telematico, anche in tempo di pace, come il costante utilizzo di antivirus o l'esecuzione periodica di *backup* diretti a facilitare il recupero dei dati ed il rapido ripristino dei servizi di accesso alla rete, una volta cessato l'attacco informatico all'infrastruttura civile bersagliata[445].

---

[440] https://casebook.icrc.org/a_to_z/glossary/precautions-attack.
[441] A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 132.
[442] E. T. Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, in *Texas Law Review*, 2010, p. 1535.
[443] *Ivi*, p. 1551.
[444] R. Geiss, H. Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, in *Israel Law Review*, 2012, p. 394.
[445] E. T. Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, cit., pp. 215-216.

7. Il divieto di perfidia

Tra le regole del diritto bellico che vengono particolarmente in rilievo nel contesto informatico, deve essere annoverato poi il divieto di perfidia[446]. Si è suggerito che costituisca perfidia, per esempio, l'invio di *e-mail* falsamente provenienti dal Comitato internazionale della Croce Rossa (CICR) o dal Servizio di Supporto di Microsoft[447].

La perfidia rientra, a pieno titolo, nel novero dei metodi di combattimento proibiti dal diritto dei conflitti armati[448]. Secondo la definizione codificata nel testo dell'art. 37, comma 1, del I Protocollo Aggiuntivo alle Convenzioni di Ginevra del 1949, costituiscono perfidia tutti gli atti che fanno appello – con la chiara intenzione di ingannarla – alla buona fede del nemico, allo scopo di indurre il medesimo a credere di avere il diritto di ricevere o, viceversa, l'obbligo di riconoscere la protezione prevista dalle norme del diritto internazionale umanitario[449].

Di conseguenza, è qualificabile come perfido l'atto di chi simula la resa o una incapacità dovuta a ferite o malattie o, ancora, l'atto di chi simula di possedere lo *status* di civile o un particolare *status* protetto, con il preciso intento di ingannare l'avversario, allo scopo di colpirlo o catturarlo[450]. È vietato, in particolare, l'utilizzo indebito di emblemi e segni riconosciuti dal diritto internazionale (art. 38 I PA), nonché l'utilizzo di simboli ed uniformi di nazionalità diversa dalla propria (art. 39 I PA)[451].

Ancorché non richiamato nel II Protocollo del 1977, il divieto di perfidia si applica anche nel corso di un conflitto armato non internazionale[452]. La violazione del

---

[446] M. Gervais, *Cyber Attacks and the Laws of War*, in *Berkeley Journal of International Law*, 2012, p. 573.
[447] *Ibidem*.
[448] V. Rusinova, *Perfidy*, in *MPEPIL*, 2011.
[449] I. Henderson, *Emerging Technology and Perfidy in Armed Conflict*, in *International Law Studies*, 2015, p. 469 ss.
[450] E. David, *Principes de droit des conflits armés*, Bruxelles, 2008, p. 438.
[451] https://casebook.icrc.org/a_to_z/glossary/perfidy.
[452] M. Madden, *Of Wolves and Sheep: A Purposive Analysis of Perfidy Prohibitions in International Humanitarian Law*, in *Journal of Conflict and Security Law*, 2012, p. 444.

divieto in discorso – il quale è posto a tutela del principio di distinzione – costituisce un crimine di guerra[453].

A proposito del divieto di perfidia, il Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica, alla regola 122, dispone quanto segue: «*In the conduct of hostilities involving cyber operations, it is prohibited to kill or injure an adversary by resort to perfidy. Acts that invite the confidence of an adversary to believe that he or she is entitled to, or is obliged to accord, protection under the law of armed conflict, with intent to betray that confidence, constitute perfidy*»[454].

Secondo la citata disposizione, affinché una data *cyber operation* possa ritenersi un atto di perfidia, essa deve quindi necessariamente:

a) suscitare la fiducia dell'avversario, il quale deve a sua volta avere il diritto di ricevere o, al contrario, l'obbligo di riconoscere la protezione contemplata dalle norme di *ius in bello*;

b) provocare l'effetto proibito della morte, del ferimento o della cattura dell'avversario. Di conseguenza, le *cyber operations* i cui effetti si verificano solo nella dimensione del ciberspazio o, ancora, quelle che si limitano solamente a danneggiare o distruggere beni di natura materiale non sono coperte dal divieto.

Infine, affinché possa parlarsi di perfidia, occorre che la condotta perpetrata sia intenzionale. In altre parole, l'autore della stessa deve volontariamente ingannare il nemico mediante l'operazione telematica sferrata.

Alla luce di quanto precede, deve dunque considerarsi un atto di perfidia, ad esempio, l'invio di *malware* tramite *e-mail* che sembrerebbero provenire da un ufficio delle Nazioni Unite, da uno Stato neutrale o, comunque, da uno Stato non impegnato nel conflitto, qualora i suddetti *malware*, una volta attivati, determinino il malfunzionamento del sistema informatico dell'infrastruttura nemica bersagliata, causando – allo stesso tempo – la perdita di un certo numero di vite umane.

[453] Articoli 8, par. 2, lett. *b* (xi) e 8, par. 2, lett. *e* (ix) dello Statuto della Corte Penale Internazionale.
[454] M. N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0*, cit., p. 491.

8. Disinformazione e conflitti armati

La perfidia non deve essere confusa con gli stratagemmi di guerra, i quali sono ritenuti – ai sensi dell'art. 37, comma 2, del I Protocollo Aggiuntivo del 1977 – un metodo di guerra legittimo, purché non attuati in violazione di altre regole dello *ius in bello*[455].

A differenza della perfidia, gli stratagemmi di guerra mirano sì ad ingannare il nemico, ma rinunciando a fare appello alla sua buona fede, per indurlo ad accordare una protezione non dovuta[456]. Sono tipici esempi di stratagemmi di guerra le false informazioni, le operazioni simulate e i mascheramenti[457].

L'avvento di Internet ha fornito alle parti in lotta una pluralità di modi per sperimentare nuovi stratagemmi di guerra, come, ad esempio, la diffusione di false informazioni *online*[458].

Secondo alcuni autori, la divulgazione di false informazioni da parte dei belligeranti attraverso il *cyberspace* deve ritenersi certamente lecita, poiché non differisce – quanto a finalità militari – dalle campagne di disinformazione attuate mediante mezzi non telematici (volantinaggio, ecc.)[459].

Tuttavia, come per qualsiasi stratagemma di guerra, le false informazioni divulgate attraverso la rete non devono superare quella soglia di gravità oltre la quale si è in presenza di un atto di perfidia[460]. Sono, inoltre, proibite le false informazioni *online* dirette a spostare la popolazione civile al fine di compiere atti di violenza ai danni

---

[455] Ancorché la disposizione in commento si riferisca ai soli conflitti armati internazionali, è *communis opinio* che il ricorso agli stratagemmi di guerra sia autorizzato anche nel corso di conflitti armati non internazionali. ICRC, *International Humanitarian Law Databases*, Rule 57.

[456] https://casebook.icrc.org/a_to_z/glossary/ruse-war.

[457] K. Ipsen, *Ruses of War*, in *MPEPIL*, 1982.

[458] I. Henderson, *Emerging Technology and Perfidy in Armed Conflict*, cit., p. 473 ss.

[459] L. Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, in *International Law Studies*, 2002, p. 171.

[460] D. Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, in *Harvard Journal of International Law*, 2006, pp. 205-207.

della stessa[461], quelle che coinvolgono, poi, particolari persone o beni protetti[462], nonché quelle preliminari o di supporto al compimento di atti contrari ad altre disposizioni dello *ius in bello*[463].

La creazione e diffusione di false informazioni tramite Internet, oltre a configurare uno stratagemma di guerra finalizzato sostanzialmente a confondere il nemico per influenzarne il comportamento sul campo di battaglia, delle volte rientrano però tra quelle più sofisticate attività militari volte ad indebolire il morale della popolazione locale e delle truppe avversarie, allo scopo di minare la loro volontà di combattere (*psychological warfare*)[464].

Il Manuale di Harvard sul diritto internazionale applicabile alla guerra aerea del 2009 (HPRC, *Manual on International Law Applicable to Air and Missile Warfare*) afferma che l'applicazione delle norme di diritto umanitario che vietano gli attacchi indiscriminati e quelli diretti contro i civili o i beni civili è limitata ai soli attacchi che comportano la perdita di vite umane o il danneggiamento e la distruzione fisica di beni[465]. Ne consegue che le false informazioni, non provocando i suindicati effetti

---

[461] Si pensi, a titolo di esempio, ai messaggi diffusi da Israele, nel 2009, nel corso della cosiddetta Operazione militare Piombo Fuso, con cui i civili palestinesi sono stati invitati a spostarsi verso zone successivamente oggetto di intensi bombardamenti aerei da parte dell'esercito israeliano. UNHR Council, *Human Rights in Palestine and Other Occupied Arab Territories: Report of the United Nations Fact-Finding Mission on the Gaza Conflict*, 25 September 2009, UN Doc A/HRC/12/48, (Goldstone Report), par. 531-36.

[462] L. Doswald-Beck, *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, cit., p. 171.

[463] M. Castellaneta, *La disinformazione nel conflitto in Ucraina: tra ius in bello e diritto alla libertà di espressione*, in O. Porchia, M. Vellano (a cura di), *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future. Liber Amicorum in onore di Edoardo Greppi*, Torino, 2023, p. 336.

[464] La guerra psicologica, le cui origini si possono far risalire ai tempi più antichi, è stata ampiamente utilizzata a partire dal Primo conflitto mondiale e risulta, oggi, inserita nelle dottrine militari di un crescente numero di Stati. Le attività che la contraddistinguono sono, in genere, complementari alle operazioni armate sul terreno, poiché svolte in concomitanza con queste ultime. Si tratta di tutta una serie di atti non violenti quali, per esempio, la continua o alternata proiezione di luci o di musica ad alto volume per periodi prolungati di tempo. Con l'avvento di Internet, tale forma di guerra è stata condotta sempre più spesso sfruttando il settore dell'informazione e sembra oramai aver determinato un mutamento profondo della dimensione del campo di battaglia. K. Chainoglou, *Psychological Warfare*, in *MPEPIL*, 2016.

[465] *Program on Humanitarian Policy and Conflict Research at Harvard University (HPCR), Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge, 2009, Rule 21, par. 1, p. 105.

materiali e tangibili, sono sempre ammesse, anche allorquando abbiano come unico o principale destinatario la popolazione civile dello Stato avversario[466].

Quanto disposto dal Manuale solleva inevitabilmente non poche perplessità se si tiene conto che le operazioni di guerra psicologica, sebbene non equivalgano ad un attacco cinetico ai sensi del diritto umanitario, potrebbero comportare conseguenze psicologiche per la popolazione coinvolta nel conflitto ben più gravi e durature, rispetto alle lesioni fisiche causate da taluni attacchi convenzionali[467].

Nell'ottobre 2005, Israele ha impiegato, come strumento di guerra psicologica, le proprie forze dell'aeronautica militare per generare migliaia di boom sonici sulla Striscia di Gaza, a volte anche a distanza di una sola ora durante la notte[468]. La citata pratica militare, ritenuta non letale dalle autorità governative israeliane e intesa a minare il sostegno della popolazione ai diversi gruppi armati presenti sul territorio, è stata definita dalle Nazioni Unite un «*indiscriminate noise attack*», e condannata in seno alla stessa Organizzazione per aver causato comprovati problemi cardiaci e gravi disturbi mentali, specie tra i soggetti più giovani[469]. La sua legittimità è stata messa in dubbio anche dal Relatore Speciale sulla situazione dei diritti umani nei territori palestinesi occupati, il quale – in un importante rapporto del 2006 – ha riscontrato che: «*shelling and sonic booms violated the fundamental rights to life and human dignity, and even less attention was paid to the constraints of international humanitarian law; it was already clear that collective punishment was to be the instrument used to bring about regime change*»[470].

In conclusione, le vigenti disposizioni del diritto internazionale bellico non vietano la disinformazione[471], che rientra, dunque, tra i metodi di combattimento concessi

---

[466] *Ivi*, Rule 21, par. 2, p. 105.

[467] S. Cherry*, Modern Armed Conflicts: Disinformation Campaigns Shaping the Digital Information Landscape,* in *The Serials Librarian*, 2024, p. 19 ss.

[468] *Israeli sonic booms terrorising Gaza*, *Aljazeera*, 2 gennaio 2006.

[469] *Palestinians hit by sonic boom air raids*, *The Guardian*, 3 novembre 2005.

[470] United Nations Commission on Human Rights, *Report by Special Rapporteur John Dugard on the Situation of Human Rights in the Palestinian Territories Occupied by Israel since 1967*, 5 September 2006, UN Doc A/HRC/2/5, par. 10.

[471] La Commissione europea nel 2018 ha definito la disinformazione come «un'informazione rivelatasi falsa o fuorviante concepita, presentata e diffusa a scopo di lucro oppure per ingannare intenzionalmente il pubblico, e che può arrecare un pregiudizio pubblico. Il pregiudizio pubblico include minacce ai processi politici democratici e di elaborazione delle politiche e a beni pubblici quali la tutela della salute dei cittadini, dell'ambiente e della sicurezza dell'UE. La disinformazione

nel corso delle ostilità[472]. Tuttavia, le innovative modalità con cui la disinformazione è stata spesso utilizzata dalle parti belligeranti nel corso dei conflitti armati più recenti mettono in discussione la sua qualificazione come stratagemma di guerra[473].

Mentre questi ultimi, di solito, hanno come destinatario i membri delle forze armate nemiche, le moderne campagne di disinformazione sono state rivolte, al contrario, principalmente nei confronti dei civili, come strumento di guerra psicologica[474].

Ora, se le false informazioni promulgate tramite Internet rappresentano, in tempo di pace[475], un grande rischio per la tenuta ed il corretto funzionamento delle moderne società democratiche[476], in tempo di guerra queste appaiono ancora più pericolose, perché suscettibile di provocare enormi sofferenze per le popolazioni delle parti in conflitto[477]. Si pensi, a titolo di esempio, alla realizzazione e divulgazione in rete di *fake news* riguardanti un imminente attacco nucleare e aventi come bersaglio prevalentemente i civili dello Stato nemico.

Riteniamo, pertanto, le false informazioni promulgate mediante l'utilizzo della rete ammesse nella sola misura in cui queste risultino dirette alla realizzazione di un vantaggio militare concreto e diretto ed abbiano come destinatari esclusivamente i combattenti nemici ed obiettivi militari. Sebbene, come visto, non costituiscano un attacco nel senso proprio del termine e la dottrina maggioritaria deponga in senso

---

non include gli errori di segnalazione, la satira e la parodia, o notizie e commenti chiaramente identificabili come di parte». Vedi: Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, 26 aprile 2018, Contrastare la disinformazione online: un approccio europeo, COM (2018), p. 236.

[472] Sempreché, si badi, questa non sia accompagnata da *hate speech* o incitamento al genocidio. M. Holvoet, *International Criminal Liability for Spreading Disinformation in the Context of Mass Atrocity*, in *Journal of International Criminal Justice*, 2022, p. 223 ss.

[473] E. Katz, *Liar's War: Protecting Civilians from Disinformation during Armed Conflict*, in *International Review of the Red Cross*, 2021, p. 659.

[474] *Ivi*, pp. 664-665.

[475] Per quanto riguarda le implicazioni della disinformazione nei rapporti tra Stati in tempo di pace ed una sua possibile regolamentazione internazionale, vedi: C. Serrano, *From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does International Law provide?*, in *Spanish Yearbook of International Law*, 2020, p. 129 ss; Y. Zerbe, *Cyber-Enabled International State-Sponsored Disinformation Operations and the Role of International Law*, in *Swiss Review of International and European Law*, 2023, p. 49 ss.

[476] B. Baade, *Fake News and International Law*, in *European Journal of International Law*, 2018, p. 1357 ss.

[477] M. Castellaneta, *La disinformazione nel conflitto in Ucraina: tra ius in bello e diritto alla libertà di espressione*, cit., pp. 329-330.

opposto[478], a nostro giudizio, le false informazioni unicamente finalizzate a diffondere il panico tra la popolazione locale appaiono di dubbia legittimità.
A tale proposito, si ricorda che l'art. 51, par. 2, del I Protocollo Aggiuntivo del 1977 stabilisce che «sono vietati gli atti o minacce di violenza, il cui obiettivo principale sia quello di diffondere il terrore fra la popolazione civile». A ben guardare, il testo della norma non parla di «attacchi» o di «operazioni militari», bensì semplicemente di «atti» oppure di «minacce» di violenza nei confronti dei civili interessati dal conflitto armato. Data la vaghezza e l'elasticità che caratterizzano le espressioni in parola, non vi è motivo di escludere che le false informazioni *online* potrebbero qualificarsi in particolare come «minacce di violenza» e, di conseguenza, rientrare nell'ambito di applicazione della norma, laddove suscettibili di creare il terrore tra la popolazione locale.

9. La tutela del patrimonio culturale

Fra le norme consuetudinarie e convenzionali del diritto internazionale umanitario che devono essere necessariamente osservate al momento della pianificazione e dell'esecuzione di un attacco cibernetico vi sono quelle poste a protezione del patrimonio culturale[479].

---

[478] J. M. Henckaerts, L. Doswald-Beck (eds.), *Customary International Humanitarian Law, Vol. 2: Practice*, Cambridge, 2005, Rule 57, p. 258.

[479] La letteratura riguardante la tutela del patrimonio culturale in tempo di guerra è sterminata. In particolare, si veda: A. F. Panzera, *La Tutela Internazionale dei Beni Culturali in Tempo di Guerra*, Torino, 1993; F. Francioni, *Patrimonio comune della cultura. Sovranità e conflitti armati*, in *Studi in ricordo di Antonio Filippo Panzera*, Vol. I, Bari, 1995, p. 381 ss.; M. Serisic, *Protection of Cultural Property in Time of Armed Conflict*, in *Netherlands Yearbook of International Law*, 1996, pp. 3-14; A. Gioia, *La protezione dei beni culturali nei conflitti armati*, in F. Francioni (a cura di), *Protezione Internazionale del Patrimonio Culturale: Interessi Nazionali e Difesa del Patrimonio Comune della Cultura*, Milano, 2000; F. Francioni, F. Lenzerini, *The Destruction of the Buddhas of Bamiyan and International Law*, in *European Journal of International Law*, 2003, pp. 619-651; M. Frulli, *Advancing the Protection of Cultural Property through the Implementation of Individual Criminal Responsibility: The Case-Law of the International Criminal Tribunal for the Former Yugoslavia*, in *Italian Yearbook of International Law*, 2005, pp. 195-216; A. Malintoppi, *La protezione dei beni culturali in caso di conflitto armato*, Milano, 2006; P. Benvenuti, R. Sapienza (a cura di), *La tutela internazionale dei beni culturali nei conflitti armati*, Milano, 2007; L. Zagato, *La protezione dei beni culturali in caso di conflitto armato all'alba del secondo Protocollo 1999*, Torino, 2007; A. Maugeri, *La tutela dei beni culturali nel diritto internazionale penale*, Milano, 2008; M. Frulli, *The Criminalization of Offences against Cultural Heritage in Times of Armed Conflict: The Quest for Consistency*, in *European Journal of International Law*, 2011, pp. 203-217;

La tutela del patrimonio culturale, in tempo di guerra, è affidata principalmente alla Convenzione UNESCO del 1954 per la protezione dei beni culturali in caso di conflitto armato, nonché ai due Protocolli ad essa annessi, adottati, rispettivamente, nel 1954 e nel 1999[480]. La Convenzione, entrata in vigore il 7 agosto 1956, è stata finora ratificata da 126 Stati[481], mentre il I Protocollo – in vigore dalla medesima data e diretto sostanzialmente ad impedire la sottrazione di beni culturali da un territorio occupato – vincola, attualmente, 103 Stati. Ha, invece, un ambito di applicazione considerevolmente più ridotto il II Protocollo – firmato il 26 marzo 1999 ed entrato in vigore dal 9 marzo 2004 – il quale è stato, al momento, ratificato da soli 67 Stati[482].

Da un'analisi di insieme delle fonti normative convenzionali citate si evince come, è vietato attaccare, anche a titolo di rappresaglia, i beni culturali situati nel territorio del nemico e risulta proibito, in termini assoluti, il loro impiego per finalità militari[483].

Ai sensi dell'art. 6, lett. *a)*, del II Protocollo del 1999, un bene culturale può essere attaccato soltanto se, per via della sua funzione, sia stato reso un obiettivo militare legittimo e non vi sia alcuna valida alternativa che permetta di ottenere un vantaggio militare comparabile a quello che deriverebbe dall'attaccare il bene in questione. In base all'art. 6, lett. *b)*, invece, agli Stati è consentito disporre di un bene culturale per scopi bellici solamente laddove il vantaggio militare che deriverebbe da tale utilizzo non sia conseguibile altrimenti. In caso di attacco, l'art. 7 del II Protocollo,

---

U. Leanza, *Lo stato dell'arte della protezione dei beni culturali in tempo di guerra*, in *La Comunità internazionale*, 2011, pp. 371-388; A. Magrone, *L'azione dell'UNESCO per la protezione dei beni culturali inseriti nella Lista del patrimonio mondiale culturale e naturale in caso di conflitti armati*, in A. Cannone (a cura di), *La protezione internazionale ed europea dei beni culturali*, Bari, 2014, pp. 91-104 ; L. Pineschi, *Tutela del patrimonio culturale e missione di pace delle Nazioni Unite, un binomio possibile? Il caso MINUSMA*, in *Rivista di diritto internazionale*, 2018, pp. 5-57; I. Caracciolo, U. Montuoro (eds.), *Preserving Cultural Heritage and National Identities for International Peace and Security*, Torino, 2019.

[480] Molte delle disposizioni contenute nei suelencati strumenti pattizi sono gradualmente divenute sicura espressione di regole di diritto internazionale consuetudinario.

[481] L'Italia ha provveduto con L. 7 febbraio 1958 n. 729.

[482] In Italia il II Protocollo è in vigore dal 29 maggio 2009, per effetto della L. di ratifica 16 aprile 2009 n. 45.

[483] A. Annoni, F. Salerno, *La tutela internazionale della persona umana nei conflitti armati*, cit., p. 207.

obbliga i belligeranti ad adottare ogni possibile precauzione per limitare i danni ai beni culturali[484].

I suindicati strumenti pattizi predispongono, pertanto, una tutela autonoma per i beni culturali, vincolando gli Stati parti contraenti ad attivarsi, già in tempo di pace, per garantirne la salvaguardia contro gli effetti prevedibili di un conflitto armato[485].

Ai sensi della Convenzione UNESCO del 1954, godono di protezione tutti i beni, mobili o immobili, di grande importanza per il patrimonio culturale dei popoli, quali siti archeologici, monumenti architettonici, musei, opere d'arte, oggetti di interesse storico, complessi di costruzioni che, nel loro insieme, sono di interesse artistico[486].

L'art. 53 del I Protocollo Aggiuntivo del 1977 sulla protezione delle vittime dei conflitti armati internazionali estende, inoltre, l'immunità dagli attacchi armati, contemplata dalla Convenzione UNESCO del 1954, anche ai luoghi di culto, i quali rappresentano il patrimonio spirituale di un determinato popolo.

In virtù dell'art. 8, par. 2, lett. *b)* (ix), dello Statuto della Corte penale internazionale, l'attacco intenzionale contro i suindicati beni costituisce un grave crimine di guerra e comporta, di conseguenza, la responsabilità penale individuale dei combattenti coinvolti; sempreché, beninteso, tali beni non fossero impiegati dal nemico a fini militari.

Il patrimonio culturale deve essere rispettato anche durante un conflitto armato non internazionale. Ai sensi dell'art. 19 della Convenzione UNESCO, invero, tutte le parti impegnate in un simile conflitto sono tenute al rispetto delle disposizioni in essa contemplate. Utilizzando una formula analoga, l'art. 22 del II Protocollo UNESCO, prevede espressamente che tutte le disposizioni in esso contenute si applichino automaticamente ai conflitti armati non internazionali che abbiano luogo sul territorio di una parte contraente. Del resto, il divieto di compiere atti ostili contro i beni culturali e quello di utilizzarli in supporto allo sforzo bellico è previsto

[484] Sul II Protocollo del 1999 vedi, in particolare, A. Gioia, *The Development of International Law Relating to the Protection of Cultural Property in the Event of Armed Conflict: The Second Protocol to the 1954 Hague Convention*, in *Italian Yearbook of International Law*, 2001, pp. 25-57.
[485] R. Wolfrum, *Cultural Property, Protection in Armed Conflict*, in *MPEPIL*, 2010.
[486] Convenzione del 1954 per la protezione dei beni culturali in caso di conflitto armato, art. 1.

anche nell'art. 16 del II Protocollo Aggiuntivo del 1977 sulla protezione delle vittime dei conflitti armati non internazionali.

L'esigenza di salvaguardare il patrimonio culturale dagli effetti della guerra si avverte, con particolare evidenza, in caso di occupazione bellica[487]. A tale proposito, l'art. 4 della Convenzione UNESCO vieta, in maniera tassativa, la requisizione e la confisca di beni mobili di interesse culturale. Il successivo art. 5, invece, obbliga la Potenza occupante a collaborare con le autorità competenti dello Stato occupato alla salvaguardia ed alla conservazione dei beni culturali presenti nel territorio occupato, nonché l'obbligo di assistere tali autorità nella prevenzione e repressione dei furti e dei saccheggi dei suddetti beni. Degno di nota è, oltretutto, il I Protocollo UNESCO, il quale obbliga la Potenza occupante a restituire alle competenti autorità dello Stato occupato, una volta terminate le ostilità, i beni culturali eventualmente trafugati in territorio occupato.

In materia di tutela del patrimonio culturale, il Manuale di Tallinn 2.0 sul diritto internazionale applicabile alla guerra cibernetica – alla regola 142 – dispone esplicitamente che: «*The parties to an armed conflict must respect and protect cultural property that may be affected by cyber operations or that is located in cyberspace. In particular, they are prohibited from using digital cultural property for military purposes*»[488].

La disposizione – specificatamente dedicata all'integrità del patrimonio culturale – impone a tutte le parti in lotta l'obbligo di rispettare e salvaguardare i cosiddetti beni culturali in formato digitale (come, ad esempio, le collezioni di archivi oppure le collezioni scientifiche in versione digitale), e proibisce di avvalersi di tali beni per scopi bellici.

La definizione di bene culturale in formato digitale risulta attualmente piuttosto controversa[489]. Un importante riferimento a tale nozione è, tuttavia, rinvenibile

---

[487] Per quanto concerne la tutela del patrimonio culturale in tempo di occupazione bellica, vedi: M. Frigo, *La protezione dei beni culturali nei territori occupati: il divieto di esportare i beni culturali da un territorio occupato e gli obblighi di restituzione*, in *Studi in onore di Vincenzo Starace*, Vol. 1, 2008, p. 325 ss.

[488] *Tallinn Manual 2.0*, cit., p. 534.

[489] R. Alcala, *Cultural Evolution: Protecting "Digital Cultural Property" in Armed Conflict*, in *International Review of the Red Cross*, 2022, p. 1096.

nella Carta UNESCO per la conservazione del patrimonio culturale digitale, adottata dalla Conferenza Generale dell'UNESCO, nel corso della sua trentaduesima sessione, svoltasi a Parigi il 17 ottobre 2003[490].

La Carta, a norma dell'art. 1, afferma che: «*The digital heritage consists of unique resources of human knowledge and expression. It embraces cultural, educational, scientific and administrative resources, as well as technical, legal, medical and other kinds of information created digitally, or converted into digital form from existing analogue resources. Where resources are "born digital", there is no other format but the digital object. Digital materials include texts, databases, still and moving images, audio, graphics, software and web pages, among a wide and growing range of formats. They are frequently ephemeral, and require purposeful production, maintenance and management to be retained. Many of these resources have lasting value and significance, and therefore constitute a heritage that should be protected and preserved for current and future generations. This ever-growing heritage may exist in any language, in any part of the world, and in any area of human knowledge or expression*»[491].

A ben guardare, sono due le tipologie di beni culturali in versione digitale che rientrano nella definizione fornita dalla norma: a) le opere che consistono sostanzialmente in riproduzioni digitali di beni culturali preesistenti[492], e b) le opere che, diversamente, sono state create in digitale e sussistono solo in tale formato[493].

Relativamente alla prima categoria di beni culturali digitali, essi ricevono tutela nei confronti di eventuali attacchi telematici soltanto qualora l'opera originale risulti

---

[490] Il testo della Carta è consultabile al seguente indirizzo: https://www.tuttocamere.it/files/attivita/UNESCO_Carta_Conservazione.pdf.

[491] Secondo la Carta, peraltro, i documenti e i contenuti digitali costituenti un bene culturale hanno valore e rilevanza duratura e, conseguentemente, rappresentano un patrimonio in continuo sviluppo, che deve essere protetto e conservato anche per le generazioni future. Tale patrimonio può esistere in qualunque lingua ed in qualsiasi ambito della conoscenza e dell'espressione umana.

[492] Appartengono a questo genere di materiale digitale, ad esempio, le scansioni digitali di siti Unesco effettuate da CyArk, un'organizzazione senza scopo di lucro con sede in California, fondata nel 2003 con la finalità di condividere e conservare in forma digitale il patrimonio culturale più significativo per l'intera umanità.

[493] Tra i contenuti creati ed esistenti unicamente in versione digitale rientrano le opere riconducibili alle correnti ed ai movimenti artistici noti come *New Media art*, *Digital art*, *Electronic art* e, infine, *Virtual art*. In argomento, F. Popper, *Art - Action and Participation*, New York, 1975; M. Costa, *Il sublime tecnologico*, Salerno, 1990.

inaccessibile, sia stata completamente distrutta o danneggiata o, ancora, il numero di copie digitali che è possibile effettuare della stessa sia alquanto limitato[494].

Deve essere respinta, pertanto, la tesi di chi estende la tutela prevista dalle pertinenti norme di *ius in bello* a qualsiasi surrogato digitale di un'opera fisica preesistente[495]. Come opportunamente sostenuto da Dinnis "[…] *no one would suggest that the millions of souvenir copies of Michelangelo's David sold in Florence each year are protected under the IHL despite the undoubted protected status of the original*"[496].

Viceversa, nel caso di opere esistenti solamente in forma digitale, gli Stati hanno l'obbligo di attivarsi, già in tempo di pace, per assicurare la loro protezione contro gli effetti prevedibili di un conflitto armato[497]. Al fine di garantire l'osservanza del predetto obbligo, questi potrebbero, ad esempio, effettuare periodicamente dei *backup* delle opere in questione.

L'art. 4, par. 3, della Convenzione UNESCO del 1954 vieta, poi, ogni atto di furto, saccheggio o sottrazione indebita di beni culturali situati nel territorio avversario[498]. Ne discende, quindi, il divieto assoluto per i belligeranti di effettuare copie non autorizzate di opere costituenti il patrimonio digitale della parte avversa[499].

L'invasione dell'Ucraina da parte della Federazione Russa ha messo in luce tutta la vulnerabilità delle opere digitali in contesti di conflitto armato e la necessità di una maggiore attenzione da parte degli Stati ad assicurarne un'adeguata salvaguardia[500]. Ciò, sebbene il governo russo non abbia, sinora, fatto ampio utilizzo delle proprie

---

[494] Come sostenuto, in sintesi, dal filosofo tedesco Walter Benjamin: "*A copy of a unique work of art, even the most perfect reproduction of it, could never equal the original because copies could not capture the "authenticity" or possess the "aura" of their exemplars*". W. Benjamin, *The Work of Art in the Age of Its Technological Reproducibility, and Other Writings on Media*, Harvard, 2008, pp. 170-172.

[495] R. Alcala, *Cultural Evolution: Protecting "Digital Cultural Property" in Armed Conflict*, cit., p. 1103; R. Ong, *Hard Drive Heritage: Digital Cultural Property in the Law of Armed Conflict*, in *Columbia Human Rights Law Review*, 2021, p. 285.

[496] H. H. Dinnis, *Cyber Warfare and the Laws of War*, cit., p. 231.

[497] Convenzione del 1954 per la protezione dei beni culturali in caso di conflitto armato, art. 3.

[498] R. Ong, *Hard Drive Heritage: Digital Cultural Property in the Law of Armed Conflict*, cit., p. 278.

[499] H. H. Dinnis, *Cyber Warfare and the Laws of War*, cit., p. 235.

[500] R. Alcala, *Ukraine Symposium - The Ukraine Conflict and The Future of Digital Cultural Property*, in *Lieber Institute West Point*, 13 May 2022.

capacità militari in campo cibernetico, a differenza di quanto previsto da molti esperti[501].

Durante il conflitto russo ucraino tuttora in corso è apparsa, infatti, fondamentale l'attività svolta da *Saving Ukrainian Cultural Heritage Online* (SUCHO), un'associazione costituita da diversi volontari internazionali, il cui compito consiste essenzialmente nella individuazione ed archiviazione di testi, depositi archiviali, immagini fisse ed in movimento, e *database* costituenti il patrimonio culturale digitale del popolo ucraino[502].

Appena poche ore dopo che i membri di tale organizzazione avevano eseguito il *backup* del materiale digitale rinvenibile nella pagina web dell'archivio di Stato di Kharkiv, il sito ha subito un pesante attacco informatico avversario[503]. Tra i contenuti e le informazioni definitivamente cancellate a seguito dell'attacco telematico, ma – fortunatamente – salvate per via della precedente operazione di *backup*, vi erano numerose scansioni digitali di diversi libri e manoscritti di assoluta rilevanza per il patrimonio culturale ucraino[504].

10. La salvaguardia dell'ambiente naturale

Oggetto di particolare protezione in tempo di guerra è anche l'ambiente naturale[505]. Come per i beni culturali ed i luoghi di culto, le norme contemplate dal I Protocollo Aggiuntivo alle Convenzioni di Ginevra del 1949 affiancano quelle contenute in determinate convenzioni settoriali.

Nell'ambito del I Protocollo, assumono rilevanza l'art. 35, par. 3, che proibisce l'utilizzo di mezzi e metodi di combattimento concepiti con la sola finalità di

---

[501] K. E. Eichensehr, *Ukraine, Cyberattacks, and the Lessons for International Law*, in *American Journal of International Law*, 2022, p. 145 ss.

[502] https://www.sucho.org/.

[503] F. Bajak, *Cyberattacks accompany Russian military assault on Ukraine*, *AP News*, 24 February 2022.

[504] H. Stephenson, *Preserving Ukraine's Cultural Heritage Online. A Tufts Librarian Leads an International Effort to Save Digital Information Threatened by Russia's Invasion*, *TuftsNow*, 18 March 2022.

[505] R. G. Tarasofsky, *Legal protection of the environment during international armed conflict*, in *Netherlands Yearbook of International Law*, 1993, p. 17 ss.; I. Peterson, *The Natural Environment in Times of Armed Conflict*, in *Leiden Journal of International Law*, 2009, p. 325 ss.

provocare danni ambientali «estesi, durevoli e gravi»[506] e l'art. 55, par. 2, che vieta gli attacchi armati contro l'ambiente naturale a titolo di rappresaglia[507].

La tutela dell'ambiente in caso di conflitto armato è poi alla base della Convenzione del 1977 sul divieto di ricorrere a tecniche di modifica dell'ambiente naturale per scopi militari o per ogni altro fine ostile (Convenzione ENMOD)[508]. La Convenzione è stata aperta alla firma a Ginevra il 18 maggio 1977 ed è entrata in vigore il 5 ottobre 1978[509].

Un ulteriore riferimento alla salvaguardia dell'ambiente in situazioni di conflitto armato è contenuto, inoltre, nel testo dell'art. 8, par. 2 (*b*) (iv), dello Statuto della Corte penale internazionale[510], nonché nella risoluzione delle Nazioni Unite del 3 aprile 1991 n. 687, in cui si affermava la responsabilità dell'Iraq per i danni ambientali connessi alla invasione del Kuwait[511].

La protezione dell'ambiente naturale in relazione ai conflitti armati è stata altresì allo studio della Commissione di diritto internazionale a partire dal 2013 (Special Rapporteur Marie G. Jacobsson), la quale ha da poco approvato un progetto di articoli in materia[512].

Ora, riteniamo che il divieto di causare danni all'ambiente naturale, anche a titolo di rappresaglia, possa pienamente applicarsi anche agli attacchi informatici[513].

---

[506] I suindicati termini devono essere interpretati restrittivamente, nel senso che la disposizione si ritiene violata solamente in presenza di un danno significativo. M. Bothe, *War and Environment*, in *EPIL*, 2000, p. 1344.

[507] Ai sensi della norma, oggetto di tutela è l'ambiente naturale in quanto tale, a prescindere dal fatto che il suo danneggiamento si ripercuota sulla popolazione civile. Y. Dinstein, *Protection of the Environment in International Armed Conflict*, in *Max Planck Yearbook of United Nations Law*, 2001, p. 532.

[508] Con l'espressione «tecniche di modifica dell'ambiente» si intende, ai sensi dell'art. 2 della citata Convenzione, «qualsiasi tecnica che abbia come obiettivo quello di modificare – attraverso una manipolazione volontaria di processi naturali – la dinamica, la composizione o la struttura della Terra […]».

[509] Per un commento alla Convenzione, si veda: G. Fischer, *La Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins hostiles*, in *Annuaire français de droit international*, XXIII, 1977, p. 820 ss.

[510] La norma in questione dispone quanto segue: «*Intentionally launching an attack in the knowledge that such attack will cause incidental loss of life or injury to civilians or damage to civilian objects or widespread, long-term and severe damage to the natural environment which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated*».

[511] S/RES/678 (1990), 29 novembre 1990, par. 16.

[512] https://documents.un.org/doc/undoc/ltd/g22/348/04/pdf/g2234804.pdf.

[513] W. M. Arkin, *Cyber Warfare and the Environment*, in *Vermont Law Review*, 2001, p. 791.

Risulta evidente, invero, come pure siffatti attacchi possano determinare danni ambientali, al pari di qualsiasi altro mezzo o metodo di guerra convenzionale[514].

Di conseguenza, al momento dell'esecuzione di un attacco telematico, gli effetti sull'ambiente devono essere tenuti in debito conto, proprio come per qualunque attacco cinetico. Così, per esempio, se si pianifica un attacco cibernetico contro un impianto di stoccaggio di petrolio, il danno ambientale che presumibilmente ci si può attendere come conseguenza logica dell'operazione deve necessariamente essere considerato.

L'appartenenza al diritto consuetudinario degli obblighi di cui all'art. 35, par. 3 e all'art. 55 è però tuttora contestata[515]. Sembra, allora, opportuno domandarsi se le predette regole vincolino soltanto gli Stati parti del I Protocollo Aggiuntivo.

A nostro parere la risposta è negativa. La sussistenza di un obbligo generale di preservare l'ambiente naturale in contesti di conflitto armato, oltre ad essere ampiamente riconosciuta in dottrina[516], è stata enunciata altresì nel principio 24 della Dichiarazione di Rio del 1992 sull'ambiente e lo sviluppo[517], e ribadita sia dalla Commissione dei reclami Eritrea-Etiopia nel 2004[518], che dalla Corte internazionale di giustizia nel più volte citato parere consultivo sulla *liceità della minaccia o dell'uso delle armi nucleari*[519].

In definitiva, il divieto di effettuare cyber attacchi suscettibili di produrre disastri ecologici non vincola unicamente gli Stati membri del I Protocollo del 1977.

Quanto detto rileva, tuttavia, soltanto per i conflitti armati internazionali. Nel II Protocollo Aggiuntivo del 1977 sulla protezione delle vittime nei conflitti armati

---

[514] H. H. Dinnis, *Cyber Warfare and the Laws of War*, cit., p. 221.
[515] S. Vöneky, R. Wolfrum, *Environment, Protection in Armed Conflict*, in *MPEPIL*, 2016.
[516] W. D. Verwey, *Protection of the Environment in Times of Armed Conflict: In Search of a New Legal Perspective*, in *Leiden Journal of International Law*, 1995, p. 7 ss.; M. Castellaneta, *La responsabilità internazionale degli Stati per danni all'ambiente causati nel corso di conflitti armati*, in *Rivista di diritto internazionale*, 1998, p. 632 ss.
[517] Secondo il suddetto principio la guerra ha un effetto distruttivo sullo sviluppo sostenibile. Di conseguenza, gli Stati sono tenuti a rispettare le norme inerenti alla protezione dell'ambiente in fase di conflitto armato e a cooperare per il loro progressivo riconoscimento.
[518] Ethiopia's Central Front Claim Partial Award, 2004, cit., par. 100.
[519] Corte internazionale di giustizia, *Legality of the Threat or Use of Nuclear Weapons*, cit., par. 31.

non internazionali mancano, infatti, disposizioni analoghe a quelle sancite dal I Protocollo[520].

11. L'interdizione di attaccare determinate categorie di beni

Abbiamo visto come l'obbligo per le parti in conflitto di tutelare, nel corso delle ostilità, tanto l'ambiente naturale quanto il patrimonio culturale dell'avversario si applichi anche in caso di attacchi di natura telematica.
Dalla lettura dell'art. 54 del I Protocollo Aggiuntivo alle Convenzioni di Ginevra del 1949, si ricava poi – seppur indirettamente – il divieto di attaccare, distruggere o mettere deliberatamente fuori uso, attraverso l'impiego di strumenti telematici, i beni indispensabili alla sussistenza della popolazione civile nemica, come le riserve di acqua, quale che sia lo scopo effettivamente perseguito dai belligeranti[521].
Anche le strutture sanitarie adibite a scopi medici devono essere rispettate[522]. I loro sistemi informatici non possono, pertanto, divenire oggetto di attacchi telematici a meno che i suddetti edifici non siano funzionali al compimento di atti dannosi nei confronti dell'avversario. In questo caso, prima di sferrare l'attacco informatico, i belligeranti sono comunque tenuti a concedere al nemico un termine ragionevole per porre fine all'utilizzo illecito della struttura. Il medesimo regime giuridico si applica, *mutatis mutandis*, ai trasporti e ai dati sanitari[523].
Infine, i combattenti non possono sferrare, neppure a titolo di rappresaglia, attacchi cibernetici aventi come obiettivo le opere o le installazioni che contengono forze pericolose, come le dighe e le centrali nucleari adibite alla produzione di energia elettrica, qualora l'attacco possa causare una fuoriuscita di forze pericolose tale da

[520] K. Hulme, *Natural Environment*, in E. Wilmshurst, S. Breau (eds.), *Perspectives on the ICRC Study on Customary International Humanitarian Law*, Cambridge, 2009, p. 230.
[521] Ai sensi della citata disposizione, la proibizione viene meno laddove gli oggetti essenziali per la sopravvivenza della popolazione civile siano utilizzati dalla Parte avversaria per il sostentamento dei soli membri delle proprie forze armate.
[522] La regola riveste carattere consuetudinario e si applica tanto nei conflitti armati internazionali, quanto in quelli non internazionali. Essa riguarda tutte le installazioni sanitarie, fisse o mobili, civili o militari, permanenti o temporanee.
[523] T. Rodenhäuser, *Hacking Humanitarians? International Humanitarian Law and the Protection of Humanitarian Organizations Against Cyber Operations*, in *EJIL:Talk!*, 16 March 2020.

arrecare perdite consistenti tra la popolazione civile nemica (art. 56 del I Protocollo Aggiuntivo del 1977). L'attacco è vietato anche quando l'installazione costituisce un obiettivo militare. Tuttavia, la protezione accordata cessa qualora l'installazione venga usata in via esclusiva per scopi militari o, ancora, a causa della presenza nelle vicinanze di altri obiettivi militari, a condizione che questi siano impiegati nelle operazioni militari e l'attacco cibernetico sia il solo modo per neutralizzarli. In questi casi, i belligeranti sono, comunque, tenuti ad adottare tutte le precauzioni possibili «per evitare che le forze pericolose siano liberate».

Nel 2007, Israele ha distrutto con un raid aereo un presunto reattore nucleare in Siria, mettendo completamente fuori uso il sistema radar siriano mediante attacchi telematici preparatori[524]. Appare allora opportuno chiedersi se la predetta operazione configuri una violazione dell'art. 56 del I Protocollo Aggiuntivo del 1977.

A nostro avviso, la risposta sembrerebbe essere positiva. A ben guardare, invero, sebbene l'attacco informatico abbia avuto come bersaglio solamente la rete Internet del sistema radar avversario, determinandone il malfunzionamento, questo ha, di fatto, reso possibile l'attacco cinetico verso l'impianto nucleare che si intendeva distruggere. L'attacco informatico può ritenersi, quindi, parte integrante dell'intera operazione bellica, poiché sussiste un nesso diretto di causalità tra il risultato ottenuto dal suo impiego ed il successivo ricorso alla forza cinetica da parte delle forze aeree israeliane. In altre parole, l'operazione militare, nella fattispecie qui analizzata, sarebbe costituita da due fasi temporalmente distinte, ma strettamente (e imprescindibilmente) connesse tra loro[525].

[524] Von E. Follath, H. Stark, *The Story of "Operation Orchard": How Israel Destroyed Syria's Al Kibar Nuclear Reactor*, *Spiegel International*, 2 November 2009.

[525] L'utilizzo del *malware* dovrebbe essere visto, pertanto, come parte dell'uso della forza cinetica conseguenzialmente impiegata per distruggere la centrale. Gli effetti dell'operazione informatica risultano essere, infatti, la condizione anteriore e necessaria che ha permesso alle forze israeliane di colpire la centrale.

CAPITOLO III

Lo *status* giuridico degli attori coinvolti nella pianificazione ed esecuzione di attacchi informatici in contesti di conflitto armato

L'ipotesi di pervenire ad una apposita disciplina convenzionale internazionale in materia di attacchi cibernetici, dalla dottrina più volte avanzata, non trova ancora adeguato interesse da parte degli Stati della comunità internazionale[526]. Pertanto, riteniamo che i nuovi scenari militari descritti vadano necessariamente collocati nel solco della disciplina normativa esistente, convenzionale e consuetudinaria.
Poiché, come abbiamo osservato nei capitoli precedenti, le regole sulla conduzione delle ostilità non dipendono né dal tipo di arma impiegata, né dalla modalità di attacco compiuto, si può sostenere che il diritto bellico attualmente in vigore include anche il ricorso a mezzi informatici per colpire le forze armate nemiche nel corso delle ostilità.
L'inquadramento degli attacchi informatici nel diritto internazionale dei conflitti armati implica la definizione dello *status* giuridico di tutti coloro che realizzano – direttamente o indirettamente – l'attacco, al fine di determinare le possibili misure che lo Stato colpito dall'operazione potrebbe legittimamente adottare contro di loro.

1. La nascita di unità specializzate in operazioni cibernetiche (offensive e difensive) in seno agli eserciti degli Stati e le problematiche connesse al loro inquadramento giuridico

Come abbiamo detto in precedenza, in forza del principio di distinzione, solamente gli obiettivi di tipo militare possono essere oggetto di attacco[527]. Per quanto

[526] A. P. Johnson, *Is It Time for a Treaty on Information Warfare?*, in *International Law Studies*, 2002, p. 439 ss.
[527] A. P. V. Rogers, *Law on the Battlefield*, Manchester, 2004, p. 63.

concerne la definizione di obiettivo militare possono essere ritenuti tali tanto le persone fisiche, quanto i beni[528].

Tra le persone fisiche rientrano, in primo luogo, coloro che fanno parte delle forze armate avversarie[529]. L'art. 1 del Regolamento annesso alla IV Convenzione dell'Aia del 1907 qualifica, infatti, come belligeranti tutti membri delle forze armate di una Potenza in conflitto (anche allorquando non coinvolti attivamente nelle ostilità) e quelli delle milizie o dei corpi volontari, sia pure *lato sensu*, inquadrati tra le forze armate di una parte belligerante (cosiddetti combattenti regolari)[530]. Ai sensi della disposizione in oggetto, i componenti di milizie o di corpi volontari che non fanno, invece, parte delle forze armate di uno Stato in conflitto (cosiddetti combattenti irregolari) possono godere dello *status* di combattenti solamente qualora in grado di soddisfare le seguenti quattro condizioni cumulative:

a) essere sottoposti ad un comando responsabile per i propri subordinati;

b) portare un segno distintivo fisso che li renda riconoscibili a distanza;

c) portare apertamente le armi;

d) conformarsi, nelle operazioni militari, alle leggi ed alle consuetudini della guerra.

Nel definire l'ambito di applicazione soggettivo delle proprie disposizioni, le quattro Convenzioni di Ginevra del 1949 hanno successivamente esteso la categoria dei soggetti abilitati all'esercizio della violenza bellica ai componenti delle forze armate regolari di un governo o di un'autorità non riconosciuta dalla controparte nemica[531], nonché ai gruppi di resistenza organizzati riconducibili ad una delle parti in lotta, che operano fuori o all'interno del loro territorio[532].

---

[528] *Ibidem*.

[529] La qualità di membro delle forze armate dipende, si noti, dal diritto interno di ciascuno Stato.

[530] E. Crawford, *The Treatment of Combatants and Insurgents under the Law of Armed Conflict*, Oxford, 2010, p. 58 ss.

[531] L'ipotesi può riguardare, ad esempio, le forze armate di un governo fantoccio o di un governo in esilio o, ancora, quelle di un governo che non sia mai stato riconosciuto dalla controparte avversaria, come accaduto per il governo dei Talebani durante il conflitto tra Afghanistan e Stati Uniti nel 2001.

[532] Questi ultimi, oltre a soddisfare i requisiti stabiliti dal Regolamento annesso alla IV Convenzione dell'Aia del 1907 per i combattenti irregolari, devono appartenere ad un'entità che possa essere definita un movimento organizzato e possa vantare un solido rapporto con uno dei belligeranti. E. Crawford, *The Treatment of Combatants and Insurgents under the Law of Armed Conflict*, cit., p. 61 ss.

Da ultimo, il I Protocollo Aggiuntivo del 1977 ha profondamente rivisitato la nozione di combattente dettata dalla disciplina precedente. Esso, invero, ha posto fine alla discriminazione tra combattenti regolari e combattenti irregolari, fornendo una definizione di forze armate che supera definitivamente tale distinzione[533]. L'art. 43 del I Protocollo determina tutta una serie di requisiti indispensabili per acquisire lo *status* di combattente legittimo e, di conseguenza, godere di quello di prigioniero di guerra[534], in caso di cattura da parte del nemico[535].

Ai sensi della suindicata disposizione, le forze armate delle parti belligeranti (che comprendono non solamente le forze armate in uniforme, bensì anche i membri dei movimenti di liberazione nazionale e i guerriglieri), per poter essere considerate combattenti legittimi, devono necessariamente:

---

[533] J. M. Henckaerts, *Armed Forces*, in *MPEPIL*, 2010.

[534] La prigionia di Guerra inizia nel momento in cui l'individuo cade in potere del nemico o perché catturato in battaglia, oppure per effetto di resa o capitolazione. Tale condizione si giustifica esclusivamente con il fine di impedire che il soggetto ritorni nell'esercito di appartenenza finché il conflitto armato non termini. Lo *status* di prigioniero di guerra è disciplinato dal Regolamento annesso alla IV Convenzione dell'Aia del 1907, dalla III Convenzione di Ginevra del 1949, che risulta interamente a questi dedicata, nonché dagli artt. 43-47 del I Protocollo Aggiuntivo del 1977. Da un'analisi delle suindicate fonti convenzionali si evince come il trattamento di prigioniero di guerra consti di tutta una serie di diritti e doveri. I prigionieri di guerra sono, innanzitutto, tenuti a fornire allo Stato nemico solamente alcune tassative informazioni inerenti alla loro identità (quali nome, cognome, grado, data di nascita) e non, al contrario, informazioni di interesse militare. Essi non possono poi rinunciare ai loro diritti, neanche in parte, né possono essere oggetto di rappresaglie, ma soltanto – a certe condizioni – di provvedimenti disciplinari e penali. Possono essere internati in campi che non si trovano nei luoghi di combattimento e che siano comandati da un ufficiale militare dello Stato avversario. Devono, inoltre, essere trattati con rispetto della persona e dell'onore. Non possono essere forzati a prestare servizio nell'esercito nemico, ma possono essere impiegati in lavori non connessi alle operazioni belliche, escluso, comunque, lo sminamento. Al termine delle ostilità i prigionieri di guerra devono essere rimpatriati immediatamente. Non occorre, quindi, attendere la conclusione di un trattato di pace, essendo sufficiente la cessazione effettiva delle ostilità. Il ritardo ingiustificato e deliberato nel loro rimpatrio costituisce una grave violazione delle norme umanitarie. In argomento, V. Starace, *Prigionieri di guerra (Diritto internazionale)*, in *Nss. D.I.*, XIII, 1966, p. 852 ss.; R. Falk, *International Law Aspects of Repatriation of Prisoners of War during Hostilities*, in *American Journal of International Law*, 1973, pp. 465-478; A. Rosas, *The Legal Status of Prisoners of War: A Study in International Humanitarian Law Applicable in Armed Conflicts*, Helsinki, 1976; R. Lapidoth, *Qui a droit au statut de prisonnier de guerre?*, in *Revue générale de droit international public*, 1978, pp. 170-210; A. Panzera, *Prigionieri di guerra (Diritto internazionale)*, in *Nss. D.I.*, Appendice, V, 1984, p. 1220 ss.; A. Jachec-Neale, *Status and Treatment of Prisoners of War and Other Persons Deprived of Their Liberty*, in E. Wilmshurst, S. Breau (eds.), *Perspectives on the ICRC Study on Customary International Humanitarian Law*, Cambridge, 2007, pp. 302-336; R. M. Chesney, *Prisoners of War*, in *MPEPIL*, 2009; S. Scheipers, *Prisoners of War*, Oxford, 2010;

[535] La norma ha assunto rilevanza consuetudinaria e, conseguentemente, si applica anche alle forze delle Nazioni Unite e di altre organizzazioni internazionali, quando coinvolte in un conflitto armato internazionale.

a) appartenere ad una parte in conflitto;
b) essere organizzate;
c) essere sottoposte ad un comando responsabile per la condotta dei propri subordinati.

La disposizione – rientrante nel novero del diritto internazionale consuetudinario – chiarisce, dunque, che tutti gli individui appartenenti agli organi delle parti in lotta o i soggetti la cui condotta sia a queste imputabili sono combattenti legittimi, fatta eccezione per il personale medico sanitario e quello religioso[536].

In quanto legittimi combattenti, tali individui hanno pieno diritto a partecipare direttamente alle ostilità[537]. Ne consegue che, essi possono essere oggetto di attacco in qualunque momento e non solo quando effettivamente impegnati in atti ostili[538]. Quanto detto rileva ovviamente anche per il personale militare specializzato nella preparazione ed esecuzione di attacchi informatici, a cui spetta – come per qualsiasi altro membro delle forze armate – sia lo *status* di combattente legittimo, che quello di prigioniero di guerra, nelle ipotesi di cattura da parte dell'avversario[539].

Sempre più Stati della comunità internazionale dispongono, all'interno del proprio esercito, di sezioni *ad hoc* responsabili della conduzione di operazioni telematiche tanto difensive, quanto offensive[540]. Tali reparti militari sono, oggi, rinvenibili tra le forze armate della maggior parte dei Paesi al mondo[541]. Si pensi, su tutti, allo *United States Cyber Command (USCYBERCOM)*, uno degli undici comandi dell'Esercito degli Stati Uniti, responsabile di garantire la sicurezza delle reti

[536] K. Ipsen, *Combatants and Non-Combatants*, in D. Fleck (ed.), *The Handbook of International Humanitarian Law,* Oxford, 2008, p. 98.
[537] M. Sassòli, *Combatants*, in *MPEPIL*, 2015.
[538] L'unica eccezione a questa regola concerne gli individui *hors de combat*, ossia coloro che non possono più essere oggetto della violenza bellica avversaria perché hanno manifestato l'intenzione di arrendersi, sono in potere dell'avversario o, ancora, risultano incapaci di difendersi in quanto feriti, malati o naufraghi. Sul punto: R. Goodman, *The Power to Kill or Capture Enemy Combatants*, in *European Journal of International Law*, 2013, pp. 819-853; D. M. Banaszewska, *Hors de combat*, in *MPEPIL*, 2015.
[539] S. Watts, *Combatant Status and Computer Network Attack*, in *Virginia Journal of International Law*, 2010, pp. 415-420.
[540] G. Feo, *L'esercito italiano cambia pelle: due nuovi reggimenti per gestire droni e combattimenti cyber*, *La Repubblica*, 24 gennaio, 2024.
[541] J. Blessing, *The Global Spread of Cyber Forces*, *2000-2018*, in G. Visky, *et al.* (eds.), NATO CCDCOE Publications, Tallinn, 2021, pp. 233-255.

informatiche e delle infrastrutture critiche contro le minacce e gli attacchi provenienti dal ciberspazio e suscettibili di ledere i valori e gli interessi nazionali[542]. In quanto legittimi combattenti, i componenti di tali unità militari hanno il diritto di prendere attivamente parte alle ostilità e sono, in qualsiasi momento, durante il conflitto, passibili di attacco (sia cinetico che telematico)[543]. Gli atti cibernetici ostili da loro compiuti sono imputabili allo Stato da cui dipendono e per conto del quale agiscono, fatta chiaramente eccezione per quelli configuranti crimini di guerra o altre gravi violazioni del diritto umanitario, per i quali viene invece in rilievo, come vedremo più avanti, il regime della responsabilità penale individuale[544].

2. *Segue:* L'applicabilità dello *status* di combattente legittimo ai membri del gruppo Anonymous nel corso del conflitto russo-ucraino

Pochi giorni dopo l'inizio del conflitto tra Russia e Ucraina, il 24 febbraio 2022, il collettivo di *hackers* che prende il nome di Anonymous ha dichiarato guerra alle forze armate russe[545]. Si stima che i suoi membri, in breve tempo, abbiano raccolto dati personali riguardanti più di centoventimila militari russi, riuscendo ad ottenere informazioni sensibili quali la data di nascita e il numero di passaporto e, allo stesso tempo, abbiano avuto accesso ai siti Web di diverse agenzie governative e agenzie di stampa russe, sottraendo migliaia di documenti[546].
Deve, tuttavia, essere esclusa la possibilità di qualificare tali soggetti alla stregua di "combattenti legittimi".
In primo luogo, infatti, non ci sembra possa affermarsi che Anonymous disponga di una struttura di comando ben identificabile. Sotto questo profilo, l'associazione appare più come un movimento che incoraggia i propri seguaci a compiere specifici

[542] https://www.cybercom.mil/.
[543] ICRC, *International Humanitarian Law Databases*, Rule 3.
[544] https://casebook.icrc.org/a_to_z/glossary/combatants.
[545] D. Milmo, *Anonymous: the hacker collective that has declared cyberwar on Russia*, *The Guardian*, 27 February 2022.
[546] S. Seibt, *Ukraine conflict presents a minefield for Anonymous and hacktivists*, in *France 24*, 23 March 2022.

atti di criminalità informatica, piuttosto che come un vero e proprio gruppo armato strutturato e gerarchicamente organizzato, con soggetti che rivestono posizioni apicali e sono capaci di dirigere e coordinare le attività dei suoi membri. Come precisato anche dal Manuale di Tallinn 2.0, il fatto che un certo numero di *hackers* stiano attaccando simultaneamente un certo Stato non implica di per sé che questi individui siano organizzati[547]. Ciò che qualifica un gruppo di *hackers* come gruppo organizzato che partecipa ad un conflitto armato è il fatto di avere un comando che coordina le attività dei singoli membri, ad esempio, individuando ed assegnando a ciascuno di essi un obiettivo militare da colpire con azioni informatiche[548].

Inoltre, non ci pare che il gruppo sia dotato di un codice di condotta che possa, in qualche modo, dimostrarne il carattere e la gestione militare[549]. Manca, infatti, un codice di disciplina in seno al gruppo che preveda in maniera chiara le regole per poter entrare a fare parte dello stesso e, eventualmente, delle sanzioni disciplinari nel caso in cui un membro adotti un comportamento contrario a quanto indicato[550].

In secondo luogo, oltre all'assenza di una tipica organizzazione militare e di una persona al comando che sia responsabile per la condotta dei propri subordinati, non si può di certo affermare che l'associazione appartenga ad una delle parti in lotta, dal momento che non vi è stata alcuna richiesta da parte del governo ucraino di intervenire in suo supporto e, soprattutto, non essendo i partecipanti al gruppo inquadrati tra le forze armate di detto Stato.

Infine, deve escludersi che la maschera normalmente utilizzata dai componenti del movimento durante le loro dichiarazioni sul Web possa considerarsi un'uniforme.

Affermare il contrario significa sostenere che ogni partecipante sia un obiettivo militare legittimo e, come tutti i militari durante le ostilità, possa essere colpito in qualsiasi momento ed in qualsiasi situazione esso si trovi, anche in circostanze non collegate al conflitto armato in corso (ipotesi del tutto inverosimile se si considera

[547] *Tallinn Manual 2.0*, cit., p. 390 ss.
[548] *Ibidem*.
[549] R. Buchan, *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, in *Chinese Journal of International Law*, 2016, p. 749.
[550] *Ibidem*.

che questi individui, solitamente, agiscono da terminali o da dispositivi informatici situati a notevole distanza dal teatro delle operazioni belliche).

3. I combattenti non privilegiati autori di attacchi telematici in situazioni di conflitto armato

Sono esclusi dalla categoria dei combattenti legittimi e non hanno diritto allo *status* di prigionieri di guerra dopo la cattura i mercenari, le spie e, infine, i sabotatori, i quali sono tutti ritenuti combattenti non privilegiati[551].

Devono essere qualificati come mercenari quegli *hackers* che reclutati, localmente o all'estero, da taluno dei belligeranti, partecipano direttamente alle ostilità[552].

A tale proposito, devono però sussistere le condizioni cumulative previste dall'art. 47 del I Protocollo Aggiuntivo del 1977, il cui testo prevede una definizione di mercenario piuttosto restrittiva[553]. Ai sensi della norma è mercenario chiunque: a)

---

[551] R. Baxter, *So-called "Unprivileged Belligerency": Spies, Guerrillas, and Saboteurs*, in *British Yearbook of International Law*, 1951, pp. 323-345; A. Behnsen, *The Status of Mercenaries and Other Illegal Combatants under International Humanitarian Law*, in *German Yearbook of International Law*, 2003, pp. 494-520; K. Dörmann, *The Legal Situation of Unlawful/Unprivileged Combatants*, in *International Review of the Red Cross*, 2003, pp. 45-74.; S. Scheipers, *Unlawful Combatants: A Genealogy of the Irregular Fighter*, Oxford, 2015. La categoria dei combattenti non privilegiati, alla quale appartengono i combattenti che – come vedremo – non rispettano l'obbligo di distinzione dalla popolazione civile, non deve essere confusa con quella dei cosiddetti combattenti illegittimi. I mercenari, le spie e, ancora, i sabotatori sono tutti soggetti che rientrano pienamente nella definizione di combattente prevista dalle norme di *ius in bello*, ma che – una volta catturati – non godono dello *status* di prigionieri di guerra. Per quanto concerne, viceversa, i combattenti illegittimi, si tratterebbe di una terza categoria di soggetti invocata da taluni Stati, come per esempio Israele, ed in cui vi rientrerebbero tutti quei membri di gruppi armati organizzati che partecipano in maniera continuativa al conflitto senza, tuttavia, soddisfare le condizioni richieste dalle pertinenti norme di *ius in bello* per poter essere considerati legittimi combattenti. In particolare, gli Stati Uniti hanno qualificato in questi termini i membri di Al Qaeda catturati in Afghanistan nel corso del 2001. Non essendo qualificabili come civili, i combattenti illegittimi sono passibili di attacco esattamente negli stessi termini in cui lo sono i combattenti legittimi. Si afferma, inoltre, che tali individui non hanno diritto né allo statuto di prigionieri di guerra, né al trattamento garantito ai civili trattenuti per motivi di sicurezza. Una siffatta interpretazione delle norme umanitarie non trova però adeguato riscontro nella prassi internazionale. L'esistenza di una terza categoria di soggetti che si ponga a cavallo fra quella dei civili e quella dei legittimi combattenti, oltre a non essere menzionata in alcuna convenzione di diritto bellico, è stata esclusa, infatti, sia dalla giurisprudenza internazionale, che da quella interna. K. Dörmann, *Combatants, Unlawful*, in *MPEPIL*, 2015.

[552] H. H. Dinnis, *Cyber Warfare and the Laws of War*, cit., p. 173.

[553] Su iniziativa dei Paesi del terzo mondo è stata conclusa, nel 1989, una Convenzione internazionale contro il reclutamento, l'impiego, il finanziamento e l'addestramento di mercenari. La Convenzione, entrata in vigore nel 2001, ha un oggetto ben più ampio dell'art. 47 del I Protocollo Aggiuntivo e non appartiene, a stretto rigore, al diritto umanitario. Tale strumento, vincolante 37

sia appositamente reclutato per combattere in un determinato conflitto armato; b) di fatto prenda direttamente parte alle ostilità; c) sia mosso essenzialmente da scopo di lucro; d) non sia cittadino di una parte in conflitto; e) non sia membro delle forze armate di una parte in conflitto; f) non sia stato inviato da uno Stato non parte nel conflitto in missione ufficiale quale membro delle forze armate di detto Stato[554].

Di conseguenza, affinché possano essere considerati alla stregua di mercenari, tali soggetti non dovranno né essere cittadini di una delle parti in lotta o residenti in un territorio da questa controllato, né essere membri delle sue forze armate[555]. Inoltre, dovranno essere motivati essenzialmente da scopi di lucro, nonché essere stati appositamente reclutati per combattere – mediante strumenti informatici – in quello specifico conflitto armato[556].

In caso di cattura, in quanto combattenti non privilegiati, essi non avranno diritto al trattamento di prigionieri di guerra e saranno, di conseguenza, alla completa mercè dell'avversario[557].

Il trattamento riservato ai mercenari è diverso da quello previsto dalle norme di diritto bellico per i c.d. *contractors*. Di conseguenza, la condizione degli *hackers* mercenari che affiancano il belligerante nel corso delle ostilità deve essere tenuta distinta da quella delle società militari private (*Private Military Companies*) che svolgono, dietro compenso, nell'ambito del conflitto, funzioni nel settore della sicurezza informatica commissionate dallo Stato[558].

Stati tra cui l'Italia, pone il divieto di utilizzo di mercenari tanto nel contesto di conflitti armati internazionali, quanto in quello di conflitti armati interni. T. Treves, *La Convention de 1989 sur les mercenaires*, in *Annuaire français de droit international*, 1990, p. 520 ss.

[554] Con riferimento all'elemento del profitto personale, l'art. 47 del I Protocollo Aggiuntivo precisa che al mercenario deve essere stata promessa una remunerazione materiale nettamente superiore a quella prevista per i combattenti aventi rango e funzioni simili nelle forze armate dello Stato che lo ha reclutato, localmente o all'estero. Questa indicazione è diretta ad escludere dalla categoria di mercenario gli stranieri che acconsentono a combattere per garantire il sostentamento proprio o quello delle loro famiglie, nonché gli stranieri che acconsentono a combattere per motivi puramente ideologici. J. Tercinet, *Les mercenaires et le droit international*, in *Annuaire français de droit international*, 1977, p. 269 ss.

[555] Parimenti, non possono essere qualificati mercenari gli esperti informatici ed i consiglieri militari membri delle forze armate di uno Stato terzo al conflitto e inviati da detto Stato in missione ufficiale.

[556] H. P. Hestermeyer, *Mercenaries*, in *MPEPIL*, 2010.

[557] K. Fallah, *Corporate Actors: The Legal Status of Mercenaries in Armed Conflict*, in *International Review of the Red Cross*, 2006, p. 599 ss.

[558] T. Maurer, *Cyber Mercenaries, The State, Hackers, and Power*, Cambridge, 2018.

Per quanto concerne i membri di queste ultime (chiamati, di solito, con l'acronimo inglese di «*contractors*»), questi saranno qualificati alla stregua di combattenti legittimi ove incorporati nelle forze armate dello Stato belligerante che li ha assoldati[559]. Tale inquadramento può avvenire attraverso una procedura formale secondo il diritto nazionale di detto Stato o *de facto*, mediante cioè l'assegnazione di funzioni continuative di combattimento[560].

In altri termini, ove siano parte di una struttura militare organizzata sottoposta ad un comando responsabile facente capo allo Stato che li ha assoldati e soggetta ad un sistema disciplinare interno in grado di garantire il rispetto delle norme di diritto internazionale umanitario, tali individui saranno legittimi destinatari della violenza bellica dell'avversario e, qualora catturati, avranno diritto al trattamento riservato ai prigionieri di guerra, sempreché, beninteso, abbiano avuto cura di distinguersi dalla popolazione civile[561].

In caso contrario, se del tutto estranei all'organizzazione militare dello Stato da cui dipendono, i "*cyber contractors*" saranno ritenuti come civili, con la conseguenza che non potranno prendere parte alle ostilità e, in caso di cattura, saranno punibili per gli atti di belligeranza eventualmente compiuti, non avendo diritto al trattamento di prigioniero di guerra[562]. Essi saranno, inoltre, suscettibili di attacco

---

[559] Sulla disciplina internazionale dei *contractors* vedi in generale: D. Avant, *The Market for Force: The Consequences of Privatizing Security*, Cambridge, 2005; S. Chesterman, C. Lehnardt (eds.) *From Mercenaries to Market: the Rise and Regulation of Private Military Companies*, Oxford, 2007; S. V. Percy, *Mercenaries: the History of a Norm in International Relations*, Oxford, 2007; C. Hoppe, *Passing the Buck: State Responsibility for Private Military Companies*, in *European Journal of International Law*, 2007, p. 989 ss; F. Francioni, N. Ronzitti, *War by Contract: Human Rights, Humanitarian Law, and Private Contractors*, Oxford, 2011; H. Tonkin, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge, 2011.

[560] Fra i *contractors* e lo Stato per cui questi svolgono la propria attività militare, raramente vi è un rapporto diretto, poiché ad assoldarli sono, in genere, le compagnie militari private. A differenza dei mercenari, essi hanno, peraltro, spesso la nazionalità dello Stato che ne richiede i servigi. Pur avendo compiti di combattimento, i *contractors* non devono soddisfare i numerosi criteri prescritti dall'art. 47 del I Protocollo Aggiuntivo. A. Annoni, F. Salerno, *La tutela internazionale della persona umana nel diritto internazionale*, cit., p. 118.

[561] C. Lehnardt, *Private Military Companies*, in *MPEPIL*, 2011.

[562] E. C. Gillard, *Business Goes to War: Private Military Security Companies and International Humanitarian Law*, in *International Review of the Red Cross*, 2006, p. 525 ss.

solamente mentre impegnati nella commissione di un atto qualificabile come partecipazione diretta alle ostilità[563].

4. *Segue:* La disciplina dello spionaggio cibernetico in tempo di guerra

I mercenari devono essere, inoltre, differenziati dalle spie[564]. Mentre i primi non usufruiscono in nessun modo delle tutele disposte per i combattenti, per le spie è necessario effettuare una distinzione[565]. Qualora si tratti di componenti dell'esercito di una parte in conflitto che raccolgono informazioni segrete nel territorio dello Stato avversario indossando l'uniforme delle forze armate a cui appartengono, tali soggetti non saranno considerati spie, bensì combattenti legittimi[566].
Ai sensi dell'art. 29 del Regolamento annesso alla IV Convenzione dell'Aia del 1907, viene considerata spia una persona che «agendo clandestinamente o sotto falsi pretesti ottiene o cerca di ottenere informazioni nella zona di operazioni del belligerante, con l'intenzione di comunicarle al nemico»[567].
Elementi caratterizzanti lo spionaggio sono, dunque, il fine di ottenere informazioni di valore militare e la volontà di comunicarle al nemico[568]. Non possono, pertanto, ritenersi spie coloro che vengono a conoscenza di dette informazioni casualmente o coloro i quali non hanno intenzione di trasmettere al nemico le informazioni carpite[569]. Dalla norma si evince, inoltre, come soltanto la raccolta di informazioni rilevanti per le parti belligeranti possa qualificarsi come spionaggio[570]. Non rientra, invece, in questa categoria l'attività che abbia ad oggetto informazioni prive di collegamento con il conflitto armato[571].

---

[563] S. Lewis, *The Targeting of Civilian Contractors in Armed Conflict*, in *Yearbook of International Humanitarian Law*, 2006, p. 25 ss.
[564] ICRC, *International Humanitarian Law Databases*, Rule 107.
[565] M. Castellaneta, *Conflitti armati (diritto internazionale)*, cit., p. 329.
[566] *Ibidem*.
[567] Le informazioni trasmesse all'avversario devono essere carpite agendo clandestinamente oppure sotto falsi pretesti, con la conseguenza che un militare in uniforme non può quindi essere considerato come dedito allo spionaggio.
[568] G. Balladore Pallieri, *Il diritto bellico*, Padova, 1954, p. 223.
[569] https://casebook.icrc.org/a_to_z/glossary/spies.
[570] A. P. Sereni, *Diritto internazionale, IV, Conflitti internazionali*, Milano, 1965, p. 1880.
[571] *Ibidem*.

Secondo quanto stabilito dall'art. 46, par. 1, del I Protocollo Aggiuntivo del 1977, le spie non godono, in caso di cattura, né del trattamento di prigionieri di guerra, in quanto combattenti non privilegiati, né delle garanzie che spettano, di regola, ai civili che si trovano in mano all'avversario[572]. La norma ha adattato lo spionaggio alla nuova realtà della guerra. Risulta, infatti, venuto meno il requisito restrittivo della «zona di operazioni del belligerante»: pertanto, oggi, un atto di spionaggio può essere commesso in qualsiasi parte del territorio controllato dallo Stato nemico. Da un'analisi di insieme delle fonti normative convenzionali citate si evince che, pur non essendo dichiarata esplicitamente lecita, l'attività di spionaggio viene, comunque, inquadrata nell'ambito di quelle misure legittime adottabili durante un conflitto armato, in quanto strumento di difesa o di offesa per le parti in lotta[573].

Lo spionaggio condotto in tempo di guerra non è, dunque, di per sé vietato dal diritto internazionale[574]. Del resto, l'art. 24 della IV Convenzione dell'Aia sulle leggi e gli usi della guerra terrestre riconosce come lecito l'impiego dei mezzi necessari per procurarsi informazioni inerenti al nemico nel suo territorio, allo scopo di indebolirne la difesa ed aumentare la propria capacità di offesa[575]. Tale disciplina corrisponde al diritto internazionale consuetudinario[576]. Ciononostante, essa trova applicazione soltanto nei conflitti armati internazionali[577].

Ora, nulla impedisce alle Potenze belligeranti di effettuare, nel corso di un conflitto armato, anche operazioni di spionaggio di tipo cibernetico[578]. A giudizio di chi scrive, in assenza di un diritto pattizio che disciplini espressamente la dimensione del ciberspazio, occorrerà fare riferimento, in via analogica, a quanto statuito dalle

[572] C. Schaller, *Spies*, in *MPEPIL*, 2009.
[573] M. C. Ciciriello, *Spionaggio (Diritto internazionale)*, in *Enciclopedia giuridica*, vol. XXX, p. 1993.
[574] E. Crawford, A. Pert, *International Humanitarian Law*, Cambridge, 2020, p. 107.
[575] M. C. Ciciriello, *Spionaggio (Diritto internazionale)*, cit., p. 1993.
[576] W. H. Boothby, *The Law of Targeting*, Oxford, 2012, p. 277.
[577] *Ivi*, p. 276.
[578] Sulla disciplina dello spionaggio cibernetico svolto in tempo di pace vedi, su tutti, R. Buchan, *Cyber Espionage and International Law*, Oxford, 2018; P. O. Kaan, *Confronting Cyber Espionage under International Law*, New York, 2019; T. Moulin, *Cyber-espionage in International Law*, Manchester, 2023.

regole del diritto umanitario tradizionali, sempreché applicabili al singolo caso di specie[579].

In altri termini, in tempo di guerra, l'attività di spionaggio (sia esso cibernetico o meno) non è ritenuta in sé un'attività sottoposta a divieto da parte del diritto internazionale[580]. La liceità dello spionaggio in presenza di uno stato di guerra, a prescindere dalle modalità attraverso cui questo viene condotto, è confermata dalla prassi, passata e presente, degli Stati e ammessa dalla maggioranza della dottrina internazionalistica[581].

Lo spionaggio cibernetico svolto in maniera deliberatamente clandestina fa sì, tuttavia, che il suo autore possa essere qualificato come spia. Occorre però che l'individuo autore dell'operazione sia geograficamente collocato nel territorio della parte avversa. La necessità della presenza fisica dell'agente in detto territorio per tutto il tempo in cui compie l'azione è considerata, invero, una *conditio sine qua non* per l'applicazione delle norme in materia di spionaggio da larghissima parte della dottrina[582]. Come affermato da Balladore Pallieri «non è mai spia colui che raccoglie informazioni intorno ad un esercito avversario, restando o nel proprio Stato o in uno Stato neutrale»[583]. Di conseguenza, dovrebbe essere negato lo *status* di spia a quei soggetti che effettuano operazioni di spionaggio cibernetico avvalendosi di *servers* situati nel territorio di uno Stato estraneo al conflitto armato.

In conclusione, riteniamo che la sottrazione di dati riservati attraverso strumenti telematici possa astrattamente essere assimilata alle condotte qualificabili come spionaggio e, conseguentemente, che gli individui responsabili possano essere considerati spie laddove sussista la compresenza dei requisiti della clandestinità della condotta, del fine della raccolta delle informazioni e della presenza fisica dell'agente nel territorio controllato dall'avversario.

---

[579] G. Gallo, *I cavi sottomarini e il diritto internazionale: quale protezione per le cosiddette "arterie" della globalizzazione?*, cit., p. 393.
[580] L. C. Green, *The contemporary law of armed conflict*, Manchester, 2008, p. 145.
[581] *Ibidem*.
[582] Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, cit., p. 277.
[583] G. Balladore Pallieri, *Il diritto bellico*, cit., p. 224.

Analogo discorso vale per coloro che, in fase di conflitto armato, tramite l'utilizzo di strumenti cibernetici, si siano resi autori di atti di sabotaggio.

Il sabotaggio non è definito dal Regolamento annesso alla IV Convenzione dell'Aia del 1907, né disciplinato dal I Protocollo Aggiuntivo del 1977. Ad ogni modo, può essere ritenuto come l'atto di chi penetra nel territorio soggetto al controllo del nemico allo scopo di compiere atti ad esso nocivi mediante la distruzione di beni[584].

Il sabotaggio è proibito se commesso in abiti civili o indossando la divisa nemica, anche quando l'utilizzo di quest'ultima è limitato alla sola penetrazione in territorio avversario[585]. Nel primo caso, infatti, si ha una violazione della disposizione del diritto di guerra che impone ai combattenti l'obbligo di distinguersi dai civili. Il militare che compie un'operazione di sabotaggio indossando la divisa del nemico commette, invece, una violazione dell'art. 39, par. 2, del I Protocollo, il cui testo vieta l'utilizzo di insegne, emblemi ed uniformi nemiche allo scopo di dissimulare, favorire, proteggere o impedire le operazioni belliche. Resta, invece, ammesso il sabotaggio commesso dietro le linee nemiche da militari in uniforme, purché i beni distrutti costituiscano un obiettivo militare[586].

Come più volte sottolineato, le operazioni cibernetiche vengono, di solito, condotte nell'anonimato da individui che si trovano al sicuro nel proprio Stato, spesso a migliaia di chilometri di distanza dal teatro dei combattimenti. Di conseguenza, nel contesto informatico, saranno considerati alla stregua di sabotatori solamente gli agenti in uniforme fisicamente presenti nel territorio della parte avversa oppure in un territorio da questa controllato che, attraverso l'impiego di mezzi telematici, si rendano autori di atti ad essa dannosi.

[584] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 188.
[585] https://casebook.icrc.org/a_to_z/glossary/saboteur.
[586] N. Ronzitti, *Diritto internazionale dei conflitti armati*, cit., p. 188.

5. Cyber Levée en masse

Sono tante le guerre, in passato, in cui la popolazione civile si è impegnata, in aggiunta ai membri delle forze armate, nella difesa del proprio territorio[587].
In base ad una risalente regola di diritto internazionale bellico, rinvenibile tanto nel Regolamento dell'Aia del 1907, quanto nella III Convenzione di Ginevra del 1949, viene riconosciuto ai civili di un territorio non ancora occupato, che non hanno avuto il tempo di organizzarsi in unità di forze armate regolari, all'avvicinarsi del nemico, il diritto di imbracciare spontaneamente le armi per respingere le truppe d'invasione, nel rispetto ovviamente delle norme consuetudinarie e convenzionali della guerra (cosiddetta levata di massa).
La disposizione presuppone che la popolazione non abbia avuto il tempo sufficiente di organizzarsi in vere e proprie unità di forze armate regolari. Di conseguenza, sono escluse come condizioni per il riconoscimento dello *status* di combattente legittimo, sia la presenza di una struttura organizzata e diretta da un responsabile, sia l'utilizzo di segni distintivi fissi riconoscibili a distanza[588]. Risulterebbe, infatti, particolarmente difficile pensare che in un arco di tempo così breve, come quello di un'invasione, i partecipanti di una *levée en masse* riescano ad organizzarsi in una struttura militare, nonché a munirsi di uniformi che li contraddistinguono[589].
Altro requisito essenziale della "levata in massa" è, poi, quello della spontaneità[590]. Occorre, in altri termini, che i membri di una *levée en masse* decidano di agire spontaneamente, senza cioè che vi sia stata la richiesta di una delle parti in lotta di intervenire in suo supporto[591].
Gli abitanti di un territorio occupato non godono, invece, di tale diritto perché in questo caso la popolazione civile – se vuole combattere contro l'occupante – deve

[587] Il concetto di "levata di massa" ha avuto origine durante le guerre rivoluzionarie francesi, in particolare, nel periodo storico immediatamente successivo al 16 agosto 1793.
[588] Commentario alla III Convenzione di Ginevra relativa al trattamento dei prigionieri di guerra, 1949, p. 68.
[589] *Ibidem*.
[590] W. S. Williams, R. Lawless, *Levée en Masse in Twenty-First-Century Armed Conflict*, in M. N. Schmitt (ed.), *Prisoners of War in Contemporary Conflict*, Oxford, 2023, p. 256 ss.
[591] *Ibidem*.

formare un movimento di resistenza organizzato[592]. Né la levata in massa è possibile nei confronti di un esercito che si ritira, dal momento che tanto il Regolamento dell'Aia, quanto la III Convenzione di Ginevra del 1949 fanno specificamente riferimento ad un esercito che invade il territorio di un altro Stato[593]. Gli abitanti in *levée en masse* possono agire anche qualora vi sia un esercito regolare ancora operante. Essi possono condurre le loro operazioni militari in connessione o separatamente da quest'ultimo[594].

Infine, ai sensi dell'art. 4 A 6) della III Convenzione di Ginevra, in caso di cattura, sono ritenuti prigionieri di guerra, in quanto combattenti legittimi, a condizione che portino in modo visibile le armi e rispettino gli usi e le leggi della guerra[595].

Secondo alcuni autori, in futuro, non si può escludere che, nel corso di un'invasione, la popolazione civile possa concretamente avvalersi di mezzi informatici come principale strumento di resistenza, per via della loro notevole accessibilità e facilità di impiego rispetto alla maggior parte delle armi tradizionali oggi esistenti[596].

Nei giorni immediatamente successivi all'invasione russa dell'Ucraina, il vice primo ministro ucraino Mykhaylo Fedorov ha annunciato, in un tweet, la creazione di un vero e proprio esercito cibernetico, conosciuto – a livello internazionale – con il nome inglese di *IT Army of Ukraine*[597]. Secondo i rapporti ufficiali, si stima che ad esso abbiano aderito fino a 400.000 persone provenienti da tutto il mondo[598]. I suoi membri sono divisi in unità informatiche sia offensive, che difensive: mentre l'unità offensiva aiuta l'esercito regolare ucraino a condurre massicce operazioni di spionaggio cibernetico a danno delle truppe d'invasione, quella difensiva invece è

[592] E. Crawford, *Tracing the Historical and Legal Development of the Levée En Masse in the Law of Armed Conflict*, in *Journal of the History of International Law*, 2017, p. 329 ss.
[593] *Ibidem*.
[594] E. David, *Principes de droit des conflits armés*, cit., p. 465.
[595] https://casebook.icrc.org/a_to_z/glossary/levee-en-masse.
[596] C. Waters, *New Hacktivists and the Old Concept of Levée En Masse*, in *The Dalhousie Law Journal*, 2014, p. 772 ss.
[597] *Ukraine cyber official: We only attack military targets*, *The Independent*, 4 March 2022.
[598] S. Schechner, *Ukraine's "IT Army" Has Hundreds of Thousands of Hackers, Kyiv Says*, *The Wall Street Journal*, 4 March 2022.

prevalentemente impiegata nella difesa di infrastrutture statali fondamentali, quali centrali elettriche e sistemi idrici[599].

Il governo ucraino ha utilizzato i canali della piattaforma Telegram per condividere un elenco di obiettivi militari che il suddetto esercito avrebbe dovuto attaccare[600].

Dall'inizio del conflitto armato, secondo diverse fonti ufficiali, risulta che i suoi partecipanti abbiano lanciato una vasta serie di *cyber attacks* contro importanti infrastrutture della Federazione Russa e abbiano messo temporaneamente fuori uso numerosi siti web appartenenti al Cremlino[601].

Ci si è chiesti, allora, se tali soggetti soddisfino i criteri richiesti dal diritto bellico per poter essere considerati *levée en masse* e, se sì, quali conseguenze giuridiche derivino da tale qualificazione[602].

Secondo taluni autori, come Buchan e Tsagourias, una tale ipotesi appare alquanto improbabile, in primo luogo, poiché la maggior parte dei volontari aderenti a questo peculiare esercito non sono abitanti del territorio invaso, ma operano rimanendo al sicuro in una località non rivelata e, in secondo luogo, perché – al momento in cui si scrive – una parte del territorio ucraino risulta occupata dal nemico[603].

La posizione ci sembra senz'altro da condividere. Oltretutto, in forza di quanto previsto dalle pertinenti regole di *ius in bello*, gli abitanti in *levée en masse* non possono mai colpire obiettivi militari situati nel territorio dello Stato aggressore e, nel caso del conflitto russo-ucraino, la maggior parte delle infrastrutture avversarie oggetto di *cyber attacks* rientra proprio in questa categoria di beni[604].

Più in generale, pare piuttosto difficile immaginare come i membri di una "cyber" levata di massa possano portare «apertamente» le armi in base a quanto richiesto dall'art. 4 A 6) della III Convenzione di Ginevra[605].

---

[599] J. Schectman, C. Bing, *Exclusive Ukraine calls on hacker underground to defend against Russia*, *Reuters*, 25 February 2022.
[600] M. Cage, *Is a Russian cyberwar coming?*, *The Washington Post*, 22 February 2022.
[601] D. Uberti, *Hackers Target Key Russian Websites*, *WSJ PRO Cybersecurity*, 28 February 2022.
[602] D. Wallace, *Levée En Masse in Ukraine: Applications, Implications, and Open Questions*, in *Lieber Institute West Point*, 11 March 2022.
[603] R. Buchan, N. Tsagourias, *Ukrainian "IT Army": A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?*, in *EJIL:Talk!*, 9 March 2022.
[604] D. Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, cit., p. 192.
[605] C. Waters, *New Hacktivists and the Old Concept of Levée En Masse*, cit., p. 772 ss.

La disposizione, a ben guardare, riserva la qualifica di combattente legittimo ai soli partecipanti alla levata di massa che portino le armi «apertamente» nel corso delle operazioni belliche[606]. Secondo Dinstein, l'espressione «apertamente» significa che i belligeranti – a seconda anche delle circostanze ambientali e della natura dell'arma – non devono nascondere le loro armi durante l'esecuzione o la preparazione di un attacco allo scopo di fingere di possedere lo *status* di civile[607]. Senza un'arma ben visibile, invero, risulta praticamente impossibile distinguere un *levée en masse* da un civile protetto[608].

Peraltro, è anche nell'interesse degli abitanti in *levée en masse* portare la armi in modo visibile al fine di essere riconoscibili e, conseguentemente, acquisire lo *status* di prigioniero di guerra in caso di cattura[609]. Se non lo fanno, essi corrono il rischio di venir processati per aver violato una regola basilare del diritto di guerra[610].

A nostro avviso, la regola secondo cui i combattenti devono distinguersi dalla popolazione civile mentre sono coinvolti in un attacco o in un'operazione bellica preparatoria dello stesso è fondamentale e deve essere sempre osservata. Il lancio di un attacco informatico, che per sua stessa natura avviene a distanza, difficilmente potrà dirsi compatibile con tale regola, dal momento che l'esposizione aperta delle armi non sarebbe visibile dalle altre parti coinvolte nel conflitto armato. Per tale ragione, come osservato anche da altri autori[611], la nozione di levata in massa appare di scarsa rilevanza pratica nel contesto in esame.

6. I civili che prendono parte alle ostilità

Come più volte ribadito, l'art. 48 del I Protocollo Aggiuntivo del 1977 detta la regola fondamentale secondo cui i belligeranti hanno l'obbligo di distinguere, in

[606] UK Ministry of Defence, *The Manual of the Law of Armed Conflict*, cit., para. 4.8.
[607] Y. Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, cit., p. 54.
[608] D. Wallace, S. R. Reeves, *The Law of Armed Conflicts "Wicked" Problem: Levée en Masse in Cyber Warfare*, in *International Law Studies*, 2013, p. 664.
[609] T. Pfanner, *Military Uniforms and the Law of War*, in *International Review of the Red Cross*, p. 93 ss.
[610] D. Stephens, T. Skousgaard, *Flags and Uniforms in War*, in *MPEPIL*, 2009.
[611] D. Wallace, S. R. Reeves, *The Law of Armed Conflicts "Wicked" Problem: Levée en Masse in Cyber Warfare*, cit., p. 664.

ogni momento, tra beni di carattere civile e obiettivi militari, per un verso, nonché tra popolazione civile e combattenti, per altro verso[612].

Le operazioni militari non possono, di conseguenza, essere dirette né contro i civili, né contro i beni a questi appartenenti (che comprendono sia la proprietà privata che quella pubblica)[613].

Il divieto di attaccare la popolazione civile è stato ritenuto corrispondente al diritto consuetudinario dalla giurisprudenza del Tribunale internazionale penale per la *ex* Iugoslavia[614]. La sua violazione costituisce un crimine di guerra ai sensi di quanto prescritto dall'art. 8, lett. *b)*, dello Statuto della Corte penale internazionale.

Sono qualificati come civili tutti coloro che non appartengono alle forze armate dei belligeranti (tra queste sono da ricomprendere anche i combattenti irregolari)[615].

A differenza dei combattenti, i civili non hanno diritto a prendere attivamente parte alle ostilità[616]. Ove lo facciano, questi possono essere sottoposti alla potestà punitiva dello Stato avversario, anche qualora le loro azioni non siano qualificabili come crimini di guerra[617].

La partecipazione diretta alle ostilità comporta per i civili la perdita temporanea della protezione dagli attacchi normalmente loro riconosciuta[618]. In altri termini,

---

[612] La popolazione civile non è suscettibile di attacco nemmeno a titolo di rappresaglia (art. 51, par. 6, I Protocollo Aggiuntivo del 1977). Con il termine rappresaglia bellica si intende la violazione, da parte di un belligerante, di una norma di diritto umanitario in risposta ad una precedente violazione di una simile norma commessa dal nemico. Il diritto umanitario contemporaneo non vieta, in termini assoluti, il ricorso a questo particolare genere di contromisura, ma lo sottopone, ad ogni modo, a stringenti limitazioni. Il I Protocollo di Ginevra vieta, ad esempio, le rappresaglie belliche contro i feriti, i malati e i naufraghi (art. 20). M. Ruffert, *Reprisals*, in *MPEPIL*, 2021.

[613] ICRC, *International Humanitarian Law Databases*, Rule 1 and Rule 7.

[614] Tribunale penale internazionale per la *ex* Iugoslavia, *Prosecutor v. Kupreskic*, ICTY, Case No IT-95-16, 14 gennaio 2000, par. 513.

[615] N. Ronzitti, *Civilian Population in Armed Conflict*, in *MPEPIL*, 2010.

[616] F. Kalshoven, L. Zegveld, *Constraints on the Waging of War: An Introduction to International Humanitarian Law*, Geneva, 2001, pp. 99-100.

[617] Al contrario, come detto in precedenza, i combattenti non sono punibili per aver preso parte alle ostilità, ma soltanto per l'eventuale commissione di crimini di guerra.

[618] Tale regola è espressione del diritto internazionale consuetudinario. J. M. Henckaerts, L. Doswald-Beck (eds.), *Customary International Humanitarian Law, Vol. I: Rules*, cit., Rule 6, pp. 19-24.

per tutta la durata di detta partecipazione, essi possono essere oggetto della violenza bellica del nemico[619].

Il concetto di partecipazione diretta alle ostilità non risulta però sempre di facile determinazione[620]. Nel 2008, nel tentativo di meglio definire i contorni della regola, il Comitato internazionale della Croce Rossa ha redatto una guida interpretativa di tale nozione[621], fondata sulle tre seguenti condizioni che devono (cumulativamente) realizzarsi[622]:

a) deve sussistere la concreta probabilità che le azioni del civile siano in grado di nuocere alle capacità militari o alle operazioni militari del nemico o, in alternativa, di comportare la morte ed il ferimento di persone, oppure il danneggiamento e la distruzione di beni protetti dagli attacchi (criterio della soglia)[623];
b) deve esserci poi un nesso di causalità tra l'azione del civile e il danno che si verifica come conseguenza diretta di tale azione o dell'operazione militare di cui tale azione è parte integrante (cosiddetto nesso di causalità)[624];
c) l'azione deve essere specificatamente diretta a cagionare il danno e favorire, così, una parte in conflitto a detrimento dell'altra (nesso bellico)[625].

---

[619] Ciò non vuol dire che colui che imbracci le armi contro l'avversario perda la propria qualifica di civile divenendo combattente, ma semplicemente che il belligerante nemico è autorizzato a ricorrere all'impiego della violenza bellica nei suoi confronti.

[620] In un conflitto armato non internazionale la partecipazione diretta alle ostilità discenderebbe dal coinvolgimento dell'individuo nella preparazione, esecuzione o comando di operazioni militari nell'ambito di un gruppo armato organizzato.

[621] Tale documento ha suscitato vivaci critiche fra gli studiosi della materia. Vedi, su tutti, D. Akande, *Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities*, in *International and Comparative Law Quarterly*, 2010, p. 180 ss.

[622] Soltanto in presenza delle tre suindicate condizioni cumulative il civile perde la protezione di cui normalmente gode e diviene legittimo obiettivo della violenza bellica del nemico.

[623] La soglia del danno prevista dalle linee guida – non giuridicamente vincolanti – del Comitato internazionale della Croce Rossa non è, dunque, limitata ai soli atti di belligeranza capaci di causare morte, lesioni di persone e distruzione di beni, ma ricomprende anche tutte quelle azioni suscettibili di influenzare negativamente le operazioni militari o la capacità militare del nemico.

[624] La sussistenza del nesso di causalità dipende dal tipo di attività che il civile svolge: alcune di esse sono per loro natura idonee ad essere considerate diretta partecipazione alle ostilità, mentre altre devono essere necessariamente valutate caso per caso, sulla base della loro esatta finalità. ICTY, *The Prosecutor v. Strugar*, IT-01-42-A, 17 luglio 2008, par. 177.

[625] Il ricorso alle armi per legittima difesa non configura una ipotesi di partecipazione diretta alle ostilità, dal momento che il civile, in questo caso, non agisce nell'interesse di una delle parti in lotta, ma semplicemente per tutelare la propria incolumità.

Le raccomandazioni fornite dal Comitato internazionale della Croce Rossa nel 2008 riguardano anche la durata della partecipazione diretta alle ostilità[626]. Queste chiariscono, invero, in che misura le attività che precedono e quelle che seguono l'effettuazione di un attacco possano essere ritenute parti integranti dello stesso e considerano conclusa detta partecipazione nel momento in cui il civile rientra dal luogo di esecuzione dell'attacco, deponendo eventualmente le armi utilizzate[627].
Ove la partecipazione diretta alle ostilità si riveli essere del tutto sporadica, il civile potrà divenire oggetto di attacco soltanto nel momento in cui risulta effettivamente impegnato nel compimento dell'atto di belligeranza (oppure nelle fasi prodromiche o immediatamente successive allo stesso)[628]. Potrà, invece, essere attaccato anche negli intervalli di tempo che intercorrono tra un atto ostile e quello susseguente qualora faccia parte di un gruppo di resistenza organizzato[629].
Inoltre, quando dai civili vengono condotti atti ostili da località remote, come nel caso degli attacchi di natura informatica, la citata guida interpretativa afferma espressamente che: «*the duration of direct participation in hostilities will be*

[626] https://casebook.icrc.org/a_to_z/glossary/direct-participation-hostilities.
[627] A seguito di tale momento, il soggetto in questione tornerà a beneficiare della protezione dagli attacchi riconosciutagli pur rimanendo, allo stesso tempo, passibile di cattura per avere preso indebitamente parte alle ostilità. La *ratio* del divieto di attaccare i civili che non stanno prendendo direttamente parte alle ostilità, a prescindere dal loro oggettivo coinvolgimento (passato o futuro) nei combattimenti, è quella di evitare l'uccisione di persone innocenti. Prima di colpire un civile nemico è necessario identificare l'individuo presunto responsabile di atti di violenza armata, ossia stabilire se si è realmente di fronte ad un civile innocente o ad un civile che ha illegittimamente preso parte alle ostilità. Soltanto se il civile è catturato mentre è impegnato nell'azione militare sul campo di battaglia non possono esservi dubbi circa il suo *status* e la sua responsabilità personale per aver attaccato illegittimamente il nemico. Il belligerante che abbia l'assoluta certezza che i civili stavano effettivamente prendendo parte attiva alle ostilità può colpirli soltanto come *extrema ratio*, qualora risultasse impossibile catturarli. In altri termini, i belligeranti devono sempre tentare di catturare i civili sospettati di prendere parte indebitamente alle ostilità, utilizzando mezzi letali soltanto ove appaia impossibile catturarli. Al contrario, per quanto concerne i civili diversi da quelli catturati mentre compiono azioni militari nel campo di battaglia, il belligerante è libero di procedere con il loro arresto. Occorre però provare in via giudiziaria, ossia a seguito di un giusto processo, che essi intendevano commettere atti ostili o che abbiano commesso tali atti. A. Cassese, P. Gaeta, *Le sfide attuali del diritto internazionale*, Bologna, 2008, pp. 78-79.
[628] Secondo il documento, costituiscono partecipazione diretta alle ostilità solo le azioni preparatorie allo svolgimento di uno specifico attacco, mentre non assumono alcuna rilevanza le attività genericamente finalizzate alla realizzazione di futuri atti ostili. CICR, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, May 2009, pp. 43-45.
[629] N. Melzer, *Civilian Participation in Armed Conflict*, in *MPEPIL*, 2010.

restricted to the immediate execution of the act and preparatory measures forming an integral part of that act»[630].

Infine, sempre secondo quanto affermato dal Comitato internazionale della Croce Rossa: «*The electronic interference with military computer network […] whether through computer network attacks (CNA) or computer network exploitation (CNE) […]*» rappresenta un tipico esempio di partecipazione diretta alle ostilità qualora soddisfi i tre suindicati criteri (*threshold of harm*, *direct causation*, *belligerent nexus*)[631].

Ciò premesso, è possibile individuare tre distinte categorie di civili potenzialmente coinvolti in un conflitto armato caratterizzato dal ricorso all'impiego di strumenti telematici: a) coloro i quali sviluppano i programmi informatici successivamente utilizzati, con scopi di offesa o di difesa, nel corso delle ostilità dai belligeranti; b) coloro che forniscono attività di mera assistenza e manutenzione tecnica alle parti in lotta; c) coloro i quali procedono alla installazione o all'attivazione del *software* malevolo sui sistemi informatici avversari sferrando, di fatto, l'attacco telematico[632].

Questi ultimi possono agire sia su istruzioni da parte dello Stato belligerante, sia in modo del tutto indipendente, per supportare un belligerante a scapito di un altro, come nelle ipotesi dei cosiddetti "*patriotic hackers*"[633].

Ora, per quanto concerne la prima categoria di individui, a nostro giudizio, non vi è partecipazione diretta alle ostilità dal momento che manca il nesso di causalità tra la condotta posta in essere dal civile e il danno che da quel comportamento deriva. Non vi è, invero, nessun nesso causale diretto tra l'attività compiuta dal civile, ossia lo sviluppo del programma informatico e i danni che potrebbero derivare dal suo utilizzo, da parte dei belligeranti, in situazioni di conflitto armato[634]. In altri termini,

---

[630] CICR, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, cit., p. 68.
[631] *Ivi*, p. 48.
[632] D. Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, in *Journal of Conflict and Security Law*, 2012, p. 295.
[633] M. Roscini, *Cyber Operations and the Use of Force in International Law*, cit., p. 204.
[634] E. Crawford, *Identifying the Enemy Civilian Participation in Armed Conflict*, Oxford, 2015, p. 148.

la condotta del programmatore del *software* malevolo non si inserisce nel quadro delle operazioni militari che hanno determinato il verificarsi del danno. La condotta del programmatore non fa, pertanto, in nessun modo parte del conflitto armato o, comunque, non è così strettamente a questo connessa da divenirne parte integrante. In altri termini, essa non ha alcun collegamento diretto con le ostilità, non essendo intenzionalmente a sostegno di una parte in lotta e a danno dell'altra.

Parimenti anche coloro i quali, durante i combattimenti, forniscono ai belligeranti solo assistenza tecnica non partecipano direttamente alle ostilità, dal momento che anche la loro attività non soddisfa il requisito essenziale del nesso di causalità[635]. Manca, invero, un collegamento diretto e prossimo tra la condotta di tali soggetti ed il danno prodotto. Sul punto la Guida interpretativa appare piuttosto chiara nel sottolineare la necessaria presenza di un nesso causale sufficientemente stretto tra il comportamento del civile e il danno verificatosi come conseguenza dello stesso, escludendo, pertanto, che una semplice facilitazione alla realizzazione del danno possa rientrare nel concetto di partecipazione diretta alle ostilità[636].

Ai sensi dell'art. 4 A 4) della III Convenzione di Ginevra del 1949, gli individui che seguono fisicamente le forze armate senza, tuttavia, farne direttamente parte – come, ad esempio, i corrispondenti di guerra, i fornitori ed i membri di unità di servizi incaricati del benessere delle truppe – sono equiparati, in caso di cattura, ai prigionieri di guerra. Poiché si tratta di individui privi di vere e proprie funzioni di combattimento, tali soggetti mantengono lo *status* di civile e non possono essere fatti oggetto di attacco. I tecnici informatici incaricati della manutenzione di siti web, programmi *software*, apparecchiature digitali e reti telematiche militari che accompagnano le forze armate in presenza di una autorizzazione da parte di queste ultime, a nostro parere, possono rientrare in tale categoria di persone, a patto che siano solo un anello della catena causale che determina il verificarsi del danno e non abbiano fornito un contributo decisivo ed autonomo al realizzarsi dello stesso.

---

[635] *Ivi*, pp. 146-147.

[636] CICR, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, cit., p. 52.

Diversamente, prendono direttamente parte alle ostilità i civili che hanno volontariamente lanciato l'operazione informatica, a condizione che quest'ultima: a) sia suscettibile di influire negativamente sulle capacità militari o sulle operazioni militari del nemico o, alternativamente, comporti la morte, il ferimento di persone o la distruzione ed il danneggiamento di beni protetti; b) sia volta ad arrecare un vantaggio ad una parte in conflitto e danneggiare l'altra; c), il danno provocato sia la conseguenza diretta ed immediata della stessa[637].

Appare, invece, alquanto incerto lo *status* di quei civili coinvolti nella conduzione di attacchi telematici senza esserne però consapevoli, in quanto il loro computer risulta gestito da un *botmaster*[638], il quale si avvale del dispositivo per effettuare attacchi cibernetici di tipo *DDoS*[639]. In tali casi, come correttamente sostenuto da Roscini, se l'attacco informatico costituisce un «attacco» ai sensi dell'art. 49, par. 1, del I Protocollo del 1977, si configura certamente una ipotesi di partecipazione diretta alle ostilità da parte del *botmaster*, il quale sarà inevitabilmente soggetto alla legge del *targeting* ai sensi dell'articolo 51, par. 3, del I Protocollo Aggiuntivo, durante l'intera durata di detta partecipazione[640]. Al contrario, per quanto concerne i civili coinvolti nell'operazione, una siffatta situazione è per certi versi analoga, a nostro avviso, a quella dei civili che trasportano inconsapevolmente le armi in luogo di conflitto armato. Pertanto, come sottolinea la guida interpretativa del Comitato internazionale della Croce Rossa: «*when civilians are totally unaware of the role they are playing in the conduct of hostilities…or when they are completely deprived of their physical freedom of action, they remain protected against direct attack despite the belligerent nexus of the military operation in which they are being instrumentalized. As a result, these civilians would have to be taken into account in*

[637] D. Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, cit., p. 295.
[638] Per una definizione esaustiva di *botnet* si rimanda a: https://www.enisa.europa.eu/topics/incident-response/glossary/botnets.
[639] Per una definizione di *denial-of-service attack* si rinvia invece a: https://www.cisa.gov/news-events/news/understanding-denial-service-attacks.
[640] M. Roscini, *Cyber Operations and the Use of Force in International Law*, cit., pp. 210-211.

the proportionality assessment during any military operation likely to inflict incidental harm on them»[641].

La tesi, avanzata da una parte della dottrina[642], secondo cui i c.d. *botnets* sarebbero obiettivi militari legittimi è, dunque, da respingere, dal momento che la mera presenza in seno alla popolazione civile di singoli individui che non rispondono alla definizione di persona civile non priva detta popolazione della sua qualità di civile (art. 50, par. 3, I Protocollo).

In definitiva, l'evoluzione tecnologica ha sicuramente portato i civili ad essere sempre più coinvolti nelle ostilità, spesso senza trovarsi fisicamente sul teatro dei combattimenti[643]. Ciononostante, i criteri del danno al nemico, del nesso causale chiaro e diretto fra tale danno e l'attività posta in essere e del collegamento fra detta attività ed il conflitto, sembrano trovare riscontro unicamente per quei civili che, di fatto, sferrano l'attacco telematico. Viceversa, non possono essere ritenuti alla stregua di civili che prendono direttamente parte alle ostilità coloro che risultano coinvolti solo indirettamente nell'attacco informatico (programmatori, istruttori, analisti informatici e così via).

5. *Segue:* La configurabilità dell'attività di *cyber exploitation* come partecipazione diretta alle ostilità

A ben guardare, come messo in evidenza da una parte della dottrina[644], la nozione di «atti di ostilità» è ben più ampia rispetto a quella di «attacco». Di conseguenza, comportamenti come le attività di *intelligence* che non rientrano nella definizione propria di «attacco» (a prescindere dai mezzi tramite cui dette attività vengono

[641] CICR, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, cit., p. 60.
[642] R. Geiss, H. Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, cit., 2012, p. 385.
[643] M. H. Hoffman, *The Legal Status and Responsibilities of Private Internet Users under the Law of Armed Conflict: A Primer for the Unwary on the Shape of Law to Come*, in *Washington University Global Studies Law Review*, 2003, p. 425.
[644] C. Pilloud, *et al.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, cit., pp. 618-619.

effettuate) sono considerati «atti di ostilità» qualora vadano in fase difensiva o offensiva a detrimento del nemico[645].

Ne discende che, si configura come diretta partecipazione alle ostilità l'attività di raccolta di dati ed informazioni riservate attraverso l'utilizzo di sistemi informatici (*cyber exploitation*)[646].

Tale attività è, infatti, in grado di arrecare un pregiudizio alla compagine militare avversaria, dal momento che la raccolta e sottrazione di dati e informazioni segrete può risultare decisiva per il successo di una determinata operazione militare. La possibilità che tali azioni si configurino come partecipazione diretta alle ostilità è, fra l'altro, riconosciuta dalle linee guida del Comitato internazionale della Croce Rossa[647].

La sottrazione di dati aventi valore militare, attraverso strumenti informatici, viene impiegata sia genericamente, per pianificare una campagna militare e monitorare la risposta del nemico, sia specificamente, per rendere cioè possibili singoli attacchi. Secondo Longobardo, le attività di generica raccolta e sottrazione di informazioni in favore di una parte belligerante non costituiscono una diretta partecipazione alle ostilità, perché manca il nesso di causalità ininterrotto e decisivo fra la condotta dell'agente e un danno prodottosi nel teatro del conflitto armato[648]. Al contrario, se l'attività di *cyber exploitation* è utilizzata per carpire dati e informazioni necessarie a portare a termine una specifica operazione militare e l'attacco produce un danno

---

[645] Le operazioni di *cyber exploitation*, seppure abbiano in comune con gli attacchi cibernetici molte caratteristiche tecniche inerenti alle modalità di realizzazione, non sono però qualificabili come un «attacco» ai sensi del diritto internazionale umanitario. Tali attività militari, pur essendo spesso condotte contestualmente, devono, dunque, essere tenute distinte. Come opportunamente osservato: "*the primary technical difference between cyber-attack and cyber-exploitation is in the nature of the payload to be executed, a cyber-attack payload is destructive whereas a cyber-exploitation payload acquires information non-destructively*". R. W Aldrich, *How Do You Know You Are at War in the Information Age?*, in *Houston Journal of International Law*, 2000, p. 252.

[646] Non è avveniristico immaginare i cittadini di uno Stato impegnati, in tempo di guerra, in attività di *cyber exploitation*, dal momento che detta attività di *intelligence* risulta, di norma, condotta da agenzie statali, come la *Central Intelligence Agency (CIA)* americana, che possiedono lo *status* di civili.

[647] CICR, *Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, cit., pp. 1017-1018.

[648] M. Longobardo, *L'applicabilità delle norme riguardanti lo spionaggio e la partecipazione diretta dei civili alle ostilità al fenomeno del Cyber Exploitation*, in M. Distefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale: temi scelti*, Napoli, 2017, p. 59.

concreto all' avversario, l'attività espletata deve allora considerarsi partecipazione diretta alle ostilità[649].

La tesi sembra convincente poiché troverebbe conferma nella giurisprudenza del Tribunale internazionale penale per la *ex* Iugoslavia il quale ha indicato come civili direttamente coinvolti in ostilità gli «*intelligence agents*», nonché quelli impegnati in «*transmitting military information for the immediate use of a belligerent*», ritenendo invece « *the gathering and transmitting military information*» una forma di partecipazione indiretta alle ostilità, incapace di far venire meno l'immunità dagli attacchi[650].

Pertanto, devono essere respinte tanto l'opinione per cui l'attività di *intelligence* configuri sempre una partecipazione diretta alle ostilità, come sostenuto dal governo statunitense[651], quanto l'opposto convincimento secondo cui l'attività di *intelligence* sia sempre una forma di partecipazione solo indiretta alle ostilità e, come tale, non sia disciplinata dall'articolo 51 del I Protocollo Aggiuntivo del 1977[652].

Similmente, tale soluzione è stata accolta nel Manuale di Tallinn che considera diretta partecipazione alle ostilità soltanto l'attività di *intelligence* con un diretto e chiaro nesso causale con il danno arrecato al nemico[653].

In conclusione, si deve escludere la possibilità di qualificare alla stregua di civili che prendono parte alle ostilità gli agenti di *cyber exploitation* che siano membri delle forze armate; è invece possibile configurare come tali gli agenti di *cyber exploitation* che non siano membri delle forze armate solo allorquando le specifiche informazioni raccolte siano causa diretta di un danno al nemico prodottosi nel corso delle ostilità.

---

[649] *Ibidem*.
[650] Tribunale penale internazionale per la *ex* Iugoslavia, *The Prosecutor v. Strugar*, cit., par. 177.
[651] US AIR FORCE, *The Commander's Handbook*, Pamphlet 110-34, 1980, par. 2-8.
[652] L'art. 51, par. 3, del I Protocollo dispone che: «Le persone civili godranno di una protezione generale contro i pericoli derivanti dalle operazioni militari, salvo che esse partecipino direttamente alle ostilità e per la durata di detta partecipazione».
[653] *Manuale di Tallinn*, cit., p. 430.

8. La responsabilità penale individuale nel ciberspazio

Come detto, seppur opportunamente adattate ed interpretate, le regole ed i principi fondamentali del diritto internazionale umanitario che disciplinano la condotta delle ostilità e tutelano la popolazione ed i beni di carattere civile dagli effetti della guerra, si applicano anche agli attacchi di natura informatica. Una eventuale violazione delle suddette norme costituisce un crimine di guerra[654], a cui corrisponde la responsabilità penale individuale del suo autore[655].

Il Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica si occupa ampiamente della responsabilità penale individuale dell'autore di un attacco informatico qualificabile come crimine di guerra. Dopo aver stabilito espressamente, alla Regola 84, che: «*Cyber operations may amount to war crimes*

[654] Un crimine di guerra è una grave violazione di una norma consuetudinaria o pattizia del diritto internazionale umanitario, a cui corrisponde la responsabilità penale individuale del suo autore. A differenza dei crimini contro l'umanità, tali crimini devono essere commessi durante un conflitto armato a carattere internazionale o interno. Costituisce, quindi, elemento essenziale del crimine di guerra il nesso tra la condotta criminosa realizzata ed un conflitto armato internazionale o interno. I crimini di guerra possono essere commessi da personale militare contro i membri delle forze armate avversarie o i civili nemici, ma anche da civili contro i membri delle forze armate avversarie oppure i civili nemici. Per converso, i crimini commessi da membri delle forze armate contro i propri commilitoni (quale che sia la loro nazionalità) non costituiscono crimini di guerra: tali crimini possono rientrare nell'ambito del diritto militare interno dello Stato belligerante e in talune ipotesi (qualora abbiano le caratteristiche previste dal diritto internazionale) potrebbero essere qualificati come crimini contro l'umanità. L'elemento soggettivo del crimine di guerra è talvolta specificato dalla stessa norma internazionale che proibisce una determinata condotta criminosa. Quando le norme internazionali non stabiliscono, nemmeno implicitamente, quale sia l'elemento soggettivo richiesto, pare opportuno ritenere che esso debba corrispondere al dolo intenzionale o, in ultima analisi, se le circostanze lo permettono, a quello eventuale. La letteratura in materia di crimini di guerra è sterminata. Fra tutti, si rinvia a: H. Lauterpacht, *The Law of Nations and the Punishment of War Crimes*, in *British Yearbook of International Law*, XXI, 1944, pp. 58-95; G. Schwarzenberger, *International Law as Applied in International Courts and Tribunals*, *Vol. 2: The Law of Armed Conflict*, London, 1968; Y. Dinstein, M. Tabory (eds.), *War Crimes in International Law*, The Hague, 1996; T. Meron, *War Crimes Law Comes of Age: Essays*, Oxford, 1998; E. La Haye, *War Crimes in Internal Armed Conflicts*, Cambridge, 2008; A. Zahar , G. Sluiter, *International Criminal Law: A Critical Introduction*, Oxford, 2008; W. van der Wolf *et al.* (eds.), *War Crimes and International Criminal Law*, The Hague, 2010; E. Greppi, *I crimini dell'individuo nel diritto internazionale*, Milano, 2012; G. Acquaviva, *La repressione dei crimini di guerra nel diritto internazionale*, Milano, 2014; K. Ambos, *Treatise on International Criminal Law: The Crimes and Sentencing*, *Vol. 2*, Oxford, 2014; A. Schwarz, *War Crimes*, in *MPEPIL*, 2014; F. Mégret *et al*. (eds.), *The Oxford Handbook of International Criminal Law*, Oxford, 2018.

[655] La tesi secondo cui un attacco informatico sferrato in violazione di una norma consuetudinaria o pattizia del diritto internazionale umanitario configuri un crimine di guerra è condivisa da larga parte della dottrina. In questo senso, ad esempio, K. Ambos, *International Criminal Responsibility in Cyberspace*, in N. Tsagourias, R. Buchan (eds.), in *Research Handbook on International Law and Cyberspace*, cit., pp. 142-143.

and thus give rise to individual criminal responsibility under international law»[656], alla Regola 85, dispone, poi, quanto segue: «*Commanders and other superiors are criminally responsible for ordering cyber operations that constitute war crimes. Commanders are also criminally responsible if they knew or, owing to the circumstances at the time, should have known their subordinates were committing, were about to commit, or had committed war crimes and failed to take all reasonable and available measures to prevent their commission or to punish those responsible*»[657].

Come noto, nel diritto internazionale penale sono previste tre differenti forme di responsabilità penale individuale: a) la c.d. *responsibility for the perpetration* (responsabilità primaria), b) la *responsibility for contributing to the perpetration* (responsabilità secondaria o derivata) e, infine, c) la c.d. *command o superior responsibility*[658].

La *responsibility for the perpetration* è – in principio – la forma più grave di responsabilità penale individuale e si caratterizza per il controllo sulla commissione del crimine da parte del suo autore. Essa può essere diretta, indiretta o concorsuale. È diretta allorquando l'agente compie la condotta criminosa a titolo individuale, realizzando autonomamente ed in prima persona gli elementi costitutivi (oggettivi e soggettivi) del crimine[659]. Al contrario, è indiretta quando l'agente si avvale, nella commissione del crimine, di un altro soggetto che controlla ed utilizza come mero strumento[660]. Infine, la commissione è concorsuale se due o più soggetti collaborano consapevolmente e volontariamente alla realizzazione della condotta criminosa, in una situazione in cui ognuno dei contributi dei partecipanti alla stessa

[656] *Tallinn Manual 2.0*, rule 84, cit., p. 391.
[657] *Tallinn Manual 2.0*, rule 85, cit., p. 396.
[658] Il principio della responsabilità penale individuale si afferma, per la prima volta, con i Tribunali di Norimberga e di Tokyo, volti a giudicare i crimini internazionali commessi, rispettivamente, dalle forze armate tedesche e giapponesi durante il secondo conflitto mondiale. Fino ad allora erano soltanto gli Stati – e non gli individui – ad essere potenzialmente sanzionabili per le violazioni del diritto internazionale umanitario. A. G. O'Shea, *Individual Criminal Responsibility*, in *MPEPIL*, 2009.
[659] R. Cryer, *An Introduction to International Criminal Law and Procedure*, Cambridge, 2019, p. 362.
[660] *Ivi*, p. 364.

non soddisfa da solo gli elementi costitutivi del crimine, ma è comunque indispensabile affinché questo sia commesso[661].

La responsabilità primaria deve essere tenuta ben distinta dalla responsabilità secondaria o derivata, concernente, invece, chi ha partecipato alla commissione del crimine ordinando, sollecitando, inducendo o, ancora, agevolando la perpetrazione dello stesso[662].

Per quanto concerne, infine, la responsabilità da comando essa si configura come peculiare forma di partecipazione criminosa appositamente designata per la figura del comandante gerarchico, il quale risponde dei crimini commessi dai suoi subordinati per non aver adottato tutte quelle misure necessarie ed in suo potere per prevenire o reprimere il loro compimento[663].

Questo modello di partecipazione criminosa si spiega tenendo a mente la centralità della figura del superiore gerarchico nel diritto internazionale umanitario e trova la sua disciplina negli artt. 86 e 87 del I Protocollo Aggiuntivo del 1977, i quali stabiliscono, in sostanza, che il comandante gerarchico deve, in primo luogo, assicurarsi che i suoi subordinati conoscano i propri doveri e, in secondo luogo, prevenire o reprimere le eventuali violazioni delle norme di *ius in bello* da questi poste in essere[664].

La disciplina dettata dal I Protocollo è stata ripresa dall'art. 7, comma 3, dello Statuto del Tribunale per la *ex* Iugoslavia[665], dall'art. 6, comma 3, dello Statuto del

---

[661] A. Cassese, *International Criminal Law*, Oxford, 2008, p. 200.
[662] *Ivi*, p. 193 ss.
[663] G. Werle, *Principles of International Criminal Law*, The Hague, p. 265.
[664] *Ibidem*.
[665] Il Tribunale penale per la *ex* Iugoslavia è stato istituito dal Consiglio di sicurezza delle Nazioni Unite, nel 1993, con la risoluzione n. 827, a seguito delle notizie relative alle terribili atrocità commesse nel corso del conflitto sui territori della *ex* Iugoslavia. Molto si è discusso – al tempo dell'istituzione del Tribunale – sulla sua legittimità. In particolare, veniva messo in dubbio il fatto che il Consiglio di sicurezza avesse il potere di istituire tribunali penali internazionali. Una parte della dottrina osservava, all'epoca, che la creazione di organi giurisdizionali non rientrava nei poteri del Consiglio di sicurezza. La questione della legittimità dell'istituzione del Tribunale è stata, poi, anche sottoposta alla Camera d'appello del Tribunale stesso, nel corso del procedimento contro Dušan Tadić. A tal proposito, la Camera d'appello ha concluso che era ben possibile per il Consiglio di sicurezza istituire un tribunale penale internazionale come misura per reagire all'esistenza di una situazione di minaccia o di rottura della pace e della sicurezza internazionale. Sul tribunale penale per la *ex* Iugoslavia vedi tra gli altri: J. C. O'Brien, *The International Tribunal for Violations of International Humanitarian Law in the Former Yugoslavia*, in *American Journal of International Law*, 1993, pp. 639-659; A. Pellet, *Le tribunal criminel international pour l'ex-Yougoslavie: poudre*

Tribunale per il Ruanda[666] e, infine, dall'art. 28 dello Statuto della Corte penale internazionale.

In particolare, l'art. 28 dello Statuto di Roma statuisce che il comandante gerarchico è penalmente responsabile per i crimini commessi dalle proprie forze armate «sotto il suo effettivo comando e controllo o sotto la sua effettiva autorità e controllo», quando sapeva o aveva sufficienti informazioni che gli permettevano di sapere che i suoi sottoposti stavano per commettere (o avevano commesso) una condotta criminosa e non ha assunto le misure necessarie o ragionevoli per impedire, reprimere o deferire il crimine alle autorità competenti, a fini di inchiesta ovvero di esercizio dell'azione penale.[667].

Ora, come messo in evidenza da Sliedregt, tale modello di responsabilità personale assume assoluta rilevanza nel contesto informatico, dal momento che, come detto, numerosi Stati della comunità internazionale (quali, ad esempio, Cina, Giappone,

---

aux yeux ou avancée décisive?, in *Revue Générale de droit International Public*, 1994, pp. 7-60; D. Shraga, R Zacklin, *The International Criminal Tribunal for the Former Yugoslavia*, in *European Journal of International Law*, 1994, pp. 360-380; G. H. Aldrich, *Jurisdiction of the International Criminal Tribunal for the Former Yugoslavia*, in *American Journal of International Law*, 1996, pp. 64-69; J. E. Alvarez, *Nuremberg Revisited: The Tadic Case, Symposium: The International Tribunal for Former Yugoslavia Comes to Age*, in *European Journal of International Law*, 1996, pp. 245-264; C. Greenwood, *The Development of International Humanitarian Law by the International Criminal Tribunal for the Former Yugoslavia*, in *Max Planck Yearbook of United Nations Law*, 1998, pp. 97-140; G. Mettraux, *International Crimes and the Ad Hoc Tribunals*, Oxford, 2005; W. Schabas, *The UN International Criminal Tribunals: The Former Yugoslavia, Rwanda and Sierra Leone*, Cambridge, 2006.

[666] Il Tribunale penale per il Ruanda è stato creato dal Consiglio di sicurezza delle Nazioni Unite con la risoluzione n. 955 del 1994, a seguito del genocidio e della guerra civile scoppiata in Ruanda. L'attività del Tribunale è stata frenata dalla difficoltà di accesso alle zone di guerra e, più in generale, dalla distanza dell'organo giurisdizionale dai luoghi in cui sono stati commessi i crimini. Il Tribunale è stato criticato, poi, per i suoi alti costi, la sua scarsa capacità di fornire efficace protezione alle vittime ed ai testimoni, nonché per la lentezza e la lunghezza dei procedimenti. Inoltre, si è detto che i diritti della difesa non sono stati garantiti in modo soddisfacente, a causa dell'impossibilità di svolgere adeguate indagini difensive. Sul tribunale penale per il Ruanda si veda tra gli altri: R. S. Lee, *The Rwanda Tribunal*, in *Leiden Journal of International Law*, 1996, pp. 37-61; F. Megret, *Le Tribunal Pénal International pour le Rwanda*, Paris, 2002; M. Kamatali, *The Challenge of Linking International Criminal Justice and National Reconciliation: The Case of the ICTR*, in *Leiden Journal of International Law*, 2003, pp. 115-133.

[667] Qualora il crimine non sia stato ancora commesso, il superiore è punibile per non aver adottato le misure necessarie e ragionevoli per impedire il suo verificarsi. Qualora, al contrario, il crimine sia stato commesso, il superiore è responsabile per la mancata punizione dei suoi sottoposti, per la violazione del dovere di interrompere la commissione della condotta criminosa o, ancora, per non aver denunciato il fatto alle autorità competenti, affinché queste ultime svolgano indagini o avviino azioni penali. Sono necessarie le misure che il superiore è tenuto ad adottare in base ai suoi doveri, mentre sono ragionevoli le misure che, nel caso concreto, gli sono effettivamente possibili.

Corea del Nord, Corea del Sud, Stati Uniti, Regno Unito, Canada, Russia, Spagna, Israele, Italia, India, Francia e Germania) hanno creato all'interno delle proprie forze armate delle strutture militari specializzate nella conduzione di operazioni cibernetiche (sia offensive, che difensive)[668].

È proprio su quest'ultimo modello di responsabilità personale che appare, allora, opportuno soffermarsi maggiormente[669].

Affinché il superiore gerarchico possa rispondere per i crimini di guerra commessi dai suoi subordinati attraverso l'impiego di strumenti informatici devono sussistere cumulativamente tre elementi: a) il rapporto "superiore-subordinato"; b) l'elemento psicologico, rappresentato dalla consapevolezza effettiva o potenziale che il subordinato abbia compiuto (o stia per compiere) un crimine internazionale attraverso il mezzo telematico; c) la condotta omissiva consistente nel non avere preso tutte le misure necessarie e ragionevoli per prevenire l'attacco telematico o punirne l'autore.

In altri termini, occorre, anzitutto, che il comandante gerarchico abbia il controllo effettivo dei propri subordinati, ossia la materiale capacità di prevenire e sanzionare l'attacco cibernetico costituente un crimine di guerra[670]. Secondariamente, è necessario che egli sappia o abbia motivo o dovere di sapere che il subordinato stia per effettuare l'attacco cibernetico o, viceversa, lo abbia lanciato[671]. Da ultimo, il superiore non risponderà del crimine quando, pur avendo adottato tutte le misure a sua disposizione ed in suo potere, l'evento si sia lo stesso verificato, oppure il responsabile non sia stato comunque punito[672]. Infine, a nulla rileva, a nostro parere,

---

[668] E. van Sliedregt, *Command Responsibility and Cyberattacks*, in *Journal of Conflict and Security Law*, 2016, p. 521.

[669] Per una più dettagliata disamina in tema di responsabilità da commando, si veda: I. Bantekas, *The Contemporary Law of Superior Responsibility*, in *American Journal of International Law*, 1999, pp. 573-595; M. Lippman, *The Evolution and Scope of Command Responsibility*, in *Leiden Journal of International Law*, 2000, pp. 139-170; E. van Sliedregt, *The Criminal Responsibility of Individuals for Violations of International Humanitarian Law*, The Hague, 2003; G Mettraux, *The Law of Command Responsibility*, Oxford, 2009.

[670] E. van Sliedregt, *Command Responsibility and Cyberattacks*, cit., 2016, pp. 509-516.

[671] R. Buchan, N. Tsagourias, *Autonomous Cyber Weapons and Command Responsibility*, in *International Law Studies*, 2020, p. 651 ss.

[672] *Ibidem*.

ai fini del sorgere della responsabilità, che il comandante abbia o meno un certo grado di competenze informatiche.

Ai sensi dell'art. 28 dello Statuto di Roma, la *command responsibility* non si applica ai soli vertici militari, ma anche ai civili che abbiano un potere di controllo sui propri subordinati equiparabile a quello riscontrabile nelle strutture militari. Di conseguenza, saranno responsabili per il reato commesso dai subordinati anche quei civili – quali, per esempio, gli esperti informatici che assistono alla pianificazione o all'esecuzione dell'attacco telematico configurante un crimine internazionale – che abbiano un controllo effettivo sui loro subordinati paragonabile a quello dei superiori militari.

9. *Segue:* La giurisdizione della Corte penale internazionale in caso di attacchi informatici costituenti crimini di guerra

Una volta constatato che gli attacchi informatici offrono, oggi, nuove modalità per compiere molteplici crimini di guerra, è necessario chiedersi se i crimini di guerra perpetrati attraverso tali attacchi possano essere deferiti dinanzi alla Corte penale internazionale[673].

[673] La Corte penale internazionale (CPI) è un tribunale a carattere permanente, composto da 18 giudici indipendenti, di cui almeno 9 esperti in diritto e procedura penale ed almeno 5 esperti in diritto internazionale umanitario e dei diritti dell'uomo, nominati dai Governi ed eletti a scrutinio segreto dall'Assemblea degli Stati parti. La Corte ha sede all'Aia e le sue lingue di lavoro sono l'inglese e il francese. Essa può giudicare i crimini motivo di allarme per l'intera comunità internazionale, compiuti da persone fisiche di età non inferiore ai 18 anni al momento della commissione del fatto. La competenza della Corte è limitata ai soli crimini commessi dopo l'entrata in vigore dello Statuto sul piano internazionale, cioè dopo il 1° luglio 2022; oppure dopo l'entrata in vigore dello Statuto per lo Stato che vi ha aderito successivamente, salva la possibilità per quest'ultimo di accettare, mediante dichiarazione *ad hoc*, la piena competenza della Corte anche per i crimini commessi anteriormente all'adesione. Sulla composizione ed il funzionamento della Corte, in particolare, vedi tra gli altri: W. Schabas, *An Introduction to the International Criminal Court*, Cambridge, 2001; A. Cassese, P. Gaeta (eds.) *The Rome Statute of the International Criminal Court: A Commentary*, *Vols. 1-2*, Oxford, 2002; B. Broomhall, *International Justice and the International Criminal Court: Between Sovereignty and the Rule of Law*, Oxford, 2003; J. Jones, S. Powles, *International Criminal Practice*, Oxford, 2003; R. Cryer, *Prosecuting International Crimes: Selectivity and the International Criminal Law Regime*, Cambridge, 2005; C. Kress (ed.), *The Rome Statute and Domestic Legal Orders*, *Vols. 1-2*, Baden-Baden, 2005; W. Schabas, *The International Criminal Court: A Commentary on the Rome Statute*, Oxford, 2010; C. Stahn, *The Law and Practice of the International Criminal Court*, Oxford, 2015; O. Triffterer, *The Rome Statute of the International Criminal Court: A Commentary*, Oxford, 2015; C. Stahn, *A Critical Introduction to*

Occorre, dunque, stabilire se la competenza territoriale della Corte si estenda anche alla dimensione del ciberspazio, essendo detta dimensione uno spazio meramente virtuale, privo di confini fisici ben definiti o geograficamente determinabili[674].

A norma dell'art. 12, par. 2, lett. *a*), dello Statuto di Roma, la Corte penale internazionale è competente *ratione loci* per i crimini commessi (in tutto o in parte) sul territorio di uno Stato parte.

Nel corso di un conflitto armato internazionale, ad esempio, un attacco telematico potrebbe essere sferrato dallo Stato A (il quale supponiamo non essere parte dello Statuto di Roma) e provocare la distruzione del sistema informatico di un impianto chimico situato nel territorio dello Stato B (il quale supponiamo, invece, essere parte dello Statuto), determinando la diffusione di agenti chimici tra la popolazione locale[675]. In simili casi, la Corte è certamente competente a giudicare il crimine, dal momento lo stesso si realizza sul territorio di uno Stato parte[676].

Ai sensi dell'art. 12, par. 2, lett. *b*), dello Statuto, la Corte è, inoltre, competente ogniqualvolta l'autore del crimine è cittadino di uno Stato parte.

Prendiamo lo stesso esempio invertendo, questa volta, l'ordine degli Stati: durante un conflitto armato internazionale un attacco telematico lanciato da un cittadino dello Stato B (aderente allo Statuto di Roma) produce la distruzione del sistema informatico di un impianto chimico situato nel territorio dello Stato A (il quale non ha, viceversa, aderito allo Statuto), provocando la diffusione di agenti chimici tra la popolazione civile di quest'ultimo e la perdita di un consistente numero di vite

---

International Criminal Law, Cambridge, 2018; D. Tladi, *International Criminal Court*, in *MPEPIL*, 2020.

[674] Per un'analisi più ampia del concetto multidimensionale di *cyberspace*, si rimanda a: A Segura-Serrano, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, pp. 191-272; J. Goldsmith, T. Wu, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford, 2006; J. C. Woltag, *Internet*, in *MPEPIL*, 2010; G. M. Ruotolo, *Internet (diritto internazionale)*, in *Enciclopedia del diritto*, *Annali VII*, Milano, 2014, pp. 545-567.; N. Tsagourias, *The Legal Status of Cyberspace*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., pp. 13-30; U. Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity*, Cambridge, 2017.

[675] A. L. Chaumette, *La responsabilité pénale internationale des individus en cas de cyberattaque*, in M. Grange, A. T. Norodom (sous la direction de), *Cyberattaques et droit international. Problèmes choisis*, cit., pp. 124-126.

[676] *Ibidem*.

umane[677]. Anche in un siffatto ipotetico scenario, la Corte avrebbe certamente titolo di giurisdizione, poiché l'autore del comportamento illecito possiede la nazionalità di uno Stato parte[678].

Dagli esempi appena descritti non ci sembra – al contrario di quanto da taluni autori sostenuto[679] – che la competenza territoriale della Corte non si possa estendere anche allo spazio cibernetico.

In conclusione, come affermato altresì da Vagias[680], il fatto che il ciberspazio sia uno spazio intangibile ed immateriale, libero da costrizioni fisiche, non significa che i crimini di guerra compiuti attraverso tale dimensione debbano restare impuniti.

Quanto sostenuto è, peraltro, confermato dall'attuale Procuratore della stessa Corte, il quale in una recente dichiarazione ha esplicitamente affermato che: "*The tools used to commit serious international crimes constantly evolve from bullets and bombs to social media, the internet, and perhaps now even artificial intelligence. As states and other actors increasingly resort to operations in cyberspace, this new and rapidly developing means of statecraft and warfare can be misused to carry out or facilitate war crimes, crimes against humanity, genocide, and even the aggression of one state against another. Cyber-enabled crimes may fall within the ICC's jurisdiction if the requirements of the Rome Statute are met, and my Office may investigate or prosecute such conduct*"[681].

---

[677] A. L. Chaumette, *International Criminal Responsibility of Individuals in Case of Cyber Attacks*, in *International Criminal Law Review*, 2018, pp. 22-23.
[678] *Ibidem*.
[679] J. Trahan, *The Criminalization of Cyber-Operations under the Rome Statute*, in *Journal of International Criminal Justice*, 2021, pp. 1148-1150.
[680] M. Vagias, *The Territorial Jurisdiction of the ICC for Core Crimes Committed Through the Internet*, in *Journal of Conflict and Security Law*, 2016, p. 523 ss.
[681] La dichiarazione rilasciata dal Procuratore il 22 gennaio 2024 è rinvenibile al seguente indirizzo: https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-conference-addressing-cyber-enabled-crimes-through.

10. Armi cibernetiche, controllo degli armamenti e disarmo internazionale

Dalla disamina che precede si evince come il progresso tecnologico in corso abbia consentito l'emergere di nuovi mezzi e metodi di combattimento, i quali sollevano complesse problematiche sia sul piano dello *ius ad bellum*, che su quello dello *ius in bello*. Si pensi, in aggiunta alle armi cibernetiche oggetto della nostra analisi, ai droni[682], alle armi autonome[683], a quelle semiautonome[684], a quelle altamente automatizzate[685], nonché, infine, alle nanotecnologie[686], a cui gli Stati fanno sempre più spesso ricorso durante i conflitti armati contemporanei[687].

Le armi sono da tempo oggetto di disciplina sul piano dell'ordinamento giuridico internazionale, sia per quanto riguarda il loro impiego, che per quanto concerne la loro proibizione[688]. La comunità internazionale tuttora sperimenta divere modalità

---

[682] R. Mignot-Mahdavi, *Drones and International Law: A Techno-Legal Machinery*, Cambridge, 2023.

[683] M. Wagner, *Autonomous Weapon Systems*, in *MPEPIL*, 2016.

[684] Per una distinzione tra i suelencati tipi di armi, in particolare con riferimento alle loro caratteristiche tecniche, vedi: J. F. Caron, *Defining semi-autonomous, automated and autonomous weapon systems in order to understand their ethical challenges*, in *Digital War*, 2020, pp. 173–177.

[685] Relativamente alle differenti modalità di funzionamento delle suindicate tipologie di armi, vedi: https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on laws-in-the-ccw/.

[686] K. Leins, *New War Technologies and International Law: The Legal Limits to Weaponizing Nanomaterials*, Cambridge, 2022.

[687] C. Chinkin, M. Kaldor, *International Law and New Wars*, Cambridge, 2017, pp. 285-333.

[688] La letteratura scientifica in tema di disarmo è pressocché sterminata. Per quanto concerne i profili strettamente inerenti al diritto internazionale, si vedano, su tutti, M. Politi, *Diritto Internazionale e Non Proliferazione Nucleare*, Padova, 1984; M. Bothe, N. Ronzitti, A. Rosas (eds.), *The New Chemical Weapons Convention - Implementation and Prospects*, The Hague, 1998; L. Boisson de Chazournes, P. Sands (eds.), *International Law, the International Court of Justice and Nuclear Weapons*, Cambridge, 1999; G. Den Dekker, *The Law of Arms Control: International Supervision and Enforcement*, Dordrecht, 2001; E. Myjer, *Issues of Arms Control Law and the Chemical Weapons Convention*, Dordrecht, 2001; A. Di Lieto, *Attività nucleari e diritto internazionale*, Napoli, 2005; D. Joyner, *International Law and the Proliferation of Weapons of Mass Destruction*, Oxford, 2009; S. Marchisio (a cura di), *La crisi del disarmo nel diritto internazionale*, Napoli, 2009; N. A. Sims, *The Future of Biological Disarmament: Strengthening the Treaty Ban on Weapons*, London, 2009; D. Joyner, *Interpreting the Nuclear Non-proliferation Treaty*, Oxford, 2011; D. Joyner, M. Roscini (eds.), *Non-proliferation Law as a Special Regime: A Contribution to Fragmentation Theory in International Law*, Cambridge, 2012; D. Fry, *Legal Resolution of Nuclear Non-Proliferation Disputes*, Cambridge, 2013; J. Branch, D. Fleck (eds.), *Nuclear Non-proliferation in International Law*, The Hague, 2014; W. Krutzsch, R. Trapp (eds.), *The Chemical Weapons Convention. A Commentary*, Oxford, 2014; G. Nystuen, A. G. Bersagel (eds.), *Nuclear Weapons under International Law*, Cambridge, 2014; I. Caracciolo, M. Pedrazzi, T. Vassalli (eds.), *Nuclear Weapons: Strengthening the International Legal Regime*, The Hague, 2016; S. Casey-Maslen, *A Guide to International Disarmament Law*, London, 2019; S. Casey-Maslen, *Arms Control and Disarmament Law*, Oxford, 2021.

di regolamentazione delle stesse, vietandone solo l'uso ma non il possesso[689], oppure, al contrario, tanto l'impiego, quanto la detenzione[690]. Gli strumenti giuridici adottati consistono prevalentemente in dichiarazioni di principi e trattati internazionali, taluni dei quali contengono disposizioni oggi appartenenti, in tutto o in parte, al diritto consuetudinario[691].

Ci si è chiesti, in dottrina, se anche gli strumenti informatici sviluppati per scopi principalmente militari – al pari di determinate tipologie di armi, quali quelle biologiche o chimiche[692] – possano essere disciplinati dalle regole in materia di controllo degli armamenti[693].

A parere di diversi autori[694], preliminare a qualunque regolamentazione dovrebbe essere la definizione di arma informatica, tema su cui manca un *consensus*, anche perché molti Stati sostengono che non esistono vere e proprie armi di questo genere. Secondo la Federazione Russa, per esempio, vi sarebbero notevoli difficoltà per trattare il tema, tra cui la distinzione fra tecnologie informatiche ad uso militare e tecnologie informatiche ad uso civile[695]. La definizione di armi informatiche è indubbiamente un elemento indispensabile per poter procedere ad una loro

[689] A. Cannone, *Armi vietate, diritto internazionale dei conflitti armati e crimini di guerra*, Bari, 2013; A. Cannone, *The Use of Prohibited Weapons and War Crimes*, in F. Pocar, M. Pedrazzi, M. Frulli (eds.), *War Crimes and the Conduct of Hostilities. Challenges to Adjudication and Investigation*, cit., p. 173 ss.

[690] Tra le armi di cui è proibita tanto la produzione, quanto l'utilizzo troviamo, per esempio, quelle batteriologiche. Tali armi sono oggetto di disciplina sia da parte del Protocollo di Ginevra del 1925, che ne proibisce l'impiego in situazioni di conflitto armato, sia da parte della Convenzione di Londra del 1972 (BWC), che ne vieta la fabbricazione, la messa a punto e la conservazione.

[691] È il caso, ad esempio, delle norme contenute nel Trattato di non proliferazione delle armi nucleari (NPT), concluso a Londra il 1° luglio 1968. Ai sensi del Trattato possono detenere armi nucleari solamente gli Stati che sono membri permanenti del Consiglio di Sicurezza delle Nazioni Unite ed è consentito l'utilizzo dell'energia nucleare a fini pacifici.

[692] Le armi chimiche sono disciplinate dalla Convenzione di Parigi del 1993 (CWC), che ne proibisce lo sviluppo, la produzione, lo stoccaggio e l'impiego e disciplina la loro distruzione.

[693] M. E. O'Connell, *21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and Wmds*, in *Washington University Global Studies Law Review*, 2014, pp. 523-526.

[694] P. Roguski, *An Inspection Regime for Cyber Weapons: A Challenge Too Far?*, in *American Journal of International Law*, 2021, p. 112.

[695] La posizione della Russia in tema di armi autonome ed armi cibernetiche è rinvenibile al seguente indirizzo: https://documents.unoda.org/wp-content/uploads/2020/09/Ru-Commentaries-on-GGE-on LAWS-guiding-principles1.pdf.

regolamentazione, quantunque non manchino trattati internazionali, come quello di non proliferazione nucleare (TNP), che non definiscono l'arma che disciplinano[696]. Secondo altri autori, invece, la sottoposizione delle armi informatiche a meccanismi internazionali di controllo sarebbe alquanto difficile da attuare, a causa della natura intangibile del mezzo telematico e delle peculiari modalità di funzionamento dello stesso[697]. A ben guardare, in effetti, le differenze esistenti tra le armi informatiche e quelle convenzionali sono numerose[698]. Come osservato in precedenza, in termini di modalità tecniche, gli attacchi telematici possono essere sferrati a bassissimo costo, da un numero pressoché illimitato di utenti la cui identità risulta assai difficile da individuare[699]. Detti attacchi possono, poi, essere effettuati da località remote, in preparazione oppure in concomitanza di un attacco armato convenzionale[700]. Inoltre, rispetto alle armi convenzionali, quelle informatiche, una volta attivate, possono distruggere ogni prova della loro preesistenza[701].

Diversamente, alcuni autori hanno sostenuto che il possesso di armi cibernetiche assolverebbe una funzione essenziale di deterrenza[702]. Questa impostazione non può, tuttavia, considerarsi corretta, in quanto si basa sul parallelismo – a ben vedere privo di fondamento – tra la deterrenza nucleare e quella nel campo cibernetico[703]. Le armi nucleari, a differenza di quelle cibernetiche, non sono – fortunatamente – accessibili agli individui e, come noto, non tutti gli Stati dispongono di esse[704].

Un'ulteriore questione sollevata dalla stipulazione di accordi di non proliferazione in materia di tecnologie informatiche ad uso militare riguarda la loro

---

[696] L. Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, in K. Ziolkowski, *et al.* (eds.), *4th International Conference on Cyber Conflict, Cycon 2012 – Proceedings*, NATO CCD COE Publications, Tallinn, 2012, p. 97.
[697] J. C. Woltag, *Cyber Warfare*, in *MPEPIL*, 2015.
[698] M. E. O'Connell, *21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and Wmds*, cit., pp. 523-526.
[699] L. May, *The Nature of War and the Idea of "Cyberwar"*, in J. D. Ohlin (ed.), *Law and Ethics for Virtual Conflicts*, Oxford, 2015, p. 8.
[700] *Ibidem*.
[701] N. C. Rowe, *Distinctive Ethical Challenges of Cyberweapons*, cit., pp. 310-311.
[702] H. Lin, *Cyber Conflict and International Humanitarian Law*, cit., pp. 522-523.
[703] E. Myjer, *Some Thoughts on Cyber Deterrence and Public International Law*, in N. Tsagourias, R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, cit., pp. 299-303.
[704] *Ibidem*.

verificabilità[705]. È difficile, infatti, immaginare come l'esecuzione degli obblighi imposti da siffatti accordi possa, in concreto, essere verificata tramite, per esempio, osservazione satellitare o ispezioni *in loco*[706].

Infine, secondo un ultimo orientamento[707], per le armi cibernetiche sarebbe piuttosto difficile avvalersi di efficaci sistemi di supervisione, dal momento che il codice sorgente del *software* malevolo potrebbe, in breve tempo, essere copiato e diffuso in un numero indefinito di dispositivi elettronici (sia civili che militari).

A nostro giudizio, quanto più gli attacchi informatici saranno oggetto di dibattito nel prossimo futuro, tanto più è probabile che anche le c.d. *cyber weapons* diventino oggetto di specifici regimi internazionali di supervisione che ne vietino – senza confliggere, beninteso, con la ricerca tecnologica svolta per fini civili – il trasferimento in particolari circostanze.

Non trattandosi di armi convenzionali, invero, le armi cibernetiche non rientrano nell'ambito di applicazione del Trattato sul commercio delle armi convenzionali (*Arms Trade Treaty ATT*), adottato nell'aprile 2013 dall'Assemblea generale delle Nazioni Unite, sotto la spinta di numerose ONG, ed entrato in vigore dal dicembre 2014 per 66 Stati, compresa l'Italia[708]. Il Trattato, a norma dell'art. 6, proibisce il commercio di armi convenzionali allorquando tale commercio: a) sia contrario agli obblighi scaturenti da misure adottate dal Consiglio di sicurezza delle Nazioni Unite in virtù del Capitolo VII della Carta; b) sia suscettibile di violare obblighi derivanti dai trattati internazionali di cui lo Stato contraente è parte; c) lo Stato contraente sia a conoscenza che le armi trasferite possano concretamente essere impiegate per commettere crimini internazionali e infrazioni gravi delle quattro Convenzioni di Ginevra del 1949 o, comunque, altri crimini internazionali previsti dai Trattati di cui lo stesso è parte[709].

---

[705] N. Tsagourias, G. Biggio, *The Regulation of Cyber Weapons*, in E. Myjer, T. Marauhn (eds.), *Research Handbook on International Arms Control Law*, Cheltenham, 2022, pp. 440-455.
[706] *Ibidem*.
[707] L. Arimastu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, cit., p. 108.
[708] In Italia il Trattato, attualmente vincolante 116 Stati, è stato autorizzato e reso esecutivo con l. 4 ottobre 2013 n. 118.
[709] Il testo del Trattato è consultabile – in lingua inglese ed in lingua francese – al seguente indirizzo: https://disarmament.unoda.org/ATT/docs/ATT_text_(As_adopted_by_the_GA)-E.pdf.

Sistemi di monitoraggio inerenti alle tecnologie informatiche, del resto, sono già stati previsti, in passato, per alcuni importanti *hardware* e *software dual use*[710]. Sebbene non abbia valore giuridico vincolante, si pensi, a titolo di esempio, all'Accordo multilaterale di Wassenaar, concluso all'Aia nel luglio 1996 ed entrato in vigore nel settembre 1996, il cui obiettivo essenziale risulta quello di contribuire al mantenimento della pace e della sicurezza internazionale promuovendo una maggiore trasparenza tra gli Stati membri per quanto concerne l'accumulazione di armi convenzionali e beni a duplice uso[711].

Ai sensi dell'accordo in parola, gli Stati partecipanti sono invitati, attraverso le loro politiche nazionali, a garantire che i trasferimenti di armi e tecnologie a duplice uso non contribuiscano allo sviluppo ed al rafforzamento delle capacità militari di uno Stato il cui comportamento metta a rischio la pace e la sicurezza internazionale[712]. Esso proibisce, per esempio, la vendita dei c.d. «*intrusion software*», come tali intendendosi programmi informatici appositamente creati allo scopo di eseguire la raccolta di dati presenti in un determinato dispositivo di rete, eludendo le misure di protezione in esso presenti[713].

Si potrebbe, allora, sostenere che tale accordo, stipulato da 33 Stati[714], fra cui l'Italia, possa fungere da modello per un futuro regime di verifica riguardante le tecnologie informatiche costruite per finalità esclusivamente militari, il quale dovrebbe però necessariamente coinvolgere un numero ben maggiore di Paesi e, soprattutto, essere dotato di carattere giuridico vincolante.

Incentivare le misure di sicurezza informatica, specialmente con riferimento alle infrastrutture fondamentali dello Stato, solo attraverso un maggiore coordinamento con il settore privato, come da una parte della dottrina suggerito[715], potrebbe ridurre,

---

[710] Per quanto concerne l'oggetto e lo scopo dell'accordo che, si badi, è privo di efficacia giuridica vincolante, vedi altresì: https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf).

[711] *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*, 19 December 1995. Il testo dell'accordo è gratuitamente consultabile al seguente link: https://www.wassenaar.org/.

[712] https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf.

[713] *Wassenaar Arrangement*, *List of Dual-Use Goods and Technologies and Munitions List*, in specie, Cat. 4, pp. 78-84.

[714] Gli Stati che hanno ratificato l'Arrangement sono attualmente 47.

[715] P. Roguski, *An Inspection Regime for Cyber Weapons: A Challenge Too Far?*, cit., p. 115.

ma non di certo eliminare del tutto il rischio per gli Stati di subire attacchi telematici.

In conclusione, sebbene un regime di monitoraggio delle armi informatiche non rappresenti la soluzione a tutte le questioni poste dalla c.d. guerra cibernetica, esso potrebbe certamente aiutare a prevenire e risolvere molte delle problematiche sin qui esposte. Un adeguato meccanismo di classificazione delle suddette armi, ad esempio, in base alla gravità del danno da queste prodotto, appare di ben maggiore utilità rispetto ad un generico trattato sul ciberspazio, da più parti auspicato[716], ma difficilmente realizzabile a causa delle attuali condizioni geopolitiche. Tale sistema di verifica dovrebbe essere periodicamente aggiornato, al fine di evitare che la rapidità con cui si svolge il progresso tecnologico in atto possa rendere, di fatto, inefficace qualsiasi tentativo di individuazione e sistematizzazione delle armi informatiche di cui si intende regolamentare o proibire l'utilizzo.

[716] A. P. Johnson, *Is It Time for a Treaty on Information Warfare?*, cit., 2002, p. 439 ss.

CONCLUSIONI

L'utilizzo dello spazio cibernetico per finalità militari è oramai una possibilità reale. La crescente militarizzazione di tale dimensione si riflette nell'incorporazione delle operazioni telematiche nelle dottrine militari e nella creazione di unità specializzate in operazioni cibernetiche difensive e offensive all'interno delle forze armate.

Da tempo la dottrina internazionalistica si domanda quando un attacco informatico possa costituire in concreto: a) una violazione della minaccia o dell'uso della forza armata; b) un «attacco armato» che permette allo Stato vittima di invocare il diritto alla legittima difesa, individuale ed eventualmente collettiva; c) una «minaccia alla pace», una «violazione della pace» o, addirittura, un «atto di aggressione» ai sensi dell'art. 39 della Carta delle Nazioni Unite consentendo, pertanto, al Consiglio di sicurezza di adottare le misure contemplate dal capitolo VII.

Al fine di fornire una risposta alle elencate questioni giuridiche il presente studio ha presupposto, in via preliminare, che un attacco cibernetico possa essere attribuito ad uno Stato secondo le norme sulla responsabilità internazionale. Il fatto che in nessun caso sinora sia stata dimostrata con sufficiente certezza la responsabilità di uno Stato per un attacco informatico e, tanto meno, che uno Stato abbia riconosciuto la propria responsabilità per un'attività cibernetica illecita, non vuol dire che la tecnologia informatica renda necessariamente difficile identificare l'autore originario di un attacco telematico. La tesi avanzata da taluni autori secondo cui sarebbe praticamente impossibile individuare il computer e la persona che ha effettuato un simile attacco e provare che nella sua condotta sia coinvolto, direttamente o indirettamente, un certo Stato deve essere respinta. Tale impostazione appare infondata poiché è tecnicamente fattibile non soltanto risalire all'esecutore materiale di un attacco cibernetico e alla sua collocazione geografica, ma delle volte anche alla entità governativa che lo ha commissionato. Peraltro, la suesposta tesi – qualora accettata – lascerebbe piena libertà agli Stati (specialmente

alle grandi Potenze) di lanciare attacchi informatici sia in tempo di pace, sia soprattutto in fase di conflitto armato restando, di fatto, impuniti.

Assumendo, dunque, che un attacco telematico possa determinare il sorgere della responsabilità di uno Stato, il presente lavoro è giunto alla conclusione che un attacco di questo genere possa, in astratto, configurare un uso della forza armata laddove suscettibile di provocare danni materiali a persone o oggetti comparabili a quelli prodotti da un mezzo di guerra convenzionale. Sebbene non rientri nella nozione classica di "arma", un attacco cibernetico che ha conseguenze distruttive paragonabili a quelle di un attacco convenzionale potrebbe, quindi, rappresentare, una violazione dell'art. 2, par. 4, della Carta delle Nazioni Unite. Del resto, come ha dichiarato la Corte internazionale di giustizia nel parere sulla legittimità della minaccia o dell'utilizzo di armi nucleari, reso nel 1966, le norme in materia di *ius ad bellum* «*do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed*».

Data la vaghezza e l'elasticità che caratterizzano la nozione di «minaccia alla pace» e tenuto conto dell'ampia discrezionalità di cui gode il Consiglio di sicurezza nell'accertamento di tale condizione, non vi è motivo di escludere che un attacco telematico possa essere eccezionalmente qualificato come una «minaccia alla pace» legittimando, così, il Consiglio a disporre, in particolare, misure sanzionatorie nei confronti degli individui o delle entità statali responsabili dell'operazione.

Tuttavia, ancorché possa ricadere sotto la proibizione di cui all'art. 2, par. 4, della Carta delle Nazioni Unite, deve ritenersi abbastanza improbabile che un attacco telematico possa costituire un vero e proprio «attacco armato» che giustifichi l'esercizio del diritto alla legittima difesa, cinetica o cibernetica. Come sottolineato dalla Corte internazionale di giustizia nella decisione relativa all'affare *Nicaragua contro Stati Uniti* del 1986, sono la portata e gli effetti di una operazione militare che determinano la soglia necessaria per il verificarsi di un «attacco armato» di cui all'art. 51 della Carta delle Nazioni Unite. A ben guardare, allo stato attuale, nessun attacco informatico sembrerebbe aver raggiunto, per dimensioni e gravità, la soglia in parola.

Poiché un attacco informatico non configurerebbe un «attacco armato», le reazioni da parte dello Stato vittima sono allora possibili solo sotto forma di contromisure, convenzionali o cibernetiche.

Anche a volere ammettere che un attacco informatico possa potenzialmente ammontare ad un «attacco armato» *ex* art. 51 della Carta delle Nazioni Unite, come prudentemente suggerito da ambedue le edizioni del Manuale di Tallinn sul diritto internazionale applicabile alla guerra cibernetica, i requisiti della necessità, della proporzionalità e dell'immediatezza, a cui la legittima difesa è soggetta nelle sue modalità di svolgimento, risultano difficilmente adattabili al contesto cibernetico. Come rilevato nella parte introduttiva, l'istituzione di *Computer emergency response team* (CERT) in seno alla maggior parte degli Stati – quali il *Centre for Cyber Security of Belgium*, il *Danish Computer Security Incident Response Team*, il *National Cyber Security Centre of Finland* e l'Agenzia italiana per la cybersicurezza nazionale – e la conseguente possibilità di respingere un attacco telematico principalmente attraverso misure di sicurezza informatica attiva e passiva potrebbero rendere un'eventuale risposta armata a titolo di legittima difesa non necessaria.

Ad ogni modo, come la presente indagine si propone di evidenziare, il problema di stabilire se un attacco cibernetico possa di per sé comportare l'applicazione delle norme di *ius ad bellum* è spesso sopravvalutato dalla dottrina e ha, al momento, un rilievo puramente teorico.

In primo luogo, oggi, gli attacchi informatici sono effettuati prevalentemente da individui e potrebbero costituire, di conseguenza, solamente un reato informatico rientrante tutt'al più nell'ambito di applicazione delle pertinenti leggi nazionali in tema di criminalità informatica.

In secondo luogo, la gran parte delle operazioni cibernetiche condotte dagli Stati, attualmente, ha come obiettivo la raccolta e sottrazione di informazioni segrete a distanza, oppure la creazione e diffusione di false informazioni (c.d. *fake news*) dirette a distorcere la realtà per manipolare ed influenzare l'opinione pubblica. Tali operazioni non rappresentano un uso della forza armata e, conseguentemente, non

ricadono nell'ambito di applicazione delle norme internazionali in materia di *ius ad bellum*.

Infine, come emerge dal conflitto armato tra Russia e Ucraina, gli attacchi telematici normalmente sono sferrati in preparazione oppure in concomitanza di un attacco convenzionale durante un conflitto armato preesistente. In mancanza di una prassi degli Stati, risulta piuttosto difficile immaginare una situazione in cui un attacco informatico possa di per sé dare luogo ad un conflitto armato. Lo scenario di un conflitto bellico condotto esclusivamente con strumenti informatici sembrerebbe, dunque, un'ipotesi del tutto remota.

La peculiarità della ricerca svolta consiste nell'avere esaminato le problematiche che si riscontrano nell'applicazione delle norme di diritto internazionale umanitario agli attacchi cibernetici soltanto con riferimento a scontri armati già in svolgimento. In altri termini, ritenendo che solo una significativa prassi degli Stati potrà stabilire in futuro se una operazione telematica sia in grado di fare scattare l'applicazione del diritto internazionale umanitario, ci si è chiesti in che modo tale articolato *corpus* normativo possa disciplinare le operazioni informatiche effettuate in un conflitto bellico innescato da un uso della forza armata tradizionale (c.d. cinetica).

Come sottolineato nel primo capitolo, gli attacchi telematici lanciati in presenza di concomitanti operazioni militari cinetiche, che abbiano un nesso con il conflitto, per poter essere disciplinati dalle regole umanitarie devono rientrare nella nozione di «attacco» dettata da tali norme. Devono considerarsi alla stregua di «attacchi» ai sensi del I Protocollo del 1977 le operazioni informatiche che causano la perdita di vite umane, lesioni a persone oppure danni materiali a beni e infrastrutture. Inoltre, devono essere qualificate come «attacco» a norma del I Protocollo addizionale, quelle operazioni telematiche che si limitano ad interrompere la funzionalità delle infrastrutture critiche bersagliate senza però danneggiarle fisicamente, laddove beninteso l'interruzione del funzionamento non sia limitata o breve e abbia gravi conseguenze per la popolazione civile coinvolta nel conflitto.

In favore dell'applicabilità del diritto internazionale umanitario alle suindicate operazioni informatiche si è osservato, facendo leva sulla Dichiarazione di San Pietroburgo del 1868 e sulla clausola Martens, che la mancata regolamentazione di

una determinata condotta bellica non significa che essa sia ammessa senza alcuna restrizione. Come affermato dalla Corte internazionale di giustizia nel citato parere consultivo sulla legalità delle armi nucleari il diritto umanitario si applica a «*to all forms of warfare and to all kind of weapons, those of the past, those of the present and those of the future*».

Nel secondo capitolo si è allora proceduto ad una sistematizzazione, ricostruzione e interpretazione evolutiva delle principali regole del diritto umanitario, arrivando a dimostrare che, nonostante il loro sviluppo sia avvenuto in un periodo storico in cui pensare al cyberspazio come teatro bellico risultava avveniristico, esse sono sufficientemente flessibili da adempiere adeguatamente al loro obiettivo di disciplinare la condotta delle ostilità e proteggere le popolazioni civili vittime della violenza bellica anche con riguardo alle operazioni militari di natura informatica. Sotto questo punto di vista i principi basilari del diritto umanitario mantengono tutta la loro validità ed utilità.

Escludere che un attacco cibernetico possa dare luogo ad un conflitto armato e, allo stesso tempo, riconoscere la perfetta applicabilità delle norme dello *ius in bello* agli attacchi informatici effettuati nel corso di ostilità tradizionali ha il duplice pregio di evitare il sorgere di nuovi conflitti e, comunque, tutelare le popolazioni civili dai molteplici rischi derivanti dall'impiego delle emergenti tecnologie militari.

In conclusione, se appare probabile che gli attacchi informatici aumenteranno nel prossimo futuro, è presumibile che tali attacchi supporteranno ma non sostituiranno i mezzi e metodi di combattimento tradizionali. In merito al loro regime giuridico, alcuni autori hanno sostenuto la necessità di concludere un trattato in materia di sicurezza informatica. Tuttavia, alla luce delle crescenti tensioni geopolitiche, le possibilità di adozione di un siffatto trattato restano alquanto scarse. Peraltro, un trattato che regoli le operazioni cibernetiche non pare necessario poiché, come si è detto, le norme internazionali vigenti sono sufficienti.

Maggiormente utile potrebbe essere forse, come si è auspicato nel terzo capitolo, l'introduzione di un regime internazionale di controllo delle tecnologie informatiche destinate ad un uso militare, che supervisioni, attraverso la loro individuazione e classificazione, i virus informatici progettati specificamente per

recare un danno materiale ad un altro Stato e proibisca l'utilizzo di quei programmi e codici malevoli che, a causa delle loro caratteristiche tecniche e dell'interconnettività delle reti informatiche, potrebbero diffondersi in maniera incontrollabile e indiscriminata dal sistema informatico di destinazione ad un numero indefinito di apparecchiature e dispositivi elettronici civili in violazione del principio di distinzione. Tale sistema dovrebbe promuovere una maggiore trasparenza tra gli Stati partecipanti per quanto concerne la produzione e l'immagazzinamento di beni a duplice uso e tecnologie informatiche destinate unicamente a scopi militari e, ancora, vietare la vendita dei predetti beni e delle suddette tecnologie qualora il loro trasferimento metta a rischio il mantenimento della pace e della sicurezza internazionale. Esso, inoltre, come già è stato previsto per le armi convenzionali, dovrebbe impedire il commercio di tecnologie e beni *dual use* quando il loro trasferimento: a) sia contrario agli obblighi derivanti da misure adottate dal Consiglio di sicurezza delle Nazioni Unite in base al capitolo VII della Carta; b) sia suscettibile di violare obblighi derivanti dalle norme consuetudinarie e pattizie sulla salvaguardia dei diritti dell'uomo; c) lo Stato parte contraente sia a conoscenza che le tecnologie trasferite possano essere impiegate per commettere crimini internazionali.

Tale regime internazionale di controllo potrebbe efficacemente risolvere molte delle complesse questioni sollevate dal massiccio ricorso alle nuove tecnologie da parte degli Stati nei conflitti armati, a condizione che sia dotato di carattere giuridico vincolante e coinvolga un alto numero di Stati. Non si tratterebbe solo di una convenzione in materia di disarmo e non proliferazione, bensì di un trattato volto a prevenire gravi violazioni del diritto umanitario e dei diritti umani, i quali, come è noto, si applicano anche in tempo di guerra.

BIBLIOGRAFIA ESSENZIALE

Akande D., *Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities*, in *International and Comparative Law Quarterly*, 2010, pp. 180-192.

Alcala R., *Cultural Evolution: Protecting "Digital Cultural Property" in Armed Conflict*, in *IRRC*, 2022, pp. 1083–1119.

Aldrich R. W., *How Do You Know You Are at War in the Information Age?*, in *Houston Journal of International Law*, 2000, pp. 99-110.

Almutawa A., *Designing the Organisational Structure of the UN Cyber Peacekeeping Team*, in *Journal of Conflict and Security Law*, 2020, pp. 117-147.

Ambos K., *International Criminal Responsibility in Cyberspace*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 118-143.

Annoni A., *L'occupazione ostile nel diritto internazionale contemporaneo*, Torino, 2012, pp. 186-218.

Antonopoulos C., *Non-Participation in Armed Conflict: Continuity and Modern Challenges to the Law of Neutrality*, Cambridge, 2022, pp. 201-220.

Antonopoulos C., *State Responsibility in Cyberspace*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 55-71.

Arcari M., *Uso della Forza*, in *Diritto on line Treccani Enciclopedia Italiana*, 2014.

Arimastu L., *Classifying Cyber Warfare*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 326-342.

Arimatsu L., *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, in Ziolkowski K. (eds.), *4th International Conference on Cyber Conflict, Cycon 2012 – Proceedings*, NATO CCD COE Publications, Tallinn, 2012, pp. 91-109.

Arkin W. M., *Cyber Warfare and the Environment*, in *Vermont Law Review*, 2001, pp. 779-792.

Asaro P., *On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making*, in *IRRC*, 2012, pp. 687-709.

Baade B., *Fake News and International Law*, in *European Journal of International Law*, 2018, pp. 1357-1376.

Backstrom A., Henderson I., *New Capabilities in Warfare: An Overview of Contemporary Technological Developments and the Associated Legal and Engineering Issues in Article 36 Weapons Reviews*, in *IRRC*, 2012, pp. 483-514.

Balladore Pallieri G., *Il diritto bellico*, Padova, 1954.

Banaszewska D. M., *Hors de combat*, in *MPEPIL*, 2015.

Banellier K., *Is the Principle of Distinction Still Relevant in Cyberwarfare?*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 343-365.

Beard J. M., *Law and War in the Virtual Era*, in *American Journal of International Law*, 2009, pp. 409-445.

Beckett J., *New War, Old Law: Can the Geneva Paradigm Comprehend Computers?*, in *Leiden Journal of International Law*, 2000, pp. 33-51.

Bell C., Pfeiffer J., *Indiscriminate Attack*, in *MPEPIL*, 2011.

Benatar M., *The Use of Cyber Force: Need for Legal Justification?*, in *Göttingen Journal of International Law*, 2009, pp. 375-396.

Benvenisti E., *Occupation, Belligerent*, in *MPEPIL*, 2009.

Bernstorff von J., *Martens Clause*, in *MPEPIL*, 2009.

Bianchi A., *Human Rights and the Magic of Jus Cogens*, in *European Journal of International Law*, 2008, pp. 491-508.

Blay S. K. N., *Territorial Integrity and Political Independence*, in *MPEPIL*, 2010.

Blount P., *The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons*, in *Northern Kentucky Law Review*, 2012, pp. 211-20.

Boer L., *International Law As We Know It. Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship*, Cambridge, 2021.

Boer L., *Restating the Law as It Is: On the Tallinn Manual and the Use of Force in Cyberspace*, in *Amsterdam Law Forum*, 2013, pp. 1-16.

Boogaard J., *Proportionality in International Humanitarian Law. Refocusing the Balance in Practice*, Cambridge, 2023, p. 13 ss.

Boothby W. H., *Methods and Means of Cyber Warfare*, in *International Law Studies*, 2013, pp. 387-405.

Boothby W. H., *The Law of Targeting*, Oxford, 2012, pp. 276-277.

Boothby W. H., *Weapons and the Law of Armed Conflict*, Oxford, 2009, pp. 57-62.

Bothe M., Partsch K., Solf W., *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, The Hague, Boston, London, 1982.

Bothe M., *Occupation, Belligerent*, in *EPIL*, 1997, pp. 763-773.

Bothe M., *The Law of Neutrality*, in Fleck D. (ed.), *The Handbook of International Humanitarian Law*, Oxford, 2013, pp. 571-604.

Bothe M., *War and Environment*, in *EPIL*, 2000, pp. 1342-1345.

Bowett D., *International Law and Economic Coercion*, in *Virginia Journal of International law*, 1975, pp. 245-260.

Brown D., *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, in *Harvard Journal of International Law*, 2006, pp. 179-221.

Brownlie I., *International Law and the Use of Force by States*, Oxford, 1963, pp. 361-368.

Buchan R., Tsagourias N., *Autonomous Cyber Weapons and Command Responsibility*, in *International Law Studies*, 2020, pp. 651-673.

Buchan R., *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, in *Journal of Conflict and Security Law*, 2012, pp. 212-227.

Buchan R., *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, in *Chinese Journal of International Law*, 2016, pp. 741-772.

Bufalini A., *Uso della forza, legittima difesa e problemi di attribuzione in situazioni di attacco informatico*, in Tanzi A., Lanciotti A. (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2011, pp. 405-436.

Cannizzaro E., *Il principio della proporzionalità nell'ordinamento internazionale*, Milano, 2000, p. 306.

Cannone A., *Armi vietate, diritto internazionale dei conflitti armati e crimini di guerra*, Bari, 2013.

Cannone A., *The Use of Prohibited Weapons and War Crimes*, in Pocar F., Pedrazzi M., Frulli M. (eds.), *War Crimes and the Conduct of Hostilities. Challenges to Adjudication and Investigation*, Cheltenham, 2013, pp. 173-193.

Cansacchi G., *Nozioni di diritto internazionale bellico*, Torino, 1968.

Cassese A., *International Criminal Law*, Oxford, 2008, pp. 193-200.

Cassese A., Gaeta P., *Le sfide attuali del diritto internazionale*, Bologna, 2008, pp. 78-79.

Cassese A., *The Martens Clause: Half a Loaf or Simply Pie in the Sky?*, in *European Journal of International Law*, 2000, pp. 187-216.

Castellaneta M., *Conflitti armati (diritto internazionale)*, in *Enc. dir.*, Annali V, 2012, pp. 316-370.

Castellaneta M., *La disinformazione nel conflitto in Ucraina: tra ius in bello e diritto alla libertà di espressione*, in Porchia O., Vellano M. (a cura di), *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future. Liber Amicorum in onore di Edoardo Greppi*, Torino, 2023, pp. 327-346.

Castellaneta M., *La responsabilità internazionale degli Stati per danni all'ambiente causati nel corso di conflitti armati*, in *Rivista diritto internazionale*, 1998, pp. 632-672.

Castellaneta M., *New weapons, old crimes?*, in Pocar F., Pedrazzi M., Frulli M. (eds.), *War Crimes and the Conduct of Hostilities. Challenges to Adjudication and Investigation*, Cheltenham, 2013, pp. 194-210.

Castren E., *The Present Law of War and Neutrality*, Helsinki, 1954.

Chainoglou K., *Psychological Warfare*, in *MPEPIL*, 2016.

Chaumette A. L., *International Criminal Responsibility of Individuals in Case of Cyber Attacks*, in *International Criminal Law Review*, 2018, pp. 1-35.

Chaumette A. L., *La responsabilité pénale internationale des individus en cas de cyberattaque*, in Grange M., Norodom A. (Sous la direction de), *Cyberattaques et droit international. Problèmes choisis*, Paris, 2018, pp. 107-135.

Chesney R. M., *Prisoners of War*, in *MPEPIL*, 2009.

Chinkin C., Kaldor M., *International Law and New Wars*, Cambridge, 2017, pp. 285-333.

Church W., *Information Warfare*, in *IRRC*, 2000, pp. 205-216.

Ciciriello M. C., *Spionaggio (diritto internazionale)*, in *Enciclopedia giuridica*, vol. XXX, pp. 1993-1998.

Cormack T., *International Humanitarian Law and the Targeting of Data*, in *International Law Studies*, 2018, pp. 222-240.

Conde J., *The Principle of Distinction in Virtual War: Restraints and Precautionary Measures under International Humanitarian Law*, in *Tilburg Law Review*, 2010, pp. 69-91.

Conforti B., Focarelli C., *Le Nazioni Unite*, Padova, 2017, p. 232.

Corn G. S., *Humanity, Principle of*, in *MPEPIL*, 2013.

Corten O., *Cyber-attaques et Jus Contra Bellum*, in Grange M., Norodom A. T. (Sous la direction de), *Cyberattaques et droit international. Problèmes choisis*, Paris, 2018, pp. 199-214.

Corten O., *Le droit contre la guerre*, Paris, 2007, p. 707 ss.

Crawford E., *Armed Conflict, International*, in *MPEPIL*, 2015.

Crawford E., *Identifying the Enemy Civilian Participation in Armed Conflict*, Oxford, 2015, pp. 138-150.

Crawford E., Pert A., *International Humanitarian Law*, Cambridge, 2020, pp. 106-108.

Crawford E., *Proportionality*, in *MPEPIL*, 2011.

Crawford E., *The Treatment of Combatants and Insurgents under the Law of Armed Conflict*, Oxford, 2010, pp. 48-76.

Crawford E., *Tracing the Historical and Legal Development of the Levée En Masse in the Law of Armed Conflict*, in *Journal of the History of International Law*, 2017, pp. 329-361.

Cryer R., *An Introduction to International Criminal Law and Procedure*, Cambridge, 2019, pp. 362-364.

David E., *Principes de droit des conflits armés*, Bruxelles, 2008.

Delerue F., *Cyber Operations and International Law*, Cambridge, 2020.

Delibasis D., *State Use of Force in Cyberspace for Self-Defence: A New Challenge for a New Century*, in *Peace Conflict and Development: An Interdisciplinary Journal*, 2006, pp. 1-50.

Dervan L., *Information Warfare and Civilian Populations: How the Law of War Addresses a Fear of the Unknown*, in *Göttingen Journal of International Law*, 2011, pp. 373-396.

Dev P. R., *Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, in *Texas International Law Journal*, 2015, pp. 381-401.

Dinniss H. H., *Cyber Warfare and the Laws of War*, Cambridge, 2012.

Dinniss H. H., *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, in *Israel Law Review*, 2015, pp. 39-54.

Dinstein Y., *Computer Network Attacks and Self-Defense*, in *International Law Studies*, 2002, pp. 99-121.

Dinstein Y., *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, in *International Law Studies*, 2013, pp. 257-287.

Dinstein Y., *Military Necessity*, in *MPEPIL*, 2015.

Dinstein Y., *Non-International Armed Conflicts in International Law*, Cambridge, 2014, p. 30.

Dinstein Y. (ed.), *Oslo Manual on Select Topics of the Law of Armed Conflict. Rules and Commentary*, Cham, 2020.

Dinstein Y., *Protection of the Environment in International Armed Conflict*, in *Max Planck Yearbook of United Nations Law*, 2001, pp. 523-549.

Dinstein Y., *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge, 2016.

Dinstein Y., *The Principle of Distinction and Cyber War in International Armed Conflicts*, in *Journal of Conflict and Security Law*, 2012, pp. 261-277.

Dinstein Y., *War, Aggression and Self-Defence*, Cambridge, 2017.

Dinstein Y., *Warfare, Methods and Means*, in *MPEPIL*, 2015.

Döge J., *Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime*, in *Archiv des Völkerrechts*, 2010, pp. 486-501.

Dörmann K., *Applicability of the Additional Protocols to Computer Network Attacks*, in *IRRC*, 2004, pp. 1-12.

Dörmann K., *Combatants, Unlawful*, in *MPEPIL*, 2015.

Dörmann K., *Elements of War Crimes under the Rome Statute of the International Criminal Court: Sources and Commentary*, Cambridge, 2003, pp. 161-177.

Dörr O., *Use of Force, Prohibition of*, in *MPEPIL*, 2019.

Doswald-Beck L. (ed.), *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, Cambridge, 1995.

Doswald-Beck L., *Some Thoughts on Computer Network Attack and the International Law of Armed Conflict*, in *International Law Studies*, 2002, pp. 163-185.

Doyle J., *Computer Networks, Proportionality, and Military Operations*, in *International Law Studies*, 2002, pp. 147-161.

Droege C., *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, in *IRRC*, 2012, pp. 533-578.

Ducheine P. A. L., *Military Cyber Operations*, in Fleck D., Gill T. (eds.), *The Handbook of the International Law of Military Operations*, Oxford, 2010, pp. 456-475.

Eichensehr K. E., *Ukraine, Cyberattacks, and the Lessons for International Law*, in *American Journal of International Law*, 2022, pp. 145-149.

Fallah K., *Corporate Actors: The Legal Status of Mercenaries in Armed Conflict*, in *IRRC*, 2006, pp. 599-611.

Fidler D. P., *Cyberattacks and International Human Rights Law*, in Casey-Maslen S. (ed.), *Weapons under International Human Rights Law*, Cambridge, 2014, pp. 299-333.

Fidler D. P., *Cyberspace and Human Rights*, in Tsagourias N., Buchan R. (eds), in *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 94-117.

Fischer G., *La Convention sur l'interdiction d'utiliser des techniques de modification de l'environnement à des fins hostiles*, in *Anr. fr. dr. intern*., XXIII, 1977, pp. 820-836.

Focarelli C., *Self-defence in cyberspace*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 255-283.

Fleck D., *Searching for International Rules Applicable to Cyber Warfare - A Critical First Assessment of the New Tallinn Manual*, in *Journal of Conflict and Security Law*, 2013, pp. 331-351.

Focarelli C., *Trattato di diritto internazionale*, Torino, 2015, pp. 1828-1834.

Franck T. M., *Recourse to Force State Action against Threats and Armed Attacks*, Cambridge, 2009.

Franck T. M., *Who Killed Article 2(4)? or: Changing Norms Governing the Use of Force by States*, in *American Journal of International Law*, 1970, pp. 809-837.

Gallo G., *I cavi sottomarini e il diritto internazionale: quale protezione per le cosiddette "arterie" della globalizzazione?*, in *La Comunità internazionale*, 2022, pp. 493-412.

Gargiulo P., *Nazioni Unite, cybersecurity e diritto internazionale*, in Porchia O., Vellano M. (a cura di), *Il diritto internazionale per la pace e nella guerra. Sviluppi recenti e prospettive future. Liber Amicorum in onore di Edoardo Greppi*, Torino, 2023, pp. 53-68.

Gargiulo P., *Uso della Forza (Diritto internazionale)*, in *Enciclopedia del Diritto*, Annali V, Milano, 2012, pp. 1367-1430.

Gardam J., *Necessity, Proportionality, and the Use of Force by States*, Cambridge 2004, p. 4 ss.

Garraway C., *The Use and Abuse of Military Manuals, in Yearbook of International Humanitarian Law*, 2004, pp. 425-440.

Gavouneli M., *Neutrality - A Survivor?*, in *European Journal of International Law*, 2012, pp. 267-273.

Geiss R., Lahmann H., *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, in *Israel Law Review*, 2012, pp. 381-399.

Geiss R., *Cyber Warfare: Implications for Non-international Armed Conflicts*, in *International Law Studies*, 2013, pp. 627-645.

Gervais M., *Cyber Attacks and the Laws of War*, in *Berkeley Journal of International Law*, 2012, pp. 563-564.

Gialdino C., *Occupazione bellica*, in *Enc. dir.*, Vol. XXIX, 1979, pp. 720-750.

Gill T., *Anticipatory Self-Defense in the Cyber Context*, in *International Law Studies*, 2013, pp. 438-471.

Gill T., *International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of "Armed" under the Humanitarian Law of Armed Conflict*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 366-379.

Gillard E., *Business Goes to War: Private Military Security Companies and International Humanitarian Law*, in *IRRC*, 2006, pp. 525-572.

Goldsmith J., *How Cyber Changes the Laws of War*, in *European Journal of International Law*, 2013, pp. 129-38.

Goodman R., *The Power to Kill or Capture Enemy Combatants*, in *European Journal of International Law*, 2013, pp. 819-853.

Graham D. E., *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 2010, pp. 97-102.

Gray C., *International Law and the Use of Force*, Oxford, 2000, pp. 54-57.

Green L. C., *The contemporary law of armed conflict*, Manchester, 2008, p. 145.

Greenwood C., *Scope of Application of Humanitarian Law*, in Fleck D. (ed.), *The Handbook of International Humanitarian Law in Armed Conflict*, Oxford, 2013, pp. 45-79.

Greenwood C., *Self-Defence*, in *MPEPIL*, 2011.

Greenwood C., *The Administration of Occupied Territory in International Law*, in Playfair E. (ed.), *International Law and the Administration of Occupied Territories. Two Decades of Israel Occupation of the West Bank and Gaza Strip*, Oxford, 1992, pp. 241-266.

Greenwood C., *The Relationship between ius ad bellum and ius in bello*, in *Review of International Studies*, 1983, pp. 221-234.

Greppi E., Venturini G., *Codice di diritto internazionale umanitario*, Torino, 2012.

Greppi E., *Diritto internazionale umanitario dei conflitti armati e diritti umani: profili di una convergenza*, in *La Comunità internazionale*, 1996, pp. 473-498.

Grimal F., Sundaram J., *Cyber Warfare and Autonomous Self-Defense*, in *Journal on the Use of Force and International Law*, 2017, pp. 312-343.

Grosswald L., *Cyberattack Attribution Matters under Article 51 of the United Nations Charter*, in *Berkeley Journal of International Law*, 2011, pp. 1151-1181.

Handler S. G., *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, in *Standford Journal of International Law*, 2012, pp. 209-237.

Haslam E., *Information Warfare: Technological Changes and International Law*, in *Journal of Conflict and Security Law*, 2000, pp. 157-176.

Hathaway O. A., *The Law of Cyber-Attack*, in *California Law Review*, 2012, pp. 817-886.

Hayashi H., *Military Necessity: The Art, Morality and Law of War*, Cambridge, 2020, p. 8 ss.

Heinegg W. H., *Precautions in Attack*, in *MPEPIL*, 2015.

Heinegg W. H., *Proportionality and Collateral Damage*, in *MPEPIL*, 2015.

Heinegg W. H., *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013, pp. 123-156.

Henckaerts J. M., *Armed Forces*, in *MPEPIL*, 2010.

Henckaerts J. M., Doswald-Beck L. (eds), *Customary International Humanitarian Law, Vol. 1: Rules*, Cambridge, 2005.

Henckaerts J. M., Doswald-Beck L. (eds), *Customary International Humanitarian Law, Vol. 2: Practice*, Cambridge, 2005.

Henderson I., *Emerging Technology and Perfidy in Armed Conflict*, in *International Law Studies*, 2015, pp. 468-485.

Henderson C., *The United Nations and the Regulation of Cyber-security*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 465-490.

Henderson C., *The Use of Force and International Law*, Cambridge, 2018, p. 123 ss.

Hestermeyer H. P., *Mercenaries*, in *MPEPIL*, 2010.

Hoffman M. H., *The Legal Status and Responsibilities of Private Internet Users under the Law of Armed Conflict: A Primer for the Unwary on the Shape of Law to Come*, in *Washington University Global Studies Law Review*, 2003, pp. 415-426.

Hollis Duncan B., *Why States Need an International Law for Information Operations*, in *Lewis and Clark Law Review*, 2007, pp. 1023-62.

Holvoet M., *International Criminal Liability for Spreading Disinformation in the Context of Mass Atrocity*, in *Journal of International Criminal Justice*, 2022, pp. 223-250.

Hulme K., *Natural Environment*, in Wilmshurst E., Breau S. (eds.), *Perspectives on the ICRC Study on Customary International Humanitarian Law*, Cambridge, 2009, pp. 204-237.

Intoccia G., *Communications Technology, Warfare, and the Law: Is the Network a Weapon System?*, in *Houston Journal of International Law*, 2006, pp. 467-489.

Ipsen K., *Combatants and Non-Combatants*, in Fleck D. (ed.), *The Handbook of International Humanitarian Law*, Oxford, 2008, pp. 79-117.

Ipsen K., *Ruses of War*, in *MPEPIL*, 1982.

Jensen E. T., *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, in *Stanford Journal of International Law*, 2002, pp. 207-240.

Jensen E. T., *Cyber Attacks: Proportionality and Precautions in Attack*, in *International Law Studies*, 2013, pp. 198-217.

Jensen E. T., *Cyber Warfare and Precautions Against the Effects of Attacks*, in *Texas Law Review*, 2010, pp. 1533-1569.

Jevglevskaja N., *International Law and Weapons Review: Emerging Military Technology under the Law of Armed Conflict*, Cambridge, 2021, p. 8 ss.

Johnson A. P., *Is It Time for a Treaty on Information Warfare?*, in *International Law Studies*, 2002, pp. 439-455.

Joyner C., Lotrionte C., *Information Warfare as International Coercion: Elements of a Legal Framework*, in *European Journal of International Law*, 2001, pp. 825-865.

Kalshoven F., Zegveld L., *Constraints on the Waging of War: An Introduction to International Humanitarian Law*, Geneva, 2001, pp. 99-100.

Kastenberg J. E., *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, in *AFL Review*, 2009, pp. 43-64.

Katz E., *Liar's War: Protecting Civilians from Disinformation during Armed Conflict*, in *IRRC*, 2021, pp. 659-682.

Kello L., *Cyber Threats*, in Daws S., Weiss T. (eds.), *The Oxford Handbook on the United Nations*, Oxford, 2018, pp. 528-540.

Kelsey J., *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, in *Michigan Law Review*, 2008, pp. 1427-1452.

Klabbers J., *Intervention, Armed Intervention, Armed Attack, Threat to Peace, Act of Aggression, and Threat or Use of Force: What's the Difference?*, in Weller M. (ed.), *The Oxford Handbook of the Use of Force in International Law*, Oxford, 2016, pp. 488-506.

Kliem T., *You can't cyber in here, this is the War Room! A rejection of the effects doctrine on cyberwar and the use of force in international law*, in *Journal on the Use of Force and International Law*, 2017, pp. 1-27.

Knuckey S., Moorehead A., McCalley A., Brown A., *The Proportionality Rule and Mental Harm in War*, in Kress C., Lawless R. (eds.), *Necessity and Proportionality in International Peace and Security Law*, Oxford, 2021, pp. 367-408.

Kodar E., *Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello*, in *Baltic Yearbook of International Law Online*, 2009, pp. 133-155.

Koh H. *International Law in Cyberspace*, in *Harvard International Law Journal*, 2012, pp. 1-12.

Kolb R., *Ius contra bellum, Le droit international relatif au maintien de la paix*, Bruxelles, 2003, p. 167.

Kolb R., Vité S., *Le droit de l'occupation militaire. Perspectives historiques et enjeux juridiques actuelles*, Bruxelles, 2009, p. 187.

Kolb R., *Military Objectives in International Humanitarian Law*, in *Leiden Journal of International Law*, 2015, pp. 961-700.

Kooijmans P. J., *The Enlargement of the Concept Threat to the Peace*, in Dupuy R. J. (ed.), *The Development of the Role of the Security Council*, Dordrecht, 1993, pp. 111-121.

Kretzmer D., *Emergency, State of*, in *MPEPIL*, 2008.

Krisch N., *Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 39*, in Simma B., Nolte G., Paulus A. (eds.), *The Charter of the United Nations: A Commentary*, vol. II, Oxford, 2012, p. 1332 ss.

Lahmann H., *Unilateral Remedies to Cyber Operations*, Cambridge, 2020.

Lattanzi F., *Il confine fra diritto internazionale umanitario e diritti dell'uomo*, in *Studi in Onore di Gaetano Arangio Ruiz*, Vol. III, Napoli, 2004, pp. 1985-2036.

Lehnardt C., *Private Military Companies*, in *MPEPIL*, 2011.

Lemnitzer J. M., *Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace*, in *European Journal of International Law*, 2022, pp. 789-819.

Lesaffer R., *Kellogg-Briand Pact (1928)*, in *MPEPIL*, 2010.

Lewis S., *The Targeting of Civilian Contractors in Armed Conflict*, in *Yearbook of International Humanitarian Law*, 2006, pp. 25-64.

Lin H., *Cyber Conflict and International Humanitarian Law*, in *IRRC*, 2012, pp. 515-531.

Liivoja R., McCormack T., *Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello*, in *Yearbook of International Humanitarian Law*, 2012, pp. 1-14.

Longobardo M., *L'applicabilità delle norme riguardanti lo spionaggio e la partecipazione diretta dei civili alle ostilità al fenomeno del Cyber Exploitation*, in Distefano M. (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale: temi scelti*, Napoli, 2017, pp. 37-65.

Lubell N., *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, in *International Law Studies*, 2013, pp. 251-275.

Madden M., *Of Wolves and Sheep: A Purposive Analysis of Perfidy Prohibitions in International Humanitarian Law*, in *Journal of Conflict and Security Law*, 2012, pp. 339-463.

Mačák K., *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, in *Israel Law Review*, 2015, pp. 55-80.

Marauhn T., Ntouband F. Z., *Armed Conflict, Non-International*, in *MPEPIL*, 2016.

Marchisio S., *L'ONU. Il diritto delle Nazioni Unite*, Bologna, 2012, p. 221.

Margulies P., *Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"*, in *International Law Studies*, 2013, pp. 53-76.

Maurer T., *Cyber Mercenaries, The State, Hackers, and Power*, Cambridge, 2018.

May L., *The Nature of War and the Idea of "Cyberwar"*, in Ohlin J. D. (ed.), *Law and Ethics for Virtual Conflicts*, Oxford, 2015, pp. 1-15.

Mazzeschi Pisillo R., *Diritto internazionale dei diritti umani. Teoria e prassi*, Torino, 2020, pp. 13-28.

McKenzie S., *Cyber Operations against Civilian Data, Revisiting War Crimes against Protected Objects and Property in the Rome Statute*, in *Journal of International Criminal Justice*, 2021, pp. 1165-1192.

McLaughlin R., Paige T. P., Guilfoyle D., *Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization*, in *Journal of Conflict and Security Law*, 2022, pp. 1-42.

Melzer N., *Civilian Participation in Armed Conflict*, in *MPEPIL*, 2010.

Melzer N., *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research, Geneva, 2011, pp. 1-38.

Melzer N., *Targeted Killing in International Law*, Oxford, 2008, pp. 300-311.

G. T. Merlo, *Il Dominio degli Spazi: Il cosmo, la cyberwar, la guerra futura*, in *La Comunità internazionale*, 2010, pp. 533-559.

Meron T., *The Humanization of International Law*, The Hague, 2006, pp. 91-187.

Meyrowitz H., *Le principe de l'égalité des belligérants devant le droit de la guerre*, Paris, 1970, p. 33 ss.

Meron T., *The Martens Clause, Principles of Humanity, and Dictates of Public Conscience*, in *American Journal of International Law*, 2000, pp. 78-89.

Moir L., *The Law of Internal Armed Conflict*, Cambridge, 2002, p. 34.

Morth T. A., *Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter*, in *Case Western Reserve Journal of International Law*, 1998, pp. 567-600.

Myjer E., *Some thoughts on cyber deterrence and public international law*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 284-304.

Obradovic K., *La protection de la population civile dans les conflits armés internationaux*, in Cassese A. (ed.), *The New Humanitarian Law of Armed Conflict*, Vol. I, Napoli, 1979, pp. 128-160.

O'Connell M. E., *21st Century Arms Control Challenges: Drones, Cyber Weapons, Killer Robots, and Wmds*, in *Washington University Global Studies Law Review*, 2014, pp. 515-533.

O'Connell M. E., *Cyber Security Without Cyber War*, in *Journal of Conflict and Security Law*, 2012, pp. 187-209.

O'Connell M. E., *The Prohibition on the Use of Force*, in White N. D., Henderson C. (eds.), *Research Handbook of International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum*, Cheltenham, 2013, p. 102.

O'Donnell B. T., Kraska J. C., *International Law of Armed Conflict and Computer Network Attack: Developing the Rules of Engagement*, in *International Law Studies*, 2002, pp. 359-421.

O'Keefe R., *The Protection of Cultural Property in Armed Conflict*, Cambridge, 2006, pp. 97-98.

Okimoto K., *The Distinction and Relationship between Jus ad Bellum and Jus in Bello*, Oxford/Portland, 2011, p. 19.

O'Meara C., *Necessity and Proportionality and the Right of Self-Defence in International Law*, Oxford, 2021, p. 42 ss.

Ong R., *Hard Drive Heritage: Digital Cultural Property in the Law of Armed Conflict*, in *Columbia Human Rights Law Review*, 2021, pp. 247-296.

Oppenheim L., *International law, Vol. II, War and Neutrality*, 1981, Ney York, pp. 300-398.

O'Shea A. G., *Individual Criminal Responsibility*, in *MPEPIL*, 2009.

Parks W. H., *Conventional Weapons and Weapons Reviews*, in *Yearbook of International Humanitarian Law*, 2005, pp. 55-142.

Partington E. A., *Manuals on the Law of Armed Conflict*, in *MPEPIL*, 2016.

Partsch K. J., *Armed Conflict*, in *EPIL*, 1992, pp. 249-255.

Pertile M., *La relazione tra risorse naturale e conflitti armati nel diritto internazionale*, Padova, 2012, pp. 167-177.

Peterson I., *The Natural Environment in Times of Armed Conflict*, in *Leiden Journal of International Law*, 2009, pp. 325-343.

Pfanner T., *Military Uniforms and the Law of War*, in *IRRC*, 2004, pp. 93-124.

Pictet J., *Le droit humanitaire et la protection des victimes de la guerre*, Leiden, 1973, p. 13.

Pilloud C., *et al.* (eds.), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva, Norwell, MA, USA, 1987.

Pollicino O., *The Right to Internet Access. Quid Iuris?*, in Arnauld A., Decken K., Susi M. (eds.), *The Cambridge Handbook of New Human Rights Recognition, Novelty, Rhetoric*, Cambridge, 2020, pp. 263-275.

Pomson O., *'Objects'? The Legal Status of Computer Data under International Humanitarian Law*, in *Journal of Conflict and Security Law*, 2023, pp. 349-387.

Pobjie E., *Prohibited Force. The Meaning of "Use of Force" in International Law*, Cambridge, 2024, p. 132.

Pustogarov V. V., *The Martens Clause in International Law*, in *Journal of the History of International Law*, 1999, pp. 125-135.

Quéguiner J., *Precautions under the Law Governing the Conduct of Hostilities*, in *IRRC*, 2006, pp. 793-821.

Qureshi W., *Information Warfare, International Law, and the changing battlefield*, in *Fordham International Law Journal*, 2020, pp. 907-908.

Robertson B., *Self-Defense against Computer Network Attack under International Law*, *International Law Studies*, 2002, pp. 121-147.

Roberts A., Guelff R., *Documents on the Law of War*, Oxford, 2000, p. 511.

Roberts A., *What is Military Occupations?*, in *British Yearbook of International Law*, 1984, pp. 249-267.

Rogers A. P. V., *Law on the Battlefield*, Manchester, 2004, p. 63.

Roguski P., *An Inspection Regime for Cyber Weapons: A Challenge Too Far?*, in *American Journal of International Law*, 2021, pp. 111-115.

Ronzitti N., *Civilian Population in Armed Conflict*, in *MPEPIL*, 2010.

Ronzitti N., *Diritto internazionale dei conflitti armati*, Torino, 2017.

Ronzitti N., *Neutralità*, in Cassese S. (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, pp. 1-13.

Roscini M., *Cyber Operations as a Use of Force*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 233-254.

Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford, 2014.

Roscini M., *Legittima difesa*, in *Treccani Diritto on line*, 2015.

Roscini M., *World Wide Warfare: Jus ad bellum and the Use of Cyber Force*, in *Max Planck Yearbook of United Nations Law*, 2010, pp. 86-130.

Rousseau C., *Le droit des conflits armés*, Paris, 1983, p. 24 ss.

Rowe N. C., *Distinctive ethical challenges of cyberweapons*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 307-325.

Ruffert M., *Reprisals*, in *MPEPIL*, 2021.

Ruotolo G. M., *Internet (diritto internazionale)*, in *Enciclopedia del diritto*, Annali VII, Milano, 2014, pp. 545-567.

Rusinova V., *Perfidy*, in *MPEPIL*, 2011.

Ruys T., *"Armed Attack" and Article 51 of the UN Charter*, Cambridge, 2010, p. 139.

Ruys T., *The Meaning of "Force" and the Boundaries of the Jus ad Bellum: Are "Minimal" Uses of Force Excluded from Un Charter Article 2(4)?*, in *American Journal of International Law*, 2014, pp. 159-210.

Ryan S., *Submarine Communication Cables and Belligerent Rights in Armed Conflict*, in *Ocean Yearbook Online*, 2024, pp. 1-36.

Salerno F., Annoni A., *La tutela internazionale della persona umana nei conflitti armati*, Bari, 2019.

Salter M., *Reinterpreting Competing Interpretations of the Scope and Potential of the Martens Clause*, in *Journal of Conflict and Security Law*, 2012, pp. 403-437.

Salvadego L., *Struttura e funzioni della necessità militare nel diritto internazionale*, Torino, 2016, p. 148 ss.

Sassòli M., *Combatants*, in *MPEPIL*, 2015.

Sassòli M., *International Humanitarian Law*, Cheltenham, 2019, pp. 456-467.

Sassòli M, *Legislation and Maintenance of Public Order and Civil Life by Occupying Powers*, in *European Journal of International Law*, 2005, pp. 661-694.

Sassòli M., *Military Objectives*, in *MPEPIL*, 2015.

Schaller C., *Guerrilla Forces*, in *MPEPIL*, 2019.

Schaller C., *Spies*, in *MPEPIL*, 2009.

Schmitt M. N., *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, in Ziolkowski K. (eds.), *4th International Conference on Cyber Conflict, Cycon 2012 – Proceedings*, NATO CCD COE Publications, Tallinn, 2012, pp. 283-293.

Schmitt M. N., *Classification of Cyber Conflict*, in *Journal of Conflict and Security Law*, 2012, pp. 245-260.

Schmitt M. N., *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, pp. 885-937.

Schmitt M. N., *Cyber Operations and the Jus in Bello: Key Issues*, in *International Law Studies*, 2002, pp. 89-110.

Schmitt M. N., *Wired Warfare: Computer Network Attack and Jus in Bello*, in *IRRC*, 2002, pp. 365-399.

Schreier F., *On Cyberwarfare*, DCAF Horizon 2015 Working Paper n. 7, pp 1-134.

Schrijver N., *Article 2, Paragraphe 4*, in Cot J., Pellet A., Forteau M. (sous la direction de), *La Charte des Nations Unies. Commentaire article par article*, vol. I, Paris, 2005, p. 125 ss.

Seger P., *The Law of Neutrality*, in Gaeta P., Clapham A. (eds.), *The Oxford Handbook of International Law in Armed Conflict*, Oxford, 2014, pp. 248-272.

Segura S. A., *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, pp. 191-272.

Sereni A. P., *Diritto internazionale, IV, Conflitti internazionali,* Milano, 1965.

Serrano C., *From bullets to fake news: Disinformation as a weapon of mass distraction. What solutions does International Law provide?*, in *Spanish Yearbook of International Law*, 2020, pp. 129-154.

Silver D. B., *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in *International Law Studies*, 2002, pp. 73-99.

Sivakumaran S., *The Law of Non-International Armed Conflict*, Oxford, 2012, p. 255.

Shackelford S., *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, in *Berkley Journal of International Law*, 2008, pp. 191-250.

Sharp W. G., *Cyberspace and the Use of Force*, Virginia, 1999, p. 102.

Sliedregt E., *Command Responsibility and Cyberattacks*, in *Journal of Conflict and Security Law*, 2016, pp. 505-521.

Sossai M., *The Place of Cities in the Evolution of International Humanitarian Law*, in *Italian Yearbook of International Law*, 2021, pp. 227-252.

Stahn C., *Jus ad bellum, jus in bello…jus post bellum? - Rethinking the Conception of the Law of Armed Force*, in *European Journal of International Law*, 2006, pp. 921-943.

Starace V., *Uso della forza nell'ordinamento internazionale*, in *Enciclopedia Giuridica*, vol. XXXII, Roma, 1994, pp. 1-15.

Steiger D., *Civilian Objects*, in *MPEPIL*, 2011.

Stephens D., Skousgaard T., *Flags and Uniforms in War*, in *MPEPIL*, 2009.

Strebel H., *Martens Clause*, in *EPIL*, 1982, pp. 252-253.

Swanson L., *The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian Georgian Cyber Conflict*, in *Loyola of Los Angeles International and Comparative Law Review*, 2010, pp. 303-333.

Tarasofsky R. G., *Legal protection of the environment during international armed conflict*, in *Netherlands Yearbook of International Law*, 1993, pp. 17-79.

Trahan J., *The Criminalization of Cyber-Operations under the Rome Statute*, in *Journal of International Criminal Justice,* 2021, pp. 1133-1164.

Tsagourias N., Farrell M., *Cyber Attribution: Technical and Legal Approaches and Challenges*, in *European Journal of International Law*, 2020, pp. 941-967.

Tsagourias N., *Cyber Attacks, Self-Defence and the Problem of Attribution*, in *Journal of Conflict and Security Law*, 2012, pp. 229-244.

Tsagourias N., Biggio G., *Cyber Peacekeeping Operations and the Regulation of the Use of Lethal Force*, in *International Law Studies*, 2022, pp. 36-71.

Tsagourias N., *The Legal Status of Cyberspace*, in Tsagourias N., Buchan R. (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015, pp. 13-30.

Tsagourias N., Biggio G., *The Regulation of Cyber Weapons*, in Myjer E., Marauhn T. (eds.), *Research Handbook on International Arms Control Law*, Cheltenham, 2022. pp. 440-455.

Tully S., *A Human Right to Access the Internet? Problems and Prospects*, in *Human Rights Law Review*, 2014, pp. 175-195.

Turns D., *Cyber Warfare and the Notion of Direct Participation in Hostilities*, in *Journal of Conflict and Security Law*, 2012, pp. 279–297.

UK Ministry of Defence, *The Manual of the Law of Armed Conflict*, Oxford, 2004.

Vagias M., *The Territorial Jurisdiction of the ICC for Core Crimes Committed Through the Internet*, in *Journal of Conflict and Security Law*, 2016, pp. 523-540.

Venturini G., *Diritto umanitario e diritti dell'uomo: rispettivi ambiti di intervento e punti di confluenza*, in *Rivista internazionale dei diritti dell'uomo*, 2001, pp. 57-74.

Venturini G., *Necessità e proporzionalità nell'uso della forza militare in diritto internazionale*, Milano, 1988.

Venturini G., *Necessity in the Law of Armed Conflict and in International Criminal Law*, in *Netherlands Yearbook of International Law*, 2010, pp. 45-78.

Verwey E. D., *Protection of the Environment in Times of Armed Conflict: In Search of a New Legal Perspective*, in *Leiden Journal of International Law*, 1995, pp. 7-40.

Vitucci M., *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo ucraino*, in *La Comunità internazionale*, 2023, pp. 7-31.

Vöneky S., Wolfrum R., *Environment, Protection in Armed Conflict*, in *MPEPIL*, 2016.

Wagner M., *Autonomous Weapon Systems*, in *MPEPIL*, 2016.

Walker K., *Information Warfare and Neutrality*, in *Vanderbilt Journal of Transnational Law*, 2000, pp. 1079-1202.

Wallace D., Reeves R., *The Law of Armed Conflicts "Wicked" Problem: Levée en Masse in Cyber Warfare*, in *International Law Studies*, 2013, pp. 646-668.

Waters C., *New Hacktivists and the Old Concept of Levée En Masse*, in *The Dalhousie Law Journal*, 2014, pp. 772-786.

Watts S., *Combatant Status and Computer Network Attack*, in *Virginia Journal of International Law*, 2010, pp. 391-447.

Waxman M., *Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011, pp. 420-458.

Wedgwood R. G., *Proportionality, Cyberwar, and the Law of War*, in *International Law Studies*, 2002, pp. 219-232.

Werle G., *Principles of International Criminal Law*, The Hague, p. 265.

Wet E., M. Wood, *Peace, Threat to*, in *MPEPIL*, 2009.

Williams W. S., Lawless R., *Levée en Masse in Twenty-First-Century Armed Conflict*, in Schmitt M. N. (eds.), *Prisoners of War in Contemporary Conflict*, Oxford, 2023, p. 256 ss.

Wilmshurst E., *The Chatham House Principles of International Law on the Use of Force in Self-Defence*, 2006, pp. 1-70.

Wolfrum R., *Cultural Property, Protection in Armed Conflict*, in *MPEPIL*, 2010.

Woltag J. C., *Cyber Warfare*, Cambridge, 2014.

Woltag J. C., *Cyber Warfare*, in *MPEPIL*, 2015.

Woltag J. C., *Internet*, in *MPEPIL*, 2010.

Wood M., *Peace, Breach of*, in *MPEPIL*, 2009.

Wood M., *Use of Force, Prohibition of Threat*, in *MPEPIL*, 2013.

Yip K. L., *Separation between jus ad bellum and jus in bello as insulation of results, not scopes, of application*, in *The Military Law and the Law of War Review*, 2020, pp. 1-51.

Zanardi L., *La legittima difesa nel diritto internazionale*, Milano, 1972, p. 263.

Zemanek K., *Armed Attack*, in *MPEPIL*, 2013.

Zerbe Y., *Cyber-Enabled International State-Sponsored Disinformation Operations and the Role of International Law*, in *Swiss Review of International and European Law*, 2023, pp. 49-75.

Ziolkowski K., *Stuxnet-Legal Considerations*, CCDCOE, 2012, pp. 1-25.