Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

ALESSANDRO STIANO*

L'INTERVENTO DI ANONYMOUS NEL CONFLITTO TRA RUSSIA E UCRAINA: ALCUNE RIFLESSIONI SULLO *STATUS* GIURIDICO DEGLI *HACKER* ATTRAVERSO IL PRISMA DEL DIRITTO INTERNAZIONALE UMANITARIO

1. *Introduzione*

Il conflitto in corso tra Russia e Ucraina – iniziato il 24 febbraio 2022 a seguito dell'aggressione della prima a danno della seconda[1] – ha confermato l'emersione di due fenomeni tra loro interconnessi. In primo luogo, stiamo assistendo ad un parziale cambio di paradigma che vede la conduzione delle ostilità non più esclusivamente su un campo di battaglia fisico, attraverso l'utilizzo di armi tradizionali, ma si spinge altresì sul piano virtuale con l'ausilio di strumenti informatici; in secondo luogo, e per quanto di nostro interesse, un coinvolgimento sempre maggiore di attori non statali che decidono di prendere parte alle ostilità. Espressione di entrambi questi fenomeni è il Collettivo di *hacker* che prende il nome di Anonymous, il quale pochi giorni dopo l'inizio del conflitto ha dichiarato una *cyber* guerra alla Russia[2]. Da quel momento in poi, Anonymous ha dichiarato di aver hackerato le

* Ricercatore di tipo A di Diritto internazionale, Università degli Studi di Napoli "Federico II".

[1] Per alcune considerazioni sul conflitto si veda, tra gli altri, M. MILANOVIC, *What is Russia's Legal Justification for Using Force against Ukraine*, in *EjilTalk!*, 24 febbraio 2022; A. SPAGNOLO, *Prime considerazione sul tentativo della Russia di giustificare l'intervento armato in Ucraina*, in *SidiBlog*, 25 febbraio 2022;

[2] D. MILMO, *Anonymous: the hacker collective that has declared cyberwar on Russia*, in *The Guardian*, 27 febbraio, 2022; più in generale sulla definizione di cyber war si veda G.M. RUOTOLO, *Abolish the Rules Made of Stone? Contemporary International Law and the models to Internet Regulations*, in *Italian Review of International and Comparative Law*, 2021, p. 261 ss.

informazioni personali di centoventimila soldati russi, riuscendo ad ottenere informazioni sensibili quali la data di nascita, il numero di passaporto e gli indirizzi personali; di aver attaccato la banca centrale russa, riuscendo a sottrarre migliaia di documenti; di aver hackerato la televisione russa per permettere ai cittadini di vedere le atrocità poste in essere dal Presidente russo e infine di aver hackerato i siti internet appartenenti alle agenzie governative e alle agenzie di stampa[3].

Tuttavia, l'attivismo di Anonymous non è certamente iniziato quest'anno e non è riconducibile solo al conflitto russo-ucraino. Ripercorrendo brevemente la storia del Collettivo emerge che il fenomeno Anonymous sia apparso per la prima volta nel 2003 sulla piattaforma online *4chan*[4]. Nonostante l'obiettivo del Collettivo non sia stato sempre chiaro, esso in diverse occasioni ha affermato di voler portare avanti forme di protesta sociale volte a tutelare alcuni diritti fondamentali come la libertà di espressione, di associazione e più, in generale, le libertà individuali[5]. Una prima visibilità a livello internazionale, poi, è stata acquisita in occasione degli attacchi informatici commessi nei confronti di alcune compagnie private come PayPal, MasterCard e Sony e, successivamente, contro gli Stati Uniti e la NATO; nonché per la partecipazione alle proteste portate avanti in Tunisia, Libia e Uganda durante la Primavera araba[6].

L'attivismo del gruppo di *hacker* è diventato ancor più rilevante allorquando, in seguito all'operazione *Pillar of Defence* lanciata da Israele nel 2012 e all'intervento militare di questo stesso Stato nella striscia di Gaza, Anonymous ha contribuito alla individuazione dei missili lanciati da Hamas e ha dichiarato una *cyber war* al cyberspazio israeliano. In quella occasione il Collettivo ha invitato gli altri componenti ad attivarsi «to hack, deface, hijack, database leak, admin takeover, and DNS terminate the Israeli cyberspace by any means necessary»[7]. Successivamente, alcuni membri di Anonymous hanno lanciato attacchi DDoS[8] contro i siti internet del governo israeliano, causando diversi danni ancorché di lieve entità[9].

Tanto premesso, anche in virtù di una dottrina assai scarna sul tema, vi è senz'altro l'esigenza di una riflessione sulla qualificazione giuridica degli *hacker* (con particolare riferimento al gruppo Anonymous) nell'eventualità in cui questi decidano di prendere parte ad un conflitto armato internazionale. Si cercherà di dimostrare che il Collettivo, sebbene non sia suscettibile di essere qualificato alla stregua di "legittimi combattenti", possa invece essere considerato come un gruppo di civili che "partecipano direttamente alle ostilità". L'analisi prenderà le mosse dalle norme di diritto internazionale umanitario attualmente

---

[3] D. MILMO, *Anonymous: the hacker collective that has declared cyberwar on Russia*, cit.

[4] Si tratta di un sito web *imageboard*, fondato nel 2003 da Christopher Poole, ove è possibile condividere immagini e discutere dei più svariati temi di attualità. La principale caratteristica sta nel fatto che gli utenti possono restare anonimi.

[5] Cfr. R. BUCHAN, *Cyber Warfare and the Status of Anonymous under International Humanitarian Law*, in *Chin. Jour. Int. Law*, 2016, p. 741 ss.

[6] M. DI LIDDO, A. FALCONI, G. IACOVINO, L. LABELLA, *Il Ruolo dei Social Network nelle Rivolte Arabe*, in *Osservatorio di politica internazionale*, 2011, p. 4 ss.

[7] Cfr. G. DELLA MORTE, *Big Data e protezione internazionale dei diritti umani*, Napoli, 2018, p. 203, in particolare nota n. 567.

[8] Gli attacchi DDos, acronimo di *Distributed Denial of Service*, traducibile in italiano come interruzione distribuita del servizio, consistono nell'invio di una enorme quantità di richieste di accesso ad un determinato sito internet fino a renderlo totalmente irraggiungibile.

[9] Cfr. B. VALERIANO, R. C. MANESS, *Cyber War versus Cyber Realities: Cyber Conflict in the International System*, Oxford, 2015, p. 171.

vigenti[10] e, per evitare un approccio eccessivamente teorico, sarà condotta attraverso la lente del conflitto tra Russia e Ucraina.

A questo fine si procederà anzitutto ad una disamina sulla possibile qualificazione degli *hacker* come "combattenti"*:* si prenderanno le mosse dall'articolo 4 (A) della III Convenzione di Ginevra del 1949[11] (par. 2 ss.) e poi si esaminerà l'applicabilità del concetto di *levée en masse* al contesto cibernetico e in particolare ad Anonymous (par. 3 ss.). Successivamente, dopo aver escluso l'applicabilità di entrambe le norme al contesto in oggetto, proveremo a dimostrare che durante il conflitto in corso i membri di Anonymous siano da considerare come dei "civili" che partecipano direttamente alle ostilità (par. 4 ss.). Infine, verrà tratteggiata una sintesi della ricerca condotta (par. 5).

2. *Lo* status *di combattente ai sensi dell'art. 4 (A) della Terza Convenzione di Ginevra del 1949 alla prova di Anonymous*

Come è noto, una delle norme cardine del diritto internazionale umanitario è quella che fa riferimento al principio di distinzione[12]. Brevemente, essa prevede un obbligo in capo alle parti del conflitto di distinguere tra coloro i quali assumono la qualifica di combattenti e coloro, invece, che vengono definiti civili durante un conflitto armato internazionale. Scopo

[10] Tale scelta discende anche dal c.d. principio di neutralità tecnologica, secondo cui le norme giuridiche devono essere interpretate in modo tale da poter applicate indipendentemente dal tipo di tecnologia, o dal mezzo di comunicazione, utilizzato nel caso specifico. Sul tema della neutralità tecnologica, sviluppatosi soprattutto nell'ambito del commercio internazionale, si rimanda, tra gli altri, a G. GAGLIANI, *Cybersecurity, Technological Neutrality, and International Trade Law*, in *Jour. Int. Econ. Law*, 2020, p. 723 ss.; G. M. RUOTOLO, *The EU data protection and the multilatateral trading system: Where dream and day unite*, in *Questions of International Law*, 2018, p. 5 ss.; J. HOJNIK, *Technology Neutral EU law: Digital Goods within the Traditional Goods/Services Distinction*, in *International Journal Law and Information Technology*, 2017, p. 63 ss.

[11] Secondo la lettera dell'art. 4 (A): «A. Sono prigionieri di guerra, nel senso della presente Convenzione, le persone che, appartenendo ad una delle seguenti categorie, sono cadute in potere del nemico: 1. i membri delle forze armate di una Parte belligerante, come pure i membri delle milizie e dei corpi di volontari che fanno parte di queste forze armate; 2. i membri delle altre milizie e degli altri corpi di volontari, compresi quelli dei movimenti di resistenza organizzati, appartenenti ad una Parte belligerante e che operano fuori o all'interno del loro proprio territorio, anche se questo territorio è occupato, sempreché queste milizie o questi corpi di volontari, compresi detti movimenti di resistenza organizzati, adempiano le seguenti condizioni: a. abbiano alla loro testa una persona responsabile dei propri subordinati; b. rechino un segno distintivo fisso e riconoscibile a distanza; c. portino apertamente le armi; d. si uniformino, nelle loro operazioni, alle leggi e agli usi della guerra; 3. i membri delle forze armate regolari che sottostiano ad un governo o ad un'autorità non riconosciuti dalla Potenza detentrice; 4. le persone che seguono le forze armate senza farne direttamente parte, come i membri civili di equipaggi di aeromobili militari, corrispondenti di guerra, fornitori, membri di unità di lavoro o di servizi incaricati del benessere delle forze armate, a condizione che ne abbiano ricevuto l'autorizzazione dalle forze armate che accompagnano. Queste sono tenute a rilasciar loro, a tale scopo, una tessera d'identità analoga al modulo allegato; 5. i membri degli equipaggi, compresi i comandanti, piloti e apprendisti della marina mercantile e gli equipaggi dell'aviazione civile delle Parti bellige-ranti che non fruiscano di un trattamento più favorevole in virtù di altre disposizioni del diritto internazionale; 6. la popolazione di un territorio non occupato che, all'avvicinarsi del nemico, prenda spontaneamente le armi per combattere le truppe d'invasione senza aver avuto il tempo di organizzarsi come forze armate regolari, purché porti apertamente le armi e rispetti le leggi e gli usi della guerra».

[12] Corte internazionale di giustizia, 8 luglio 1996, parere *sulla liceità della minaccia o dell'impiego di armi nucleari*, par.78, ove la Corte ha affermato che «[t]he cardinal principles contained in the texts constituting the fabric of humanitarian law are the following. The first is aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants (…)».

del principio è quello di proteggere la popolazione e gli obiettivi civili da possibili attacchi nonché tracciare una linea di demarcazione tra i combattenti e non combattenti[13]. Di conseguenza, durante un conflitto armato internazionale, agli Stati è fatto divieto di attaccare i civili e utilizzare armi che siano incapaci di operare una distinzione tra le due categorie di soggetti[14] e quindi solo i *combattenti* potranno essere destinatari della violenza bellica durante le ostilità[15].

Ora, affinché il principio possa trovare applicazione è necessario anzitutto identificare e qualificare i soggetti che assumono la qualifica di *combattenti*. Le norme che si occupano della questione sono molteplici. Innanzitutto, il Protocollo Addizionale I alle Convenzioni di Ginevra del 1949 all'art. 43, paragrafo I, definisce i combattenti come «members of the armed forces of a party to conflict»[16]; il paragrafo precedente, invece, stabilisce che «The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, inter alia, shall enforce compliance with the rules of international law applicable in armed conflict»[17]. In aggiunta alle disposizioni appena citate, è doveroso richiamare altresì l'art. 4 (A) della Terza Convenzione di Ginevra del 1949, il quale, come è noto, nonostante faccia formalmente riferimento ai criteri per individuare chi possa essere qualificato come prigioniero di guerra, è utile indirettamente per indentificare i combattenti dal momento che solo a questi ultimi è possibile riconoscere lo *status* di prigionieri di guerra.

Al primo paragrafo, infatti, la norma sottolinea che potranno essere considerati prigionieri di guerra coloro che siano membri delle forze armate regolari di uno Stato, mentre il secondo paragrafo estende tale *status* alle forze armate irregolari che siano parte del conflitto[18].

Ora, per ragioni evidenti, e cioè l'impossibilità di far rientrare Anonymous nella categoria delle forze armate regolari di uno Stato, la nostra analisi si concentrerà

---

[13] *Ibidem*.

[14] Per una analisi sull'applicazione del principio di distinzione e l'utilizzo di armi non convenzionali si v. D. AMOROSO, *Autonomous Weapons Systems and International Law: A Study on Human-Machine Interactions in Ethically and Legally Sensitive Domains*, Napoli, 2020, p. 45 ss.; M. W. MEIER, *Emerging Technologies and the Principle of Distinction*, in R.T.P. ALCALA, E.T. JENSEN (a cura di), *The Impact of Emerging Technologies on the Law of Armed Conflict*, Oxford, 2019, p. 211 ss.

[15] Sui conflitti armati internazionali e sul ruolo dei combattenti legittimi si veda, tra tutti, N. RONZITTI, *Diritto internazionale dei conflitti armati*[xii], Torino, 2021; M. CASTELLANETA, *Conflitti armati (diritto internazionale*), in *Enc. dir.*, *Annali* V, 2012, p. 316 ss.

[16] *Protocol Additional to the Geneve Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 8 giugno1977.

[17] *Ibidem*.

[18] La *ratio* di questa previsione è quella di estendere i privilegi dei legittimi combattenti anche a coloro che siano parte di forze irregolari (come, ad esempio, i movimenti di resistenza che hanno operato durante la Seconda guerra mondiale), i quali nonostante non siano ufficialmente incorporati nelle forze armate regolari di uno Stato presentano caratteristiche simili a queste. Sul punto si veda più diffusamente il commentario alla regola n. 4 del comitato della Croce Rossa Internazionale sugli studi del diritto internazionale consuetudinario; J.M. HENCKAERTS, L. DOSWALD-BECK, *Customary International Humanitarian Law*, Volume I: Rules, Cambridge, 2005, p. 15, in cui viene indicato che «[t]he Hague Regulations and the Third Geneva Convention thus consider all members of armed forces to be combatants and require militia and volunteer corps, including organised resistance movements, to comply with four conditions in order for them to be considered combatants entitled to prisoner-of-war status. The idea underlying these definitions is that the regular armed forces fulfil these four conditions per se and, as a result, they are not explicitly enumerated with respect to them».

esclusivamente sul secondo paragrafo. In proposito l'art. 4(A)(2) individua tre requisiti affinché un gruppo possa essere qualificato alla stregua di un "gruppo armato irregolare"*: i)* l'esistenza di una persona al comando che sia responsabile per le attività dei subordinati; *ii)* il bisogno di indossare elementi distintivi che siano riconoscibili a distanza; *iii)* la necessità di portare apertamente le armi.

Nei paragrafi successivi, analizzeremo singolarmente l'elemento *sub i)* mentre i requisiti *sub ii) e iii),* vista la loro stretta connessione, verranno esaminati congiuntamente nel paragrafo 2.2.

2.1. *Presenza di un comandante che sia responsabile per i propri subordinati*

L'individuazione di un soggetto al comando che sia responsabile per i propri subordinati rappresenta indubbiamente uno dei requisiti più rilevanti e allo stesso tempo più complessi per affermare l'esistenza di un gruppo organizzato. Ne è una prova il fatto che il Tribunale Penale Internazionale per la *ex*-Jugoslavia, nella decisione relativa al caso *Tarculovski*[19], abbia fornito una serie di fattori ulteriori al fine di agevolare questo processo. In via di premessa, va rilevato che nonostante nel caso di specie il Tribunale si sia pronunciato sulla sussistenza di un gruppo armato organizzato al fine di determinare l'esistenza di un conflitto armato *non* internazionale, non si individuano motivi che ostano all'utilizzo di tali elementi anche nel caso di conflitti armati internazionali[20].

Più nello specifico, in *Tarculovski*, il Tribunale ha indicato come fattori utili per individuare la presenza di un gruppo organizzato l'esistenza di: a) prove di una struttura di comando; b) prove che il gruppo ponga in essere operazioni coordinate; c) esistenza di capacità logistiche del gruppo; d) prove che dimostrino la capacità del gruppo di mantenere una certa disciplina; e) prove del fatto che l'intero gruppo riesce a parlare sotto "una sola voce"[21]. Va precisato, tuttavia, che tali elementi non sono tassativi né devono essere soddisfatti simultaneamente, è chiaro però che quanti più elementi siano soddisfatti tanto più è probabile che il gruppo possa definirsi "organizzato".

Sulla scorta di queste precisazioni, dobbiamo ora chiederci se Anonymous possa definirsi alla stregua di un gruppo organizzato.

---

[19] Tribunale penale internazionale per la ex-Jugoslavia, 10 luglio 2008, *Prosecutor v. L. Boskoski and J. Trarkulovski,* merito, IT-04-82-T.

[20] Così R. BUCHAN, *Cyber Warfare and the Status of Anonymous*, cit., p. 747; P. MARGULIES, *Networks in Non-International Armed Conflicts and Defining Organized Armed Group*, in *International Law Studies*, 2013, p. 54 ss.

[21] *Prosecutor* v. *L. Boskoski and J. Trarkulovski,* cit., par. 199-203. Più nello specifico, nella citata sentenza si può leggere: «Trial Chambers have taken into account a number of factors when assessing the organisation of an armed group. These fall into five broad groups. In the first group are those factors signalling the presence of a command structure, such as the establishment of a general staff or high command, which appoints and gives directions to commanders, disseminates internal regulations, organises the weapons supply, authorises military action, assigns tasks to individuals in the organisation, and issues political statements and communiqués, and which is informed by the operational units of all developments within the unit's area of responsibility. Also included in this group are factors such as the existence of internal regulations setting out the organisation and structure of the armed group; the assignment of an official spokesperson; the communication through communiqués reporting military actions and operations undertaken by the armed group; the existence of headquarters; internal regulations establishing ranks of servicemen and defining duties of commanders and deputy commanders of a unit, company, platoon or squad, creating a chain of military hierarchy between the various levels of commanders; and the dissemination of internal regulations to the soldiers and operational units».

Alcuni autori hanno definito il collettivo Anonymous come «a global cyber insurgency»[22]. Tale definizione, a nostro avviso, risulta rilevante dal momento che sembrerebbe conferire al gruppo una spiccata gestione e organizzazione militare. A ben vedere, però, nonostante possibili sforzi interpretativi, non ci sembra possa giungersi ad una tale conclusione per almeno due ordini di ragioni.

In primo luogo, non ci pare possa affermarsi con certezza che Anonymous goda di una *membership* organizzata e aprioristicamente identificabile: la possibilità di entrare a far parte del gruppo dipende tuttora da una mera formalità e cioè l'accesso alla piattaforma ove normalmente il gruppo si riunisce (*4Chan*) senza che tuttavia siano necessari particolari condizioni da rispettare. Anche nel caso della realizzazione di un attacco informatico, il singolo soggetto gode di piena libertà nell'attribuire la condotta ad Anonymous oppure assumersene la responsabilità ovvero, più semplicemente, decidere di non condividere alcuna informazione. In questo senso, come già sottolineato in dottrina, potrebbe affermarsi che tutti possono far parte di Anonymous in quanto si tratterebbe di una *folla* di persone che agisce insieme per differenti scopi[23]. In altre parole, Anonymous sembra comportarsi più come un movimento che inspira i suoi seguaci piuttosto che un gruppo coerente, strutturato e gerarchicamente organizzato con soggetti che rivestono posizioni apicali capaci di dirigere e coordinare le attività dei membri[24].

Anche analizzando le attività più recenti del collettivo non sembra possa giungersi a conclusioni differenti. Dal 2014, infatti, alcuni membri hanno individuato e condiviso le vulnerabilità informatiche di alcuni bersagli informatici, assumendo in un certo senso la *leadership* del gruppo[25]. Inoltre, gli stessi membri, attraverso un video condiviso mediante *YouTube*, hanno rivendicato la responsabilità di Anonymous per gli attacchi informatici posti in essere contro le infrastrutture situate in Israele nel 2014 e per quelle occorse contro la Russia nel 2022.

Se da un lato questi sviluppi hanno conferito al gruppo una identità amorfa, capace di diversificare parzialmente i ruoli e la composizione al suo interno, dall'altro lato tali elementi non sembrano sufficienti per affermare la presenza di una vera e propria struttura di comando e di attività coordinate.

In secondo luogo, anche analizzando più in generale i criteri elaborati dalla giurisprudenza internazionale per l'individuazione dell'esistenza di un gruppo organizzato, si giunge alle medesime conclusioni. Più nel dettaglio, tra i criteri individuati è possibile

---

[22] P. OLSON, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*, New York, 2021, *passim*.

[23] *Ibidem*, p. 68, secondo cui «anyone can be part of it [Anonymous]. It is a crowd of people, a nebulous crowd of people, working together and doing things together for various purposes»; P. REXTON KAN, *Cyberwar in the Underworld: Anonymous versus Los Zetas in Mexico*, in *Yale Journal of International Affairs*, 2013, p. 44 ss.. Secondo l'A. infatti «one member or a small group of members can decide to engage in an online action that is derived from the Anonymous ethos; others in the collective are then free to join the action or not».

[24] Così R. BUCHAN, *Cyber Warfare and the Status of Anonymous,* cit., p. 749.

[25] Cfr. P. OLSON, *We are Anonymous,* cit., *passim*.

richiamare i seguenti: a) esistenza di un quartier generale[26]; b) indossare una uniforme[27]; c) fornire una preparazione al gruppo e adottare azioni disciplinari nei loro confronti[28].

Ora, applicando queste condizioni ad Anonymous dovrebbe affermarsi che *i)* il sito web *4chan,* luogo virtuale dove abitualmente si riunisce il collettivo, andrebbe considerato alla stregua di un quartier generale; *ii)* la maschera normalmente utilizzata dal gruppo nelle dichiarazioni sul Web sia una uniforme; *iii)* Anonymous sia dotato di un codice di condotta, il quale prevede in maniera chiara le regole per poter entrare a farne parte e le sanzioni disciplinari nel caso un membro adotti un comportamento contrario a quanto indicato sia da ritenere responsabile e pertanto passabile di sanzioni disciplinari.

Ebbene, affermare quanto sopra vorrebbe dire disattendere la *ratio* dell'art. 4(A)(2) che, in sintesi, è quella di estendere lo *status* di combattente alle forze armate irregolari che assumono le sembianze delle forze armate regolari di un Paese[29]. E sulla scorta di quanto visto sinora non ci sembra ragionevole ritenere che Anonymous abbia un quartier generale, indossi una uniforme e allo stesso tempo sia dotato di una disciplina sintomatica di una gestione militare del gruppo. D'altro canto, anche nella prassi di alcuni Stati può scorgersi un approccio restrittivo; basti pensare al governo statunitense che ha negato lo *status* di combattente ai membri dei Talebani in Afghanistan dal momento che non solo era assente la tipica organizzazione militare ma soprattutto non vi erano elementi per stabilire con certezza la presenza di *leader* responsabili dei loro subordinati nonostante per un certo periodo i Talebani avessero una organizzazione quasi militare[30].

---

[26] Cfr. Tribunale penale internazionale per la ex-Jugoslavia, 16 giugno 2004, *Prosecutor* v. *Milosevic,* ricorso n. IT-02-54-T, par. 23. Secondo il tribunale «the Trial Chamber has considered the question of the degree of organisation of the KLA and found that there is in fact a sufficient body of evidence pointing to the KLA being an organised military force, with an official joint command structure, headquarters, designated zones of operation, and the ability to procure, transport, and distribute arms».

[27] Cfr. Tribunale penale internazionale per la ex-Jugoslavia, 30 novembre 2005, *Prosecutor* v. *Limaj, Bala and Musliu,* ricorso n. IT-03-66-T, par. 123, in cui il Tribunale ha affermato «*While the existence of a uniform may be indicative of the existence of a well-organised entity*, in the view of the Chamber, this factor alone is not determinative in this case of the existence of an organised military structure, as it has little bearing on the functioning of the KLA, especially having regard to its rapid expansion after March 1998 which undoubtedly placed unanticipated strain on the provision of commodities such as uniforms, at a time when other needs were clearly more relevant to the military functioning of the KLA» (corsivo aggiunto).

[28] *Ibidem*, par. 113-117. In particolare, al par. 117, il Tribunale ha affermato che « the Chamber accepts and finds that in mid-May 1998 the General Staff of the KLA formally moved to introduce military police within the KLA. While it is not apparent on the evidence before the Chamber that disciplinary rules were then consistently enforced in KLA units, the Chamber regards this step as affording clear evidence of the growing formality and effectiveness of the organisational structure of the KLA by mid-May 1998, and of the progress of the General Staff towards ensuring that the KLA functioned as a disciplined and coordinated military force».

[29] Sul punto, appare opportuno richiamare quanto affermato dal Comitato della Croce Rossa Internazionale, secondo cui tra le forze armate di uno Stato e quelle irregolari non dovrebbe essere nessuna differenza rispetto al grado di organizzazione richiesto. Cfr. *Official Records of the Diplomatic Conference on the Ratification and Development of International Humanitarian Law Applicable in Armed Conflicts*, Geneva (1974- 1977) (1978), vol. 8,204, par. 15.

[30] Nella specie si trattava del riconoscimento dello status di prigioniero di guerra e il governo statunitense ha affermato che «the Taliban lacked the kind of organization characteristic of the military. The fact that at any given time during the conflict the Taliban were organized into some structured organization does not answer whether the Taliban leaders were responsible for their subordinates within the meaning of GPW. Armed men who can be recruited from other units, as DoD states, through defections and bribery are not subject to a commander who can discipline his troops and enforce the laws of war». Cfr. Dipartimento della difesa statunitense, *Status of Taliban Forces under Article 4 of the Third Geneva Convention of 1949*, 7 febbraio 2002.

2.2. *Elementi distintivi riconoscibili a distanza e armi portate apertamente*

Il principio di distinzione, come anticipato, è una delle più rilevanti norme consuetudinarie del diritto internazionale umanitario[31]. Affinché tale norma venga rispettata è necessario altresì utilizzare degli elementi distintivi, tali da poter distinguere e individuare le parti durante un conflitto, e portare apertamente le armi. In questo modo dovrebbe essere più agevole per le parti dello scontro distinguere i combattenti durante un conflitto armato.

È evidente, tuttavia, che il principio *de quo* si riferisca ad un contesto bellico tradizionale – quello della Seconda guerra mondiale – ove le parti, effettivamente presenti sul campo di battaglia, avevano la possibilità di vedersi e distinguere visivamente i combattenti dai civili. A dire il vero, però, l'elemento relativo alla sussistenza di elementi distintivi non è scevro da critiche neppure se lo si analizza nel suo contesto originario. In primo luogo, infatti, non è facile comprendere la *ratio* per cui l'emblema distintivo debba essere sempre e necessariamente riconoscibile a distanza. Tale obbligo, invero, andrebbe interpretato in modo ragionevole: se infatti si pensa ai combattenti che cercano di rimanere in vita, è chiaro che questi non cercheranno di attirare l'attenzione su di sé, utilizzando invece indumenti capaci di favorirne il camuffamento. Si tratta di uno stratagemma di guerra lecito, a condizione che i combattenti si limitino a sfruttare le condizioni topografiche del campo di battaglia[32].

Un'altra criticità, poi, è rinvenibile se si pensa alle operazioni militari notturne. In questa ipotesi, infatti, appare quasi del tutto superfluo specificare che i combattenti non sono tenuti a portare un emblema distintivo illuminato che sia riconoscibile a distanza nel buio. Il punto centrale della questione, quindi, «is not whether combatants can be seen, but whether (if observed) they are likely to be mixed up with civilians»[33].

Un simile ragionamento può essere fatto anche rispetto alla necessità di *portare apertamente le armi*. Se ci si volesse limitare alla formulazione letterale della norma si dovrebbe giungere alla paradossale conclusione per cui un combattente non possa riporre le armi in una fondina o in una borsa in quanto non «portate apertamente». Il punto della questione, invece, è che il combattente dovrebbe portare le armi in modo ragionevole a seconda, anche, della natura dell'arma e dalle circostanze ambientali[34]. In altre parole, egli dovrebbe astenersi dal creare la falsa impressione di essere un civile.

Ciò detto, bisogna chiedersi se questi elementi possano essere rilevanti e di conseguenza rispettati anche da quei soggetti, come gli *hacker*, che agiscono nel contesto virtuale[35]. Innanzitutto, va sottolineato come il lancio di un attacco informatico, che per sua stessa natura avviene a distanza, difficilmente potrà dirsi compatibile con gli elementi sopra

---

[31] Cfr. J.M HENCKAERTS, L. DOSWALD-BECK (Eds.), *Customary International Humanitarian Law* ICRC, 2005, p. 3 ss.; Y. DINSTEIN, *The Principle of Distinction and Cyber War in International Armed Conflict*, in *Jour. Conf. Sec. Law*, 2012, p. 262 ss.

[32] Cfr. Y. DINSTEIN, *The Conduct of Hostilities under the Law of International Armed Conflict*, Cambridge, 2016, p. 53 ss.

[33] *Ibidem.*

[34] *Ibidem*, p. 54.

[35] Non manca in dottrina una certa letteratura che analizza, dalla prospettiva statale, la violazione del principio di distinzione attraverso l'utilizzo di armi cibernetiche. Si v., ad esempio, J. KELSEY, *Hacking into International Humitarian Law: The Principle of Distinction and Neutrality in the Age of Cyber Warfare*, in *Michigan Law Review*, 2008, p. 1436 ss., ove l'A. sostiene che gli Stati possono violare il principio in esame più frequentemente nel contesto digitale di quanto non accada in un campo di battaglia tradizionale dal momento che gli Stati utilizzano le armi cibernetiche per colpire sia persone che obiettivi civili.

descritti dal momento che l'esposizione aperta delle armi e l'utilizzo di uniformi in ogni caso non sarebbero visibili dalle altre parti coinvolte nel conflitto. Molto più che l'aspetto esteriore di un individuo o di un gruppo, il principio di distinzione nelle operazioni informatiche richiede una particolare attenzione alla condotta effettiva dell'attacco. A differenza degli attacchi convenzionali, in cui i difensori rispondono direttamente al combattente, le vittime degli attacchi informatici sono più propense a reagire tenendo in considerazione lo strumento o il metodo dell'attacco[36].

Nel contesto informatico, dunque, ciò che risulta rilevante è piuttosto il fatto che una persona possa lanciare un attacco informatico e deliberatamente decidere di falsificare l'indirizzo IP in modo da farlo apparire come appartenente al dominio di un utente civile. Riconoscere lo *status* di combattente a quest'ultimo vorrebbe dire ancora una volta violare la *ratio* dell'art. 4(2)(A), in quanto si finirebbe con l'identificare il soggetto civile come autore dell'attacco e, di conseguenza, farlo diventare il destinatario di un possibile contrattacco[37]. Allo stesso modo dovrebbe essere negato lo *status* di combattente a quei soggetti che lanciano un attacco di tipo DDoS intenzionalmente nascosti e mimetizzati tra le operazioni civili legittime, visto che questo metodo di attacco coinvolge gli utenti civili nell'operazione ostile e li mette a rischio di essere presi di mira[38].

Infine, appare opportuno notare che le operazioni informatiche il cui scopo è quello di inserire in modo nascosto un *software* malevolo nei sistemi e nelle reti informatiche (si pensi ad esempio ai casi di *Trojan Horse*) non precludono il conferimento dello *status* di combattente poiché il requisito di portare le armi apertamente non significa necessariamente che queste devono essere visibili.

In definitiva, dal momento che Anonymous ha utilizzato *software* di *spoofing* IP[39] come *The Onion Router* (Tor) per mascherare la vera fonte dei suoi attacchi informatici, creando l'impressione errata che provenissero da utenti civili, e che gli attacchi DDoS sono stati utilizzati anche per inondare i siti web bersaglio con richieste provenienti da decine di migliaia di computer civili, non si può ritenere che Anonymous abbia rispettato il principio di distinzione[40].

3. *L'applicabilità del concetto di levée en masse agli hacker*

Una volta verificata l'impossibilità di qualificare gli *hacker* come combattenti attraverso il prisma dell'art. 4(A)(2) della III Convenzione di Ginevra, bisogna chiedersi se tale *status* possa essere acquisito ricorrendo alla nozione di *levée en masse*. Prima di affrontare più nel

[36] Cfr. S. WATTS, *Combatants Status and Computer Network Attack*, in *Virg. J.. Int. Law*, 2010, p. 440 ss.
[37] *Ibidem*, p. 442.
[38] Cfr. R. BUCHAN, *Cyber Warfare and the Status of Anonymous,* cit., p. 752.
[39] In breve, la c.d. tecnica di *spoofing* dell'indirizzo IP consiste nel sostituire l'indirizzo IP del mittente nell'intestazione di un pacchetto IP con un indirizzo IP contraffatto. Tale tecnica ha due obiettivi principali: in primo luogo, mira a impersonare l'indirizzo IP da cui viene inviato il pacchetto, anonimizzando così il mittente. In secondo luogo, viene utilizzato per aggirare un sistema di filtraggio dei pacchetti (firewall), dando a un pacchetto un indirizzo IP che gli consente di essere inviato su una rete specifica. Per esempio, un pacchetto inviato da un computer esterno alla rete potrebbe avere l'indirizzo IP del mittente per sembrare che provenga dalla stessa rete del computer di destinazione e quindi non sarà bloccato dal firewall. Cfr. F. DELARUE, *Cyber Operations and International Law*, Cambridge, 2020, p. 67ss.
[40] Così R. BUCHAN, *Cyber Warfare and the Status of Anonymous,* cit., p. 752 ss.

dettaglio il problema relativo al *cyber warfare* però, appare necessario tratteggiare brevemente le principali caratteristiche di questo concetto.

Le origini della *levée en masse* risalgono al periodo della Rivoluzione francese del 1789[41] anche se un primo riconoscimento ufficiale si è avuto qualche anno dopo l'inizio della Rivoluzione. Più precisamente, attraverso un processo volto a valorizzare la figura del militare, rispetto a quanto non fosse stato fatto negli anni precedenti, con il decreto del 23 agosto 1793 si stabiliva che: «(…) from this moment until the enemies are driven out from the territory of the Republic, all Frenchmen are in permanent requisition for service in the army. Young people will go to combat; married men will forge weapons and transport supplies; women will make tents and clothes and serve in hospitals; children will shred old clothes; the elderly will get themselves carried to public squares in order to excite the courage of the warriors, to preach hate of the kings and unity of the Republic»[42].

Va precisato, tuttavia, che nella sua formulazione originaria il concetto di *levée en masse* assumeva connotazioni spiccatamente politiche piuttosto che giuridiche: l'obiettivo, infatti, era quello di coinvolgere il più ampio numero di individui al fine di difendere militarmente la nazione. Senonché, per un primo riconoscimento giuridico bisognerà aspettare il *Lieber Code* redatto da Francis Lieber durante la guerra civile americana. Si tratta di un codice composto da 157 articoli, avente ad oggetto le tematiche proprie del diritto di guerra quali, ad esempio, il trattamento dei civili, il riconoscimento dello *status* di prigioniero di guerra e alcune norme riguardanti le proprietà pubbliche e private del nemico[43].

Nel testo, agli art. 51 e 52, il concetto di *levée en masse* viene definito in questi termini: «[i]f the people of that portion of an invaded country which is not yet occupied by the enemy, or of the whole country, at the approach of a hostile army, rise, under a duly authorized levy "en masse" to resist the invader, they are now treated as public enemies, and, if captured, are prisoners of war. No belligerent has the right to declare that he will treat every captured man in arms of a levy "en masse" as a brigand or bandit. If, however, the people of a country, or any portion of the same, already occupied by an army, rise against it, they are violators of the laws of war, and are not entitled to their protection»[44]. Ulteriori riferimenti, poi, sono rinvenibili nella Dichiarazione di Bruxelles (1874)[45], nel Manuale di Oxford (1880)[46], nonché nella Convenzione dell'Aja del 1907[47]. La definizione riportata in questi ultimi è stata,

---

[41] Per una ricostruzione storica del concetto di *levée en masse* si rimanda a E. CRAWFORD, *Tracing the Historical and Legal Development of the Levée en Masse in the Law of Armed Conflict*, in *Jour. Hist. Int. Law*, 2017, p. 329 ss.

[42] Cfr. *Ibidem*, p. 334.

[43] *Ibidem*.

[44] *Instruction for the Government of Armies of United States in the Field (Lieber Code)*, 24 aprile 1863. Il testo è consultabile online all'indirizzo https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/110.

[45] Nella Dichiarazione, la *levée en masse* è definita come segue: «the population of a territory which has not been occupied, who, on the approach of the enemy, spontaneously take up arms to resist the invading troops without having has the time to organise themselves in accordance with Article 9, shall be regarded as belligerents if they respect the laws and customs of war». Cfr. P*roject of an International Declaration Concerning the Laws and Customs of War*, adottato in seno alla Conferenza di Bruxelles, 27 agosto 1874.

[46] L'art. 2 individua tra le forze armate di uno Stato anche «[t]he inhabitants of non-occupied territory, who, on the approach of the enemy, take up arms spontaneously and openly to resist the invading troops, even if they have not had time to organize themselves». Cfr. *The Laws of War on Land*, Oxford, 9 settembre 1880.

[47] Il Regolamento in questione si riferisce alla *levée en masse* in questi termini: « The inhabitants of a territory which has not been occupied, who, on the approach of the enemy, spontaneously take up arms to resist the invading troops without having had time to organize themselves in accordance with Article 1, shall be regarded as belligerents *if they carry arms openly* and if they respect the laws and customs of war» (corsivo aggiungo). Cfr. *Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land*, L'Aja, 18 ottobre 1907.

successivamente, ampiamente ripresa dalla Terza Convenzione di Ginevra, la quale risulta essere l'ultima Convenzione a conferire una qualificazione giuridica al concetto di *levée en masse*.

Più nel dettaglio, l'art. 4(A)(6) della Terza Convenzione di Ginevra riconosce lo *status* di prigioniero di guerra e, quindi, indirettamente quello di combattente alla «popolazione di un territorio non occupato che, all'avvicinarsi del nemico, prenda spontaneamente le armi per combattere le truppe d'invasione senza aver avuto il tempo di organizzarsi come forze armate regolari, purché porti apertamente le armi e rispetti le leggi e gli usi della guerra»[48].

Rispetto alla sua formulazione originaria, dunque, lo *status* di partecipante alla *levée en masse* è piuttosto limitato. Infatti, come sottolineato nel commentario alla III Convenzione di Ginevra, esso può sussistere solo per un breve periodo di tempo giacché soltanto in presenza dell'elemento della spontaneità sarà possibile utilizzare tale concetto; successivamente, se la *levée en masse* dovesse proseguire, gli individui che ne fanno parte saranno incorporati nella struttura militare dello Stato oppure saranno da questi ultimi sostituiti[49].

In virtù dell'elemento temporale, vanno esclusi come requisiti per riconoscere lo *status* di combattente ai partecipanti di una *levée en masse* sia la presenza di una struttura organizzata e diretta da un responsabile sia l'utilizzo di segni distintivi riconoscibili a distanza[50]. Risulterebbe particolarmente complesso, infatti, pensare che in un lasso di tempo così breve i partecipanti riescano ad organizzarsi in una struttura militare e riescano altresì ad indossare delle uniformi che li contraddistinguono. Per esclusione, dunque, l'elemento dirimente, al fine di attribuire lo *status* di combattente, è proprio quello relativo all'utilizzo delle armi in modo aperto; a ben vedere, infatti, è nell'interesse dei partecipanti alla *levée en masse* portare la armi in modo visibile al fine di essere riconoscibili e di conseguenza acquisire lo *status* di combattente[51].

Dopo aver delineato in termini generali il concetto di *levée en masse*, occorre chiedersi se questo possa avere una rilevanza giuridica nel *cyber warfare* e, di conseguenza, se possa essere utile per qualificare come combattenti coloro che operano in tale contesto digitale[52]. Sul punto ci sembra possano essere fatte tre considerazioni rispetto al collettivo Anonymous: due che portano ad escludere l'utilizzo del concetto in esame e una invece che va nella direzione contraria. Prendendo le mosse proprio da quest'ultimo punto, l'unico elemento che ci sembra applicabile è quello della "spontaneità". Come facilmente intuibile, questo presupposto indica che i partecipanti debbano decidere di agire spontaneamente, senza quindi vi sia stata una richiesta da parte di una delle parti in conflitto di agire a suo supporto. Se riprendiamo le condotte poste in essere da Anonymous si può dedurre che il collettivo abbia agito, almeno se si segue la filosofia che li ha sempre caratterizzati, in modo autonomo e spontaneo senza che vi sia stata alcuna coercizione o istigazione alla partecipazione da parte dell'Ucraina[53].

---

48 *Convenzione di Ginevra relativa al trattamento dei prigionieri di guerra*, Ginevra, 12 agosto 1949.

49 *Commentario alla III Convenzione di Ginevra relativa al trattamento dei prigionieri di guerra*, 1949, p. 68.

50 Cfr. D. WALLACE, S.R. REVEES, *The Law of Armed Conflict's "Wickel" Problem: Levée* en Masse *in Cyber Warfare*, in *International Law Studies*, 2013, p. 657 ss.

51 *Commentario*, cit. p. 68.

52 La letteratura sul punto è piuttosto scarna, tra i contributi più rilevanti si segnala C. WATERS, *New Hacktivists and the Old Concept of Levée En Masse*, in *Dalhousie Law Journal*, 2014, p. 772 ss.

53 Un interessante parallelismo è quello relativo al c.d. *Ukranian IT Army* e cioè alle vere e proprie forze armate informatiche che agiscono a sostegno dell'Ucraina per fronteggiare gli attacchi informatici russi. Per alcune brevi considerazioni sulla loro qualificazione giuridica si rimanda a R. BUCHAN, N. TSAGOURIAS, *Ukranian 'IT*

Escluso questo elemento, ostano all'applicazione del concetto di *levée en masse* al collettivo Anonymous le ulteriori due caratteristiche. In primo luogo, particolarmente complessa risulta essere l'applicabilità del concetto di territorio non occupato nel cyberspazio. Com'è noto, infatti, nello spazio digitale l'elemento territoriale assume una rilevanza particolarmente limitata. Uno dei fattori che ha contribuito allo sviluppo della *cyberwar* è in parte riconducibile proprio alla capacità di un individuo di organizzare efficacemente una campagna cibernetica, rimanendo al sicuro nell'anonimato da una località non rivelata. La posizione dell'attaccante cibernetico, l'infrastruttura digitale che trasmette l'attacco e l'obiettivo sono svincolati da un paradigma occupato/non occupato. La componente territoriale che aiuta a definire una *levée en masse*, e in particolare il fatto che la rivolta rimarrà limitata a un «territorio non occupato», non è quindi compatibile con la realtà della guerra cibernetica[54].

Infine, l'ultimo elemento che in definitiva ci porta ad escludere tale applicazione è quello relativo alla necessità di portare apertamente le armi. Come dimostrato in precedenza, questo requisito difficilmente potrà essere soddisfatto nel contesto informatico. Ciò appare ancor più vero se si considerano le attività poste in essere da Anonymous, le quali si sono sostanziate in operazioni tutte volte a celare l'utilizzo delle armi informatiche. Probabilmente l'unica ipotesi in cui si potrebbe giungere a conclusioni diverse potrebbe riguardare il caso in cui i membri della popolazione inizino spontaneamente a organizzare operazioni informatiche in risposta a un'invasione del loro Paese, senza aver avuto l'opportunità di organizzarsi in unità armate regolari e riuscendo a coinvolgere un cospicuo numero di cittadini con l'obiettivo di invadere *informaticamente* la controparte[55].

4. *La nozione di partecipazione diretta alle ostilità*

Esclusa anche la possibilità di qualificare il gruppo Anonymous come combattenti attraverso la nozione di *levée en masse* bisogna concludere che tali soggetti non possano essere bersaglio di attacchi e, qualora, catturati non potranno essere considerati come prigionieri di guerra. In altre parole, il gruppo Anonymous non può che essere qualificato come *civili*. A questo punto, dunque, non ci resta che analizzare se trattasi di *civili* che partecipano direttamente alle ostilità.

Il concetto di partecipazione diretta alle ostilità, nonostante sia espressamente previsto in diversi trattati internazionali, risulta essere piuttosto vago e poco chiaro[56]. Le norme che vi fanno riferimento, sebbene qualificate come diritto internazionale consuetudinario, infatti, si limitano ad affermare che «civilians shall enjoy the protection afforded by this Section,

---

Army': A Cyber Levée en Masse or Civilians Directly Participating in Hostilities?, in *Ejil:Talk*!, 9 marzo 2022, consultabile online all'indirizzo https://www.ejiltalk.org/ukranian-it-army-a-cyber-levee-en-masse-or-civiliansdirectly participating-in-hostilities/

[54] D. WALLACE, S.R. REVEES, *The Law of Armed Conflict's "Wickel" Problem*, cit., p. 660 ss.

[55] Cfr. M.N. SCHMITT (Eds.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017.

[56] Si v., tra gli altri, A. SILVESTRI, *The 'Revolving Door' of Direct Participation in Hostilities: A Way Forward*, in *Journal of International Humanitarian Legal Studies*, 2020, p. 410 ss.; M. LESH, *Direct Participation in Hostilities*, in R. LIVOJA, T. MCCORMACK (Eds.), *Routledge Handbook of the Law of Armed Conflict*, New York, 2016, p. 181 ss.; E. CHRISTENSEN, *The Dilemma of the Direct Participation in Hostilities*, in *Jour. Trans. Law Pol.*, 2010, p. 281 ss.

unless and for such time as they take a direct part in hostilities»[57]. Alle stesse conclusioni si giunge anche alla luce della (seppur limitata) giurisprudenza internazionale sul punto[58].

In ragione di tale vaghezza ed ambiguità, il Comitato della Croce Rossa Internazionale, sotto la supervisione del giurista Nils Melzer, ha condotto una ricerca della durata di sei anni al fine di chiarare le circostanze in base alle quali dei civili possano essere considerati quali diretti partecipanti alle ostilità. I risultati dello studio sono confluiti, nel 2009, nella *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (d'ora in poi, anche, Guida)[59], il cui scopo, in definitiva, è quello di chiarire la portata della nozione in esame, partendo proprio dalle norme di diritto internazionale umanitario esistenti[60].

Secondo la Guida, affinché possa parlarsi di partecipazione diretta, è necessario soddisfare simultaneamente tre requisiti:

> a) l'atto deve essere in grado di influenzare negativamente le operazioni militari o la capacità militare di una parte di un conflitto armato oppure, in alternativa, di infliggere morte, lesioni o distruzione a persone o oggetti protetti da un attacco diretto (c.d. *threshold of harm);*
>
> b) deve sussistere un nesso causale diretto tra l'atto e il danno derivante da quello specifico atto oppure da una operazione militare più ampia di cui quell'azione costituisce parte integrante (c.d. *direct causation*);
>
> c) l'atto deve essere specificamente progettato per essere a sostegno di una parte del conflitto e a danno dell'altra (c.d. *bellingerant nexus*)[61].

Nonostante gli intenti chiarificatori della Guida, non tutta la dottrina internazionalistica l'ha accolta con favore[62]. Alcuni autori, infatti, ritengono che essa adotterebbe un approccio

---

[57] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 8 giugno 1977, art. 51(3). Anche il II Protocollo utilizza pressoché la medesima formulazione; l'art. 13, par. 3, infatti, stabilisce che «Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities».

[58] « (…) to take a "direct" part in the hostilities means acts of war which by their nature or purpose are likely to cause actual harm to the personnel or matériel of the enemy armed forces», Cfr. Tribunale penale internazionale per la ex-Jugoslavia, 5 dicembre 2003, *Prosecutor v. Galic*, ricorso n. IT-98-29-T, par.48; «to take a direct part in hostilities means to engage in acts of war which, by their nature or purpose, are likely to cause actual harm to the personnel or matériel of the enemy armed forces. It submits moreover that while civilians are often used as part of a war effort, this does not turn them into legitimate military targets» Cfr. Tribunale penale internazionale per la ex-Jugoslavia 17 luglio 2008, *Prosecutor v. Strugar*, Camera d'appello, ricorso n. IT-01-41-A, par. 167.

[59] N. MELZER, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Ginevra, 2009.

[60] *Ibidem*, p. 6.

[61] Cfr. *Ibidem*., p. 46.

[62] In senso favorevole si sono espressi, tra gli altri, 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.; A. VAN ENGELAND, *Civilian or Combatant?: A Challenge for the 21st Century*, New York, 2011, p. 105 ss. In senso contrario, invece, si veda K. WATKIN, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, in *New York Journal of International Law and Policy*, 2010, p. 641 ss.; M.N. SCHMITT, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, in *New York Journal of International Law and Policy*, 2010, p. 697 ss.; ID, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, in *Harvard National Security Journal*, 2010, p. 5 ss.; W.H. BOOTHBY, *"And for Such Time As": The Time Dimension to Direct Participation in Hostilities*, in *New York Journal of International Law and Policy*, 2010, p. 741 ss.

eccessivamente restrittivo del concetto di partecipazione diretta alle ostilità[63], mentre per altri invece le conclusioni raggiunge risulterebbe per lo più dissonanti rispetto alla prassi militare degli Stati[64]. Ciononostante, va rilevato come la Guida negli anni successivi alla pubblicazione sia stata spesso utilizzata come punto di riferimento sia dagli Stati[65] sia in seno alle organizzazioni internazionali[66], diventando così una guida autoritativa del concetto di partecipazione diretta alle ostilità per l'intera comunità internazionale[67].

Ciò detto, e non essendo lo scopo di questo contributo analizzare la rilevanza giuridica della Guida, ci limiteremo ad utilizzare i risultati a cui perviene per verificare se la nozione di partecipazione diretta alle ostilità possa essere applicata al gruppo *Anonymous*[68]. Nei paragrafi successivi, dunque, si esaminerà se le attività condotte da Anonymous durante il conflitto internazionale tra Russia e Ucraina soddisfino i requisiti del *threshold of harm*, della *direct causation* e infine del *belligerent nexus*.

4.1. *Il c.d.* threshold of harm test *e la sua applicabilità ad Anonymous durante il conflitto russo-ucraino*

Iniziamo col chiederci se le condotte poste in essere nell'ambito *cyber*, durante il conflitto tra Russia e Ucraina, abbiano raggiunto la soglia del c.d. *threshold of harm* test, così come indicato dalla Guida.

Quest'ultima, come poc'anzi menzionato, individua due ipotesi alternative affinché sia raggiunta questa soglia. Per un verso è previsto che l'azione debba provocare un danno di natura militare ad una delle parti in conflitto; per altro verso, invece, è sufficiente che la condotta abbia come obiettivo persone e/o cose appartenenti a soggetti civili[69]. In quest'ultimo caso, inoltre, non è necessaria la effettiva realizzazione del danno ma è sufficiente l'*oggettiva probabilità* che quel comportamento possa causarlo[70].

Ora, rispetto all'ipotesi di danno militare, la Guida lo definisce come qualsiasi azione capace di influire negativamente sulle operazioni militari oppure, più in generale, sulla capacità militare di una delle parti in conflitto[71]; non è necessario quindi che la condotta provochi la morte di persone oppure distruzione di oggetti. A conferma di ciò, la stessa Guida afferma, facendo espresso riferimento al contesto digitale, che una ipotesti di operazione informatica capace di superare il *threshold of harm test* potrebbe realizzarsi nella «[e]lectronic

---

[63] In questi termini M.N. SCHMITT, *Deconstructing Direct Participation in Hostilities,* cit., p. 720.

[64] S. DARCY, *Direct Participations in Hostilities*, in *Oxford Bibliographies*, 2016. Più in generale per una ricostruzione della prassi in senso contrario a quanto affermato nella Guida si v. G. BARTOLINI, *Gli attacchi aerei in Siria, l'operazione "Inherent Resolve" e la complessa applicazione del diritto internazionale umanitario*, in *Dir. uomo. dir. int.*, 2017, p. 407 ss.

[65] J. MARSH, S. L. GLEBE, *Time for the United States to Directly Participate*, in *Virg. jour. Int. Law Online*, 2011, p. 20 ss.

[66] Per esempio, il Relatore Speciale dell'*UN Human Rights Council on extrajudicial, summary or arbitrary executions* nel suo rapporto sulle *killing targeted* utilizza la Guida come fonte principale in materia di diretta partecipazione alle ostilità. Cfr. P. ALSTON, *Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Study on Killing Targeted*, Human Rights Council, UN Doc A/HRC/14/24/Add.6, 2010, par. 62-69.

[67] J. MARSH, S. L. GLEBE, *Time for the United States to Directly Participate*, cit., p. 14.

[68] In termini più generali sull'applicazione della nozione di diretta partecipazione alle ostilità alla cyber war si veda D. TURNS, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, in *Jour. Conf. Sec. Law*, 2012, p. 278 ss.

[69] N. MELZER, *Interpretive Guidance,* cit., p. 47.

[70] *Ibidem.*

[71] *Ibidem.*

interference with military computer networks (…) whether through computer network attacks (CNA) or computer network exploitation (CNE), as well as wiretapping the adversary's high command or transmitting tactical targeting information for an attack»[72]. In altre parole, quindi, il danno militare si verificherebbe semplicemente attraverso una interferenza elettronica.

A ben vedere, però, oltre a questi minimi riferimenti, la Guida non aggiunge molto altro. Per questi motivi, ci sembra rilevante integrare la lettura della Guida con quanto previsto dal Manuale di Tallinn (d'ora in poi, anche Manuale) che, come ormai noto, prende ad esame anche gli aspetti relativi alle norme del diritto internazionale umanitario nel contesto *cyber*[73].

Il Manuale adotta un approccio parzialmente differente dalla Guida, dal momento che afferma «the act (or a closely related series of acts) must have the *intended* or actual effect of negatively affecting the adversary's military operations or capabilities, or inflicting death, physical harm, or material destruction on persons or objects protected against direct attack»[74]. In altre parole, il Manuale individua quale elemento determinante ai fini del *threshold of harm* test l'*intenzione* dei civili di voler arrecare un danno alle infrastrutture militari di una delle parti in conflitto, escludendo invece la necessità che vi sia un danno effettivo a tali infrastrutture. A nostro avviso, questa distinzione è di fondamentale importanza soprattutto se si ha riguardo alla natura, alle metodologie usate e all'impatto degli attacchi informatici. Solo per chiarire meglio quanto si sta dicendo si può riportare un breve esempio: si pensi all'ipotesi in cui un individuo o un'entità decida di lanciare un attacco informatico da uno Stato utilizzando come ausilio alle sue azioni alcuni *server* situati nel territorio di un secondo Stato al fine di influenzare negativamente le operazioni e le capacità militari di un avversario in un terzo Stato. Ipotizziamo che il proprietario dei *server* situati nel secondo Stato non intendesse partecipare all'attacco ma che in ogni caso i suoi *server* siano stati fondamentali per influenzare negativamente le operazioni e le capacità militari del terzo Stato. Se si seguisse esclusivamente quanto affermato nella Guida si finirebbe per giungere all'erronea conclusione per cui anche il soggetto situato nel secondo Stato dovrebbe essere considerato un diretto partecipante alle ostilità e di conseguenza diventare un possibile obiettivo di attacchi da parte del terzo Stato[75] (posto, chiaramente, che l'attacco abbia effettivamente influenzato le operazioni militari).

Ponendoci, invece, nella prospettiva del Manuale ci sembra invece si possa giungere a conclusioni parzialmente diverse. Prendendo sempre come ipotesi l'esempio formulato in precedenza, si potrebbe affermare che mancando l'elemento della intenzionalità i server/computer appartenenti ai soggetti del secondo Stato sarebbero esclusi dalla definizione di "partecipanti diretti" dal momento che questa riguarderebbe esclusivamente coloro che hanno "volontariamente" lanciato l'attacco con l'intento di influenzare le capacità militari del terzo Stato.

Ebbene, avendo riguardo alle condotte poste in essere da Anonymous a noi sembra che queste ultime possano aver raggiunto il requisito del *threshold of harm* per almeno due

---

[72] *Ibidem,* p. 48.

[73] Cfr. M.N. SCHMITT (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, 2017.

[74] Corsivo aggiunto, *Ibidem*, p. 429.

[75] È chiaro, comunque, che le eventuali reazioni dovranno comunque rispettare i principi di necessità e di proporzionalità previsti dal diritto internazionale umanitario. Su tale questione si veda, più diffusamente, E.T. JENSEN, *Unexpected Consequences From Knock-On Effects: A Different Standard for Computer Network Operations?*, in *Am. Un. Int. Law Rev.*, 2003, p. 1175, in cui l'A. suggerisce che gli stessi principi di necessità e proporzionalità applicabili nei conflitti tradizionali vadano utilizzati anche nel caso di operazioni informatiche.

ordini di ragioni. In primo luogo, e seguendo l'impostazione adottata dal Manuale, è indubbia l'intenzionalità di Anonymous di voler arrecare un danno alle forze militari russe che hanno invaso l'Ucraina. Ciò si evince dalle diverse dichiarazioni emanate dal Collettivo sia all'inizio del conflitto sia durante lo svolgimento delle ostilità[76]. Allo stesso modo, anche il requisito del danno *contro* i civili ci sembra soddisfatto, soprattutto se si considerano, da un lato, gli attacchi informatici contro la tv di Stato russa, sicuramente un servizio a disposizione dei civili, che ha avuto l'obiettivo di rendere noti ai cittadini le atrocità della guerra; e dall'altro lato il *defacement* dei siti internet appartenenti alle autorità governative russe.

4.2. *Il c.d.* direct causation test *e la sua applicabilità al gruppo Anonymous durante il conflitto russo-ucraino*

Come visto in precedenza, il requisito della *direct causation* si intende soddisfatto nel caso in cui vi sia un nesso di causalità tra la condotta posta in essere e il danno che da quel comportamento deriva oppure se, più in generale, quella condotta si inserisce in una operazione più ampia che ha determinato il danno.

Più nel dettaglio, una prima differenziazione va fatta proprio tra queste due diverse tipologie di condotte in quanto soltanto la prima soddisferebbe il requisito di un diretto collegamento tra il comportamento e il danno, mentre invece nel secondo caso saremmo dinanzi ad una ipotesi di un mero collegamento *indiretto* tra il fatto e le conseguenze.

Sul punto la Guida appare piuttosto chiara nel sottolineare la necessaria presenza di un nesso causale sufficientemente stretto tra il comportamento e il danno, escludendo invece che una semplice facilitazione possa rientrare nel concetto di partecipazione diretta alle ostilità[77]. In caso contrario, infatti, si finirebbe per privare gran parte della popolazione civile della protezione contro gli attacchi diretti accordatagli dalle norme del diritto internazionale umanitario[78]. In altre parole, la distinzione tra partecipazione diretta e indiretta alle ostilità deve intendersi sovrapponibile a quella tra causazione diretta e indiretta del danno.

Ciò detto, anche in questo caso ci sembra utile un parallelismo con quanto stabilito dal Manuale di Tallinn sul punto. A ben vedere, infatti, sia il Manuale sia la Guida sembrano concordare sul fatto che alcune attività civili possano soddisfare il requisito della diretta causalità[79]. Ad esempio, l'identificazione e la segnalazione di obiettivi, l'analisi e la trasmissione di informazioni tattiche alle forze d'attacco e l'istruzione e l'assistenza fornita alle truppe per l'esecuzione di un'operazione militare specifica, anche se condotta con mezzi informatici, soddisfano tutti il requisito della causalità diretta del danno, in virtù del legame causale diretto tra l'azione del civile e il danno che potrebbe derivare da una qualsiasi di queste azioni.

I civili che assistono le parti di un conflitto armato utilizzando strumenti informatici per identificare obiettivi sul campo o trasmettendo informazioni in tempo reale sulle capacità o sui movimenti della forza avversaria, pur non causando direttamente il danno, andrebbero comunque considerati come impegnati in una condotta che costituisce un elemento cruciale

---

[76] Cfr. M.B. PITRELLI, *Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia*, Cnbc, 28 luglio 2022, consultabile online all'indirizzo https://www.cnbc.com/2022/07/28/how-is-anonymous-attacking-russia-the-top-six-ways-ranked-.html.

[77] N. MELZER, *Interpretive Guidance,* cit., p. 52.

[78] *Ibidem.*

[79] Così C. ALLAN, *Direct Participation in the Hostilities from Cyberspace*, in *Virg. jour. Int. Law*, 2013, p. 186 ss.

per la corretta riuscita dell'atto ostile e quindi soddisfano il test di causalità diretta. In relazione ai civili che producono *malware* informatici poi, sebbene tale condotta sia normalmente considerata come causa indiretta di un danno, essa può eccezionalmente soddisfare il test di causalità diretta nel caso in cui il civile identifichi le vulnerabilità informatiche di un sistema o di una rete informatica specifica, quindi produca malware su misura e lo passi a un altro soggetto con la consapevolezza che sarà utilizzato in un attacco informatico[80].

Per quanto di nostro interesse, se prendiamo in considerazione una delle tipologie di operazioni lanciate da Anonymous e cioè gli attacchi c.d. DDoS contro i siti internet del Cremlino, del governo russo e del ministero della difesa, rendendoli inutilizzabili e irraggiungibili per un discreto periodo di tempo, probabilmente dovremmo giungere alla conclusione secondo cui anche il secondo *test* risulta soddisfatto. Tali attacchi infatti possono essere qualificati come l'arma preferita da coloro che cercano di danneggiare un avversario nel cyberspazio e sono stati ampiamente utilizzati dai membri di Anonymous sia nel conflitto in corso sia avverso i siti web israeliani nel 2014. Sul punto il Manuale non lascia alcun dubbio dal momento che afferma come gli attacchi DDoS rappresentino un esempio *inequivocabile* di un attacco informatico che causa direttamente un danno e quindi soddisfa la soglia di causalità diretta[81]. Il motivo è ravvisabile nel fatto che una volta che si venga a creare una rete sufficientemente ampia di computer compromessi, è sufficiente toccare un tasto del computer per istruire/comandare la *botnet* e attaccare il sito web bersaglio con richieste di informazioni e causare il danno richiesto.

4.3. *Il c.d.* belligerent nexus test *e la sua applicabilità al gruppo Anonymous durante il conflitto russo-ucraino*

L'ultimo elemento da analizzare è quello relativo al c.d. *belligerent nexus*. Affinché tale requisito sia soddisfatto è necessario che le condotte siano così strettamente collegate al conflitto armato da diventarne parte integrante[82] e quindi la condotta deve essere a sostegno di una delle parti del conflitto. Lo scopo di questa previsione è quello di evitare che talune attività dei civili possano essere impropriamente qualificate come partecipazione diretta nel caso in cui, in realtà, tali azioni non fanno in alcun modo parte del conflitto. Si pensi a titolo esemplificativo a quelle ipotesi in cui dei civili, approfittando della situazione di *caos* derivante del conflitto, compiano dei reati quali distruzione di negozi oppure furti negli appartamenti; in questi casi tali condotte non possono configurarsi come partecipazione diretta dal momento che non sono, appunto, strettamente collegate al conflitto internazionale.

Va rilevato, tuttavia, che a differenza della Guida il Manuale adotta un approccio meno stringente sul punto. Secondo il Manuale, infatti, tale requisito può dirsi soddisfatto semplicemente se la condotta in questione abbia un "diretto collegamento" con le ostilità[83],

[80] Cfr. R. BUCHAN, *Cyber Warfare and the Status of Anonymous,* cit., p. 763.
[81] Il Manuale alla regola 97, par. 6 stabilisce che «Other unambiguous examples include gathering information on enemy operations by cyber means and passing it to one's own State's armed forces and conducting DDoS operations against enemy military external systems»; cfr. M. N. SCHMITT (Ed.), *Tallinn Manual*, cit., p. 430.
[82] N. MELZER, *Interpretative Guidance*, cit., p. 58.
[83] Cfr. M.N. SCHMITT (Ed.), *Tallinn Manual*, cit., p. 430.

senza che sia necessario dimostrare come il comportamento sia a vantaggio di una delle due parti del conflitto e a svantaggio dell'altra[84].

Ciò detto, le condotte di Anonymous, come visto in precedenza, hanno avuto ad oggetto essenzialmente la sottrazione di una ingente quantità di dati dalla banca centrale russa e la successiva pubblicazione; l'individuazione di dati sensibili (data di nascita, indirizzi, unità di appartenenza) di più di centomila soldati russi; l'intromissione nei canali tv russi al fine di mostrare le atrocità del conflitto agli abitanti, aggirando in questo modo la censura di Stato[85].

Ebbene, a noi sembra che tali condotte possano senz'altro ritenersi collegate al conflitto in corso e le diverse dichiarazioni pubbliche rilasciate, attraverso i social, da Anonymous in merito alle sue intenzioni di iniziare una *cyberwar* contro la Russia depongano proprio in questo senso. Così facendo, quindi, se si prendesse ad esame il solo Manuale di Tallinn si giungerebbe alla conclusione per cui anche il requisito del c.d. *belligerent nexus* sia soddisfatto.

Senonché, se ci si pone nell'ottica della Guida abbiamo visto come sia altresì necessario dimostrare che tali comportamenti debbano essere a svantaggio di una delle due parti del conflitto. A ben vedere, le azioni realizzate da Anonymous ci sembrano senza dubbio *contro* il governo russo dal momento che tutte hanno avuto come bersaglio siti governativi, televisioni, banche, *database* militari appartenenti alla Stato russo. D'altro canto, se tali comportamenti siano o meno effettivamente a sostegno dell'Ucraina resta incerto; al momento non vi sono dichiarazioni ufficiali a sostegno del governo ucraino, ma allo stesso tempo va rilevato che in nessun caso il gruppo ha affermato che tali comportamenti sono autonomi ed indipendenti dal conflitto in corso. In definitiva, non può escludersi che le azioni di Anonymous, da un lato, siano a danno della Russia e, dall'altro lato, a favore quantomeno della popolazione civile ucraina.

5. *Sintesi della ricerca condotta*

L'analisi condotta nei paragrafi precedenti ha messo in luce alcuni fattori problematici relativi alla qualificazione degli attori non statali che, attraverso l'utilizzo di strumenti informatici, prendono parte ad un conflitto armato internazionale. Se da un lato, infatti, il diritto internazionale umanitario continua a fornire alcuni elementi utili per agevolare questo processo, dall'altro lato bisogna riconoscere che le norme di riferimento risentono fortemente del contesto storico in cui sono state ideate ed emanate. Ciò comporta, inevitabilmente, talune difficoltà circa la loro concreta applicabilità ai nuovi scenari bellici che si stanno profilando negli ultimi anni. Come visto, infatti, l'applicazione dell'art. 4 (A) della Terza Convenzione di Ginevra, seppur astrattamente possibile nel contesto cibernetico, mal si concilia con lo scenario bellico attuale, non permettendo in alcun modo di qualificare il

[84] Così C. ALLAN, *Direct Participation in the Hostilities from Cyberspace*, cit., p. 189 ss.

[85] P. PAGANINI, *Anonymous leaked 28GB of data stolen from the Central Bank of Russia*, in *Security Affairs*, 25 marzo 2022, consultabile online all'indirizzo https://securityaffairs.co/wordpress/129490/hacking/central-bank-of-russia-data-leak-anonymous.html. Per una breve analisi tecnica in merito agli attacchi informatici di Anonymous a danno della Russia e sulla veridicità della loro attribuzione al gruppo si veda J. FLOWER, *Hacker Group Anonymous and Others Targeting Russian Data*, in *Websiteplanet*, consultabile online all'indirizzo https://www.websiteplanet.com/blog/cyberwarfare-ukraine-anonymous.

Collettivo Anonymous alla stregua di "combattenti". E ciò a causa soprattutto delle condizioni particolarmente anacronistiche richieste dalla norma.

Esclusa, quindi, questa possibilità, e definiti i membri di Anonymous come "civili", ci siamo chiesti se si potesse utilizzare il concetto di "partecipazione diretta alle ostilità". Sul punto sono emersi due aspetti: in primo luogo, anche in questo caso, la semplice lettura della norma coadiuvata dalla Guida interpretativa del Comitato della Croce Rossa non è sempre sufficiente; in secondo luogo, ci sembra che un ausilio interpretativo rilevante sia offerto dal Manuale di Tallinn, il quale, pur prendendo le mosse dalla Guida stessa, in più di una circostanza ha agevolato la qualificazione giuridica degli *hacker* che decidono di prendere parte ad un conflitto armato.