Presupposti per la configurazione e la dichiarazione di guerra cibernetica*

di Andrea Gatti e Matteo Giannelli

Abstract: *Prerequisites for the configuration and declaration of cyber warfare* - The emergence of "unconventional" methods used to wage war raises the question of whether and how it is appropriate to determine a regulatory framework in order to identify jus ad bellum rules in cyberspace. The present essay aims to outline similarities and differences between traditional and cyberwarfare, to draw the line between legitimate and illegitimate cyberwarfare and to suggest some solutions.

Keywords: Cyberwar; Cybersecurity; Pacifist principle; Constitution; International organisations.

1. "Le parole sono importanti"

Karl von Clausewitz nel primo libro del suo "Della Guerra" ci ricorda una verità ancora molto attuale: che le guerre non contengono in sé un confine[1], e che dunque esiste un primato della politica interna per cui è lo Stato-sovrano a determinare come entrare in guerra e come condurla. Si sposa l'idea che la possibilità di porre linee rosse su un piano internazionale nello *ius in bellum* appartiene più al voler essere che alla realtà, con la quale è necessario sempre misurarsi.

Ma la stessa espressione può ben essere riconducibile anche al campo proprio dello *ius ad bellum*, quando cioè sia possibile affermare con certezza la legittimità di entrare in guerra? La natura concreta della guerra quale drammatica espressione di un'esigenza rende più difficile, ma non per questo meno utile, una sua definizione a livello giuridico che ne condizioni l'assetto e le scelte politiche interne[2].

Le riflessioni tra "Stati" e "guerre" si collocano, quindi, nell'ambito di questa problematica generale e, senza la presunzione di sviluppare nuovi modelli o concezioni, esse intendono contribuire al più ampio dibattito sui

* Il presente saggio è frutto delle riflessioni tra i due autori; ciononostante i paragrafi 2, 5 e 6 sono attribuibili ad Andrea Gatti, e i paragrafi 3 e 4 a Matteo Giannelli; la stesura dei paragrafi 1 e 7 ad entrambi.

[1] K. von Clausewitz, *Della guerra*, Milano, 2005, 19 ss.

[2] Per C. Schmitt, *Inter pacem et bellum nihil medium* (1939), in Id., *L'unità del mondo e altri saggi*, Roma, 1994, 199-200, «tutti i tentativi di dare una definizione della guerra debbono finire in un puro giudizio del tutto soggettivo e volontaristico».

DPCE online
ISSN: 2037-6677

collegamenti interno/esterno, del loro ambito di influenza e di possibili limitazioni.

Due dei tre più recenti conflitti che hanno interessato la geopolitica globale, quello in Ucraina e quello in Nagorno Karabakh, sono esemplificativi dell'esigenza testé enunciata: definiti dagli aggressori "operazioni militari speciali", tali scontri – che pure si inseriscono a tutti gli effetti nell'alveo dell'idea di guerra – fissano gli attori statuali in una situazione di incertezza che impedisce risposte chiare ed efficienti.

Ma i conflitti armati dell'era post-bipolare e multipolare contengono ulteriori elementi di complessità rispetto a quelli tradizionali: implicano la presenza di attori non statuali, l'impossibilità di definire un campo di battaglia a fronte di uno scenario complesso e globale, il problema di definire apertamente obiettivi precisi e, da ultimo, l'impiego di strumenti non convenzionali (guerra ibrida)[3] che proiettano gli scontri su un piano pluridimensionale. È questo il caso della guerra informatica che – dal caso *Stuxnet*[4] in poi – viene portata avanti, più che in tutte le altre dimensioni, in assenza di un quadro definitorio chiaro: mancano, ad esempio, una chiara definizione di responsabilità degli attacchi o anche solo un criterio che assicuri la riconducibilità degli attacchi agli Stati, una definizione di *contractor* o *cyberwarrior*, ma soprattutto dei parametri universalmente riconosciuti che possano legittimare gli Stati a scendere in guerra dopo un attacco informatico.

L'anonimato degli attaccanti, il tipo di armi (immateriali), l'estensione della superficie d'attacco (cioè il "terreno" in cui in conflitto si svolge), così come il tipo di attacco che sfrutta la pervasività e l'interconnessione delle tecnologie di informazione e comunicazione nell'ecosistema digitale, rendono il cyberspazio – cioè della quinta dimensione dello spazio, per riprendere ed estendere la nota tassonomia di Schmitt[5] – un ambiente particolarmente adatto a perpetuare l'ambigua forma giuridica della conflittualità del Terzo millennio [6] e, allo stesso tempo, a massimizzare i danni che possono essere arrecati all'avversario, senza con ciò rischiare di essere trascinati in un conflitto[7]. La drammaticità della situazione non emerge soltanto dagli enormi danni economici per le infrastrutture strategiche statali derivanti da questa situazione di *Far West* digitale – danni

[3] Si fa riferimento al concetto di guerra ibrida per descrivere le situazioni belliche caratterizzate dall'impiego simultaneo e sullo stesso campo di battaglia di armi convenzionali, informatiche e propaganda, (cfr. A. Mumford, P. Carlucci, *Hybrid warfare: The continuation of ambiguity by other means*, in *European Journal of International Security*, 8, 2023, 192-206.

[4] Su questo attacco, volto a interrompere lo sviluppo del programma nucleare iraniano, cfr., *ex multis*, M.E. O'Connell, *Cyber security without cyber war*, in *Journal of Conflict and Security Law*, 2/2012, 187 ss., spec. 194, anche per una panoramica degli episodi coevi, e P.W. Singer, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, in *Case Western Reserve Journal of International Law*, 47, 2015, 79 ss.

[5] C. Schmitt, *Il Nomos della terra nel diritto internazionale dello «Jus publicum europaeum»*, Milano, 1991.

[6] L. Martino, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, 1/2018, 63.

[7] Come si afferma nella National Security Strategy del 2017, elaborata dal Dipartimento della Difesa americano, «Le nuove tecnologie cambieranno la società e, in definitiva, il carattere della guerra».

che per natura, gravità, sistematicità e dimensione travalicano costantemente i confini delle tecnologie dell'informazione e della stessa cybersicurezza – ma anche e soprattutto per l'aumento esponenziale di attacchi diffusi, molti dei quali di natura para-militare[8], frutto delle tensioni internazionali tra superpotenze e del conflitto ad alta intensità combattuto ai confini dell'Europa. In questa dimensione, che solo una rappresentazione illusoria e consolatoria può ritenere meramente virtuale[9], emerge la grande problematicità e attualità di un fenomeno che, come già accennato, costituisce la più recente, ma certamente non l'ultima, evoluzione di un campo di battaglia che vede affiancarsi a grandi e piccoli potenze soggetti nuovi, non sempre, anzi raramente, statali.

La cyberguerra è ormai parte integrante della guerra ibrida ed è lecito interrogarsi sull'inopportuna mancanza di un testo scritto condiviso nella comunità internazionale o almeno in Occidente, che prenda in considerazione specificamente la guerra informatica valorizzando adeguatamente la portata assunta dalla Carta ONU, dei Patti internazionali sui diritti dell'uomo nonché sulle altre numerosissime convenzioni e dichiarazioni di principi dell'attuale ordinamento giuridico internazionale. Ad oggi le regole convenzionali del *cyberwarfare*, non ordinate in sistema e di controverso accertamento in quanto non scritte in carte che esplicitamente e globalmente le riconoscono, non riescono ancora a trovare riscontri nella realtà e dunque a svolgere pienamente il loro compito[10].

Il primo obiettivo del presente scritto è pertanto quello di provare a delineare le condizioni entro cui un cyberattacco può essere considerato un atto di guerra in violazione del diritto sui conflitti armati (*Law of armed conflict* - LOAC) e qualora questa operazione sia possibile, in una prospettiva deontica, provare a ipotizzare possibili rimedi.

Il secondo obiettivo consiste nel leggere i risultati così raggiunti, da una parte, alla luce della disciplina costituzionale italiana al fine di valutarne o meno la compatibilità con l'intero impianto costituzionale che vede la sua norma cardine nel principio del ripudio della guerra sancito dall'articolo 11 della Costituzione; dall'altra, alla luce delle linee guida di alcuni importanti

[8] Ad oggi il 2023 è stato l'anno peggiore di sempre in termini di evoluzione delle minacce *cyber* e dei relativi impatti. Ce lo dicono gli indicatori sui costi degli attacchi alla sicurezza. Nel 2020 i danni globali per gli attacchi *cyber* ammontavano a 1 trilione di dollari. Già nel 2022 la cifra era aumentata a 6 trilioni e, secondo le stime, si prevedono perdite per il 2023 fino a 8 trilioni di dollari e fino a 10 trilioni per il 2025. Nel 2022 in Italia sono andati a segno 188 attacchi gravi (+169%), l'83% dei quali di gravità elevata o critica. I dati reali sono sicuramente ancora meno rassicuranti, in quanto molte vittime non comunicano le violazioni subite. Secondo uno studio della Commissione europea nell'Unione ogni 11 secondi un'infrastruttura europea subisce un attacco *ransomware*, quindi un attacco *hacker* specificamente finalizzato alla criptazione e al furto dei suoi dati (cfr. *State of the Union: New EU cybersecurity rules ensure more secure hardware and software products*, *online* su www.ec.europa.eu). Di questi attacchi circa il 20% è riconducibile alla guerra fredda informatica in corso.

[9] Cfr., di recente, S. Pietropaoli, *Informatica criminale. Diritto e sicurezza nell'era digitale*, Torino, 2022, 49-51.

[10] Cfr. D. Mauri, *"Aggiornamento disponibile": nuove tecnologie, uso della forza e diritto internazionale*, in T. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Milano, 2021, 191 ss.

DPCE online
ISSN: 2037-6677

Stati del blocco occidentale (Francia, Germania, Gran Bretagna e Stati Uniti), provando così ad accennare alcune linee di collegamento e di differenziazione.

Si illustrerà infine una proposta pratica che valorizzi la disciplina comune e il collegamento organico tra gli attori internazionali.

Preso atto che lo spazio cibernetico non costituisce una nuova dimensione della conflittualità ma una dimensione trasversale e pervasiva alle quattro già conosciute (terra, mare, cielo e spazio extra-atmosferico), si spera che una riflessione su questi tre profili possa contribuire alla definizione di un tema ineludibile, se è vero che ci troviamo di fronte ad un fenomeno che sembra sempre di più la «guerra del futuro»[11] ma che, allo stesso tempo, rimane guerra a tutti gli effetti.

2. L'accertamento dello *jus ad bellum* "analogico"

La sovranità richiede di delineare un confine che ne attesti il perimetro di validità, che attesti cioè fin dove si spinge l'autorità del soggetto politico statuale che la esercita[12]. Il diritto internazionale non ignora questo problema. L'art. 2, § 4 della Carta ONU proibisce agli Stati di utilizzare la forza contro altri Stati, con l'eccezione dei casi di autodifesa e a condizione che sia presente come fattore di legittimazione una risoluzione del Consiglio di Sicurezza (delle Nazioni Unite)[13]. La sua violazione è il fattore di giustificazione del "diritto naturale di autotutela individuale o collettiva", sancito dall'art. 51 della medesima Carta. Sebbene il concetto di "uso della forza" non sia definito puntualmente da un punto di vista giuridico, tradizionalmente esso si riconduce ad un atto di violenza armata che un membro della comunità internazionale spiega nei confronti un altro per distruggerne la forza o piegarne la volontà[14]. Ciò avviene, da un punto di vista materiale o oggettivo, sempre attraverso un comportamento che violi il principio di non ingerenza nella sfera territoriale di un'altra entità sovrana. Abbiamo usato l'avverbio "tradizionalmente" perché la storia ci mostra in

[11] Così ancora, U. Gori, *Evoluzione e prospettive delle minacce e della conflittualità nello spazio cibernetico*, in U. Gori, D. Vernon de Mars (a cura di), *Cyber Warfare 2019-2020. Dall'evoluzione della Warfare alla resilienza al Covid-19*, Milano, 2021, 24, per il quale saranno decisivi una serie di fattori: «economicità, invisibilità, anonimato, attivazione da qualsiasi distanza e in qualsiasi momento (24 h/g, 7 gg/settimana), azione alla velocità della luce, bersagli molteplici, civili e militari, neutralizzazione dell'avversario senza distruzione delle sue forze e senza spargimento di sangue (o quasi), fruibilità anche da parte di entità sub-nazionali».

[12] Cfr. anche quanto esposto da V.E. Parsi, *Il posto della Guerra*, Milano, 2022, 47.

[13] "*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*".

[14] Cfr. A. Curti Gialdino, *Guerra* (voce), in *Enc. Dir.*, Milano, 1970, 850. G. Ferrari, *Guerra (Stato di)*, in *Enc. Dir.*, XIX, Roma, 1970, 831; G. Balladore Pallieri, *Diritto Bellico*, Padova, 1954, 14 ss. Definizione che si ricava anche da recenti documenti quale l'*International Law and Cyberspace Report* (febbraio 2021), 16 ss, in particolare "*the Italian Position on International Law and Cyberspace*" 8-9. E il Department of Defence, *Law of War Manual*, 2016. Sull'espressione di monopolio della forza legittima, v. M. Weber, *La politica come professione*, in ID., *Economia e società. Teoria delle categorie sociologiche*, Torino, 1999.

realtà non poche eccezioni: innanzitutto la c.d. "guerra al terrorismo" ha permesso che la controparte degli Stati fossero anche soggetti privi della statualità; in secondo luogo che una guerra contro una comunità di tipo statuale potessero potesse essere generata proprio a partire dall'azione di questi gruppi non statuali[15], ragione per cui la riferibilità allo Stato come parte del conflitto può rivelarsi in realtà indiretta o mediata[16]. Ciò, come vedremo rappresenta un aspetto importante in riferimento ad atti di forza informatici, nelle cui caratteristiche troviamo l'anonimato e la difficile riconduzione ad una fonte.

Atto di guerra, ci dice ancora la dottrina internazionalistica e costituzionalistica, deve poi essere considerata quell'azione sorretta dall'esternalizzazione di un certo *animus bellandi* nell'aggressore, fattore che esclude sia le aggressioni accidentali o circostanziate, come le rappresaglie, sia le misure di autotutela che assumono sì forma giuridica di azioni armate (arresto e detenzione degli equipaggi, cattura di navi, ecc.), ma da cui non può provarsi nessuna intenzione di instaurare uno stato di guerra[17].

Altri criteri ormai consolidati di carattere oggettivo, enucleati anch'essi attraverso la prassi del diritto internazionale, si ritrovano nelle numerose codificazioni o consolidazioni che sono sorte in questi anni, su tutti il manuale guerra del Pentagono che per ragioni autoevidenti costituisce un punto di riferimento per le prassi internazionali; ci riferiamo in particolare al principio di proporzionalità in caso di guerra di risposta ad un attacco armato, laddove tale attacco abbia comportato danni a persone o infrastrutture strategiche.

Benché la Carta ONU sia stata scritta in un momento ben anteriore alla nascita del cyberspazio, esiste un generale consenso sulla sua applicabilità anche in questo nuovo contesto.

3. Cosa è atto di guerra nel cyberspazio?

Per verificare se un attacco *cyber* può considerarsi un atto di guerra in senso proprio – e quindi se permette una risposta militare legittima – va a propria volta verificato come si inseriscono gli attacchi cibernetici nei parametri normativi anzidetti, cioè se tali parametri vadano semplicemente reinterpretati o se invece si rende necessario integrarli con componenti ulteriori.

[15] La prima operazione bellica "di risposta" in tal senso, cioè la prima a rompere il nesso tra aggressione di uno Stato ad un altro, risale al primo conflitto mondiale, quando la Serbia fu accusata di avere dato protezione al gruppo terrorista indipendentista responsabile dell'uccisione del Granduca Francesco Ferdinando. In questa categoria possiamo inserire anche l'operazione del 2001 in Afganistan, ritenuto belligerante perché, proprio come la Serbia, aveva dato rifugio a un'organizzazione terroristica. Sull'Afghanistan, C. De Fiores, *L'intervento militare in Afghanistan. Profili di diritto costituzionale interno e internazionale*, in *Politica del Diritto*, XXXIII, 2002, 79-110,

[16] Lo notava già G. de Vergottini, *Guerra e Costituzione. Nuovi conflitti e sfide della democrazia*, Bologna, 2004, 79.

[17] G. Ferrari, *Guerra* (*stato di*) (voce), in *Enciclopedia del diritto*, XIX, Milano, 1970, 821.

DPCE online
ISSN: 2037-6677

A tal fine è utile ricondurci al c.d. Manuale di Tallin, ritenuto la fonte più autorevole per definire le regole del *cyber warfare*[18]; in particolare i punti numero 10 e 11. Il punto n. 10 afferma che un'operazione cibernetica che costituisce «una minaccia o l'uso della forza contro l'integrità territoriale o l'indipendenza politica di uno Stato o che è in ogni caso in contraddizione con i fini delle Nazioni Unite, è illecita». Il punto 11 definisce in cosa consiste l'«uso della forza»: «quando la sua portata e i suoi effetti (*its scale and effects*) sono comparabili con un'operazione bellica non cibernetica» e ciò significa che tali attacchi debbano provocare rilevanti danni alla proprietà o la morte di cittadini[19]. La gravità si misura dunque per analogia con i precedenti conflitti.

Si potrebbe dunque parlare al proposito di "dottrina degli effetti": sono dunque gli effetti e non l'atto di forza informatica in sé a rilevare come causa di legittimazione per una eventuale risposta bellica[20]. In mancanza di parametri astratti condivisi si può concludere che tali effetti dovrebbero essere analoghi a quelli provocati in un precedente conflitto "analogico".

Accanto a questi criteri ne vanno aggiunti altri: quello per cui gli attacchi informatici siano attribuibili, tramite prove o solide presunzioni, ad un altro Stato.

La ricostruzione che si condivide, dunque, definisce il rapporto tra gli attacchi informatici e la guerra cibernetica come una relazione simile a quella tra genere e specie[21]. In entrambi questi fenomeni, esistono due obiettivi comuni: disturbare o distruggere le operazioni di una rete e perseguire finalità politiche o di sicurezza nazionale. Tuttavia, la guerra cibernetica si distingue per la presenza di un ulteriore elemento: il suo potenziale di causare effetti simili a quelli prodotti da un attacco convenzionale, anche attraverso l'interferenza con sistemi con i quali si gestiscono le infrastrutture critiche, ad esempio sanitarie, in società tecnologicamente avanzate.

La dottrina è arrivata alla conclusione che un atto di guerra nel mondo digitale vada considerato in chiave analogica rispetto ad un atto di guerra nel mondo reale: si può dunque ipotizzare che sia ravvisabile un "uso della forza" che sia considerabile come atto di guerra laddove ci siano danni fisici a persone e, se gravi, anche a cose[22]. Non può rilevare invece la sola invasione del territorio (violazione di un sistema), dal momento che lo spazio cibernetico è fluido e la prassi ha già mostrato numerosi attacchi incrociati.

---

[18] Il Manuale di Tallin è, come noto, frutto di un processo di elaborazione, da parte di un gruppo di esperti (accademici e militari), che ha la sua origine nell'attacco sferrato nel 2007 a danno di infrastrutture governative e d'informazione estone (la cd. Web War One). Ne esistono due versioni pubblicate da Cambridge University Press: la prima rilasciata nel 2013, la seconda nel 2017 (v. *infra* nota 25).

[19] Questo concetto è stato utilizzato anche dalla Corte di Giustizia internazionale nel caso Nicaragua (§195).

[20] Sul punto, anche per ulteriori riferimenti, M. Mirti, *Il cyberspace. Caratteri e riflessi sulla Comunità Internazionale*, Napoli, 2012, 220-2.

[21] M. Matassa, *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, Milano, 2023, 24-26.

[22] U.S. Army (*join publication*), *Cyberspace Operation 3-12* (luglio 2018), Manuale Guerra Pentagono (Cyberattacchi).

A tal proposito, non è possibile ignorare la circostanza che la realtà della guerra ibrida ha alimentato il ricorso alla nozione di autodifesa[23].

Si può citare come esempio il Comunicato della NATO adottato a Bruxelles nel giugno 2021, che afferma chiaramente che gli attacchi informatici possono essere considerati attacchi armati e far scattare l'art. 5 della Trattato[24]. In questo campo, sta emergendo una nuova prassi secondo la quale gli Stati terzi avrebbero il diritto di adottare contromisure nei confronti degli Stati responsabili di tali attacchi ibridi, il che si discosta chiaramente dal diritto tradizionale della responsabilità dello Stato

dal diritto tradizionale della responsabilità dello Stato[25].

Dunque, le tradizionali regole internazionali su come e fino a che punto si può usare la forza sono costantemente messe in discussione nel mondo interconnesso di oggi.

4. Sulla compatibilità della guerra cibernetica con l'impianto costituzionale italiano

Le difficoltà di trovare una definizione unica e condivisa vanno valutate non solo nel contesto internazionale ma anche in quello costituzionale. Ciò deve avvenire non solo alla luce del contenuto dell'articolo 11 della Costituzione, in particolare dell'interpretazione che può esser data alla formula costituzionale del «ripudio della guerra», ma anche con riferimento alla cd. "Costituzione della difesa"[26] cristallizzata dall'articolo 52 Cost. in termini di

[23] Si veda la Rule 71 (Self-defence against armed attack) del Manuale di Tallin in cui si afferma che «*A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects*».

[24] Cfr. Brussels Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, Press Release (2021) 086, disponibile al link https://www.nato.int/cps/en/natohq/news_185000.htm, spec. par. 32 «*Reaffirming NATO's defensive mandate, the Alliance is determined to employ the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, in accordance with international law. We reaffirm that a decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis. Allies recognise that the impact of significant malicious cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack. We remain committed to act in accordance with international law, including the UN Charter, international humanitarian law, and international human rights law as applicable. We will promote a free, open, peaceful, and secure cyberspace, and further pursue efforts to enhance stability and reduce the risk of conflict by supporting international law and voluntary norms of responsible state behaviour in cyberspace*».

[25] Cfr. Manuale di Tallinn 2.0, 2017, (*Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*) regola 24, par. 5 e seguenti. In dottrina per tutti M. Dawidowicz, T*hird-Party Countermeasures in International Law*, Cambridge, 2017, 111 ss.

[26] Una formula che presenta non poche incertezze di carattere definitorio. Sul punto, si vedano in particolare le riflessioni sviluppate dopo l'intervento militare nella ex-Jugoslavia del 1999, da G. De Vergottini, *Profili costituzionali della gestione delle emergenze*, in *Rassegna parlamentare*, 2001, 275 ss., e P. Carnevale, *Il ruolo del parlamento e l'assetto dei rapporti fra camere e governo nella gestione dei conflitti armati. Riflessioni alla*

DPCE online
ISSN: 2037-6677

«dovere di difesa della patria». Come vedremo, anche nel contesto cibernetico l'articolo 52 si pone quale complemento al ripudio della guerra contenuto nell'articolo 11, innanzitutto sotto il profilo della sicurezza nazionale, delle sue dimensioni e dei modi per realizzarla e garantirla.

L'esigenza di fondo di questa impostazione si traduce nel passare da quelle che sono le definizioni contenute in codificazioni private – ad esempio il già citato Manuale di Tallin – ai testi costituzionali. Ciò significa percorrere la strada di un'interpretazione evolutiva delle disposizioni *ivi* contenute, a partire dal concetto di guerra, prendendo atto che la Costituzione non "ingessa" la tecnologia nella norma giuridica[27].

La dottrina concorda sul fatto che l'articolo 11 consente la guerra in difesa del territorio nazionale e vieta le guerre di aggressione[28]. Oltre tale nucleo, nel corso della storia repubblicana si è sviluppato un ricco, talvolta aspro (che non è possibile ripercorrere in questa sede), dibattito, sulla ricca casistica che si collocano tra questi due estremi e, in primo luogo, sulla natura e sull'inquadramento costituzionale dei sistemi di difesa collettiva, come la NATO, e sulla nozione soccorso difensivo.

La guerra cibernetica, dunque, è "guerra" ai sensi dell'articolo 11? Fino ad oggi, ci si è basati principalmente sui criteri del diritto internazionale, senza tuttavia essere sufficientemente critici nei loro confronti. Un simile atteggiamento può essere rivisto, anche a seguito della giurisprudenza della Corte costituzionale italiana, che ha affermato la prevalenza dei principi supremi dell'ordinamento costituzionale persino sul diritto internazionale consuetudinario[29].

La difficoltà di definire una "dottrina costituzionale" italiana per la partecipazione alla guerra cibernetica emerge anche nel *position paper* sull'applicabilità del diritto internazionale allo spazio cibernetico redatto su iniziativa del Ministero degli Affari Esteri assieme alla Presidenza del Consiglio dei ministri, e al Ministero della Difesa e trasmesso al Gruppo di Esperti Governativi delle Nazioni Unite nel novembre 2021[30].

Si tratta di un testo che affronta molti temi e, in particolare, la sovranità nello spazio cibernetico, la responsabilità degli Stati, l'uso della forza.

Tra i punti centrali del documento vi è la sottolineatura che il diritto internazionale, cristallizzatosi nel corso dei secoli ben prima della creazione dell'ambiente digitale, lungi dall'essere superato da questo, ne costituisce la necessaria ossatura. Risulterebbe quanto meno contraddittorio che i principi

---

luce delle prassi seguite in occasione delle crisi internazionali del Golfo persico, Kosovo e Afghanistan, in *Diritto e società*, 2003, 103 ss., che, pur muovendo da impostazioni diverse, ruotano attorno al medesimo problema.

[27] Sul punto in termini generali v. S. Mannoni, *Potenza e ragione. La scienza del diritto internazionale nella crisi dell'equilibrio europeo (1870-1914)*, Milano, 1999.

[28] Per tutti L. Carlassare, *L'art. 11 nella visione dei costituenti*, Costituzionalismo, 2013, 1 ss.

[29] È il caso della notissima sentenza n. 238 del 2014 della Corte costituzionale, su cui ex multis, E. Lamarque, *La Corte costituzionale ha voluto dimostrare di sapere anche mordere*, in *Questione Giustizia*, 2015, 76 ss.

[30] Il documento è consultabile al link https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

e le regole – che hanno disciplinato i rapporti fra gli Stati per secoli – possano non applicarsi agli stessi rapporti, quando avvengono in un diverso ambiente. Così, per esempio, i principi che regolano la soluzione pacifica delle controversie internazionali o gli obblighi in materia di rispetto dei diritti umani non possono ignorati perché uno Stato agisce online, invece che nell'ambiente analogico dove essi sono stati riconosciuti da tempo, come già acquisiti dallo *ius gentium*.

I capitoli del *paper* dedicati al diritto internazionale umanitario ribadiscono, infatti, il divieto dell'uso della forza, anche nel contesto cibernetico, e hanno l'obiettivo di replicare nello spazio cibernetico, le tutele e le limitazioni che sono state faticosamente individuate nel corso dei secoli[31].

Stupisce che nel documento non ci sia spazio per considerazioni in punto di diritto costituzionale. Un tema che emerge con forza se si considera che l'attività di difesa cibernetica non può limitarsi a una mera attività di presidio ma deve assumere anche un ruolo attivo. In un tale panorama diventa importante sviluppare una capacità di difesa cibernetica attiva, «ossia proattivamente difensiva, tesa a sviluppare le vulnerabilità altrui (cd. *exploitation*) per un eventuale contrattacco nello spazio cibernetico»[32].

La difesa dello Stato come funzione inderogabile, infatti, riguarda non soltanto i confini, ma anche la sicurezza interna e internazionale se si considera che le minacce da prevenire e contrastare possono giungere da soggetti e luoghi diversi[33]. Nella società tecnologica, gli Stati devono proteggersi da influenze nascoste che operano in un ambito spesso sfuggente al controllo e privo di forma fisica, ovvero nello spazio virtuale al quale possono accedere attori sia ufficiali che non ufficiali.

In un simile contesto sembra potersi realizzare una nuova dimensione del dovere sancito dall'articolo 52 della Costituzione perché la Patria «non si deve difendere dal nemico alle porte ma da un algoritmo attivato da un click»[34].

La guerra cibernetica, intesa come un'azione condotta attraverso l'uso di strumenti cibernetici per condurre operazioni militari offensive attraverso il danneggiamento di reti, sistemi o infrastrutture digitali di un'altra nazione, risulta incompatibile con l'articolo 11. Si tratterebbe di una finalità

[31] Si tratta di un punto di difficile tematizzazione come messo ben in evidenza, con riferimento al drone warfare, da F. Ruschi, *Il diritto, la guerra e la «tecnica scatenata». Considerazioni sul* drone warfare, in Id., R. Campione, *Guerra, diritto e sicurezza nelle relazioni internazionali*, Torino, 2019, spec. 60 ss. a proposito del «diritto umanitario nell'età della guerra dis-umana».

[32] Così R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in Id., *La sicurezza nel cyberspazio*, cit., 16, che richiama Documento conclusivo dell'*Indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico* della Camera dei deputati del 2017 (approvato dalla Commissione Difesa nella seduta del 21 dicembre) dove si legge «mentre la difesa cibernetica in senso stretto (*cyber defence* o *cyber security*) comprende misure di separazione fisica o di protezione (reti autonome, *firewall*, antivirus) e protocolli di sicurezza (procedure, modi di fare), la difesa proattiva (*active cyber defence*) – primo grado verso le capacità di *exploitation* (sondare restando invisibili) e di attacco (produrre danni) nello spazio cibernetico – implica un'interazione attiva con l'esterno per proteggere la propria rete» (pag. 30).

[33] P. Bonetti, *Difesa dello Stato e potere*, in M. Cartabia, M. Ruotolo (a cura di), *Enciclopedia del diritto. I tematici. V. Potere e Diritto*, 2023, 69-72.

[34] R. Ursi, *Editoriale. La difesa: tradizione e innovazione*, in *Diritto costituzionale*, 2022, 20.

DPCE online
ISSN: 2037-6677

radicalmente opposta alla costruzione di un ordinamento che assicuri la pace e la giustizia tra le nazioni. Tuttavia, la difesa cibernetica, cioè l'uso di misure cibernetiche per proteggere l'integrità e la sicurezza nazionale, potrebbe essere compatibile con un simile impianto, ovviamente se funzionale a garantire i valori dell'articolo 11 in più ampio quadro di difesa dello Stato.

5. Spunti comparati sull'interpretazione dell'uso legittimo della forza

Se spostiamo il nostro sguardo sul panorama di diritto comparato, restando all'interno dell'omogenea categoria della tradizione giuridica occidentale, notiamo come tutti i Paesi riconoscano implicitamente o esplicitamente il principio della portata e i suoi effetti (*its scale and effects*) dell'attacco. Alcuni di questi Paesi – sia perché più esposti di altri ad attacchi per via del loro ruolo strategico negli equilibri geopolitici mondiali, sia semplicemente perché più attenti a meglio definire le minacce – hanno elaborato, nel solco dei criteri del diritto internazionale, delle proprie posizioni sulla possibilità di applicazione del diritto internazionale nel cyberspazio, cercando di enucleare dalle due variabili generali su menzionate (la portata e gli effetti degli attacchi) alcuni elementi utili alla loro determinazione.

Tra questi Paesi vanno in particolare menzionati Francia, Germania, Gran Bretagna, Australia e Stati Uniti. Una ricognizione comparata delle dichiarazioni riconducibili a tali Stati, ci mostra che in tali variabili sono da ricomprendersi: (a) nella diversa origine dell'operazione e la natura dell'istigatore (se militare o meno); (b) nell'entità dell'intrusione e/o la gravità dell'attacco; (c) negli effetti reali o perseguiti dell'operazione: ad esempio, il (diretto) ferimento o la morte di una persona fisica permette di ravvisare senz'altro l'uso della forza; (d) l'immediatezza degli effetti; (e) la natura degli obiettivi dell'attacco (ad esempio un'infrastruttura militare o il sistema di difesa nazionale)[35]. Tutte queste variabili sono riconosciute da tutti questi Paesi come capaci di integrare, alla luce del diritto internazionale,

[35] Cfr. per la Francia, *International Law Applied to Operations in Cyberspace* (https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf), per la Germania, *Cyber Security as a Dimension of Security Policy - Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London* (https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832), per la Gran Bretagna, *UK Attorney General's speech at the International Institute for Strategic Studies*, 11 gennaio 2017 (https://www.justsecurity.org/36171/read-speech-uk-attorney-general-force-imminence-international-law/), per l'Australia, *Australia's International Cyber Engagement Strategy* (https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf). Per gli Stati Uniti, *Law of War Manual* (https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF), ma anche, per la sua interpretazione, H.H. Koh, Legal Adviser Department of State, *Speech at the U.S. Cyber Command Inter-Agency Legal Conference on the applicability of international law to cyberspace*, 18 settembre 2012 (http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/).

un uso illegittimo della forza e, pertanto, di giustificare una risposta proporzionata.

All'interno di questo uniforme schema generale, alcuni Stati hanno anche presentato degli esempi su ciò che essi ritengono un uso della forza nel cyberspazio. Da tali esempi emergono le diverse sensibilità dei Paesi che le hanno elaborati. Ad esempio, la Gran Bretagna riserva un'importanza superiore alle altre esperienze statuali al criterio dell'imminenza dell'attacco come condizione che integra la necessità dell'autodifesa[36]; sulla stessa linea, in Francia, integra l'uso della forza nel cyberspazio anche il semplice addestramento di individui nella cyberguerra[37], previsioni che rispecchia e traduce sul piano del diritto internazionale la loro tradizionale sensibilità nella lotta preventiva al terrorismo.

In Australia, per contro, può integrare un uso della forza solo il danneggiamento o la distruzione di un oggetto[38] (un server, ad esempio), mentre per lo Stato francese può essere considerata uso della forza anche un'azione che non comporta una diretta ripercussione sul mondo fisico. In quest'ultimo caso, per la Francia ciò può valere se l'obiettivo perseguito dall'attacco sia un'infrastruttura militare o il sistema statale difesa (così anche per gli Stati Uniti)[39], ma anche se l'attacco abbia un serio impatto per la stabilità economica o finanziaria francese[40].

[36] *UK Attorney General's speech*, dove si individuano ulteriori 5 criteri: (a) The nature and immediacy of the threat; (b) The probability of an attack; (c) Whether the anticipated attack is part of a concerted pattern of continuing armed activity; (d) The likely scale of the attack and the injury, loss or damage likely to result therefrom in the absence of mitigating action; and (e) The likelihood that there will be other opportunities to undertake effective action in self-defense that may be expected to cause less serious collateral injury, loss or damage.

[37] *International Law Applied to Operations in Cyberspace*, cit., 4.

[38] *Cyber Engagement Strategy*, cit., 90.

[39] *Law of War Manual*, cit. 1029.

[40] *International Law Applied to Operations in Cyberspace*, cit., 3-4.

DPCE online
ISSN: 2037-6677

Gli Stati Uniti considerano l'uso della forza anche l'interferenza con il funzionamento di un reattore nucleare, la disabilitazione dei sistemi di controllo del traffico aereo (con conseguente perdita di vite umane) e l'apertura di una diga sopra un'area popolata (con la sua conseguente distruzione)[41]. Oltre all'attacco ad un reattore nucleare (con conseguente perdita diffusa di vite umane), Germania e Gran Bretagna ritengono che sia rilevante anche qualsiasi interruzione dei servizi medici essenziali che produca la morte di persone, in ciò evidenziando, forse più che negli Stati Uniti, la prospettiva personalistica tipicamente europea.

6. Pensare ad un'autorità internazionale in materia di cybersicurezza

La parziale disomogeneità delle possibili risposte agli attacchi anche all'interno del blocco di Paesi che condivide la stessa sensibilità (se non addirittura tradizione) giuridica e il carattere necessariamente transfrontaliero della guerra cibernetica impone di converso una riflessione che vada oltre l'ambiente nazionale, che parta dalla consapevolezza che le condizioni della competizione geopolitica sono mutate e le minacce sono accelerate dalla tecnologia[42]. In questo quadro, l'assenza di una cornice definitoria chiara rappresenta una enorme lacuna e debolezza nei confronti degli eccessi della sovranità e della logica di potenza.

Per prevenirne la sua forza, dirompente e "tragica" [43], dobbiamo quindi chiederci se nel cyberspazio sia possibile costruire una reale nozione di difesa comune, superando quella vocazione libertaria dello spazio virtuale che non consente i paradigmi dello Stato sovrano e regolatore, diventando espressione di poteri privati in totale assenza di «legittimazione da investiture statali o di istituzioni sovranazionali»[44].

In ambito europeo, sul punto risulta interessante la Direttiva NIS2 che armonizza le norme applicabili nel settore della gestione del rischio di cybersicurezza e della segnalazione di incidenti[45]. Tra i punti cardine di questa nuova regolazione vi è l'istituzione di una rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) per sostenere la gestione coordinata di incidenti e crisi di cybersicurezza su vasta scala e la garanzia del regolare scambio di informazioni tra gli Stati membri e le istituzioni dell'UE.

---

[41] *Law of War Manual*, cit., 1028-1029.
[42] Secondo la proposta di metodo della «digital constellation» avanzata, nel solco della riflessione intorno al costituzionalismo globale, da I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, in *Global Constitutionalism*, 2018, 112 ss.
[43] Di «tragedia della politica di potenza» parla J.J. Mearsheimer, *La tragedia delle grandi potenze*, Roma, 2019.
[44] Così S. Mannoni, G. Stazi, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, Napoli, 2021, 24.
[45] Cfr. https://digital-strategy.ec.europa.eu/it/policies/nis2-directive. Più in generale, si v. Commissione europea, *Joint communication to the European Parliamento and the Council - The EU's Cybersecurity Strategy for the Digital Decade*, 2020, online su https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164.

L'obiettivo primario dovrebbe consistere nel porre misure di sicurezza o nel rispondere in maniera tempestiva e coordinata ad ogni tipo di attacco informatico, dunque in teoria anche quelli propri di un'aggressione militare. Alla base del sistema stanno ovviamente gli obblighi di scambio di informazione, di gestione condivisa e di segnalazione dei rischi alla cybersicurezza stabiliti dalla Direttiva per i soggetti nazionali che rientrano nel suo ambito di applicazione (art. 21). Dunque, è a livello nazionale che le autorità competenti (per l'Italia, l'Agenzia nazionale per la cybersicurezza - ACN) decidono ed eseguono gli interventi necessari. Manca però a livello europeo un nucleo centralizzato esecutivo.

Anche nell'esperienza statunitense, con riferimento alla cybersicurezza propria della dimensione, diciamo così, "privatistica", esistono già enti certificatori tecnici come il *National Institute for Standard and Technologies* (NIST), una sorta di ente certificatore tecnici (il cui omologo manca in Europa), il cui obiettivo consiste nel definire un primo quadro istituzionalizzato della cyberguerra.

Nondimeno ancora nulla, in Europa o negli Stati Uniti, è stato teorizzato nel campo della cyberguerra.

Sulla scorta dell'idea promossa recentemente in campo civile sulla creazione di un *taskforce* di controllo dell'IA in senso all'ONU[46], ci pare ragionevole, in virtù del carattere transfrontaliero della minaccia, adottare una soluzione simile, o persino più avanzata, anche per la cyberguerra: pensare cioè ad un organo politico collegiale dotato di poteri di controllo, regolatori e, alla bisogna, anche coercitivi, un'organizzazione che sia finalizzata dunque tanto alla ricerca e alla standardizzazione globale delle minacce (e dunque alla creazione di una cornice giuridica entro cui categorizzarle), quanto alla loro risoluzione. Questa sorta di sistema di gestione della sicurezza comune – che avrebbe il merito di provare a risolvere la vera sfida (mai raggiunta) del diritto internazionale, vale a dire raggiungere l'ordine nella pluralità – potrebbe affiancare le Nazioni Unite per compiti di contenimento e gestione dello *ius ad bellum* informatico[47]. Diciamo "affiancare" e non "inserirsi" perché l'autorità a cui pensiamo avrebbe compiti parzialmente diversi da quelli dell'ONU: non sarebbe preordinato a stabilire la pace, ma solo i confini della guerra cibernetica.

L'applicazione pratica di questa idea incontra certamente delle difficoltà sia, ovviamente, di ordine politico – che tuttavia non interessano in questa sede - sia legate al funzionamento concreto di questo ente e dunque, in primo luogo, alla sua dimensione organizzativa.

Il prima problema pratico consiste nello stabilire la natura e i compiti di questo ente. Per quanto riguarda la natura, esso accomunerebbe quella di organo politico, in quanto composto da rappresentanti degli Stati, e quella di organo tecnico, con un proprio sistema di ricerca teorica, di sviluppo applicativo e realizzazione di prodotti di difesa, ma anche con propri dipartimenti che istruiscano gli affari. Per quanto riguarda i suoi compiti,

[46] V. dichiarazioni del Segretario Generale dell'ONU António Gutierrez, 18 luglio 2023, online su www.onuitalia.it.

[47] Sul ruolo delle Nazioni unite nel processo di rilevazione e definizione delle problematiche del cyberspace cfr. M. Mirti, *Il cyberspace. Caratteri e riflessi sulla Comunità Internazionale*, cit., 85 ss.

DPCE online
ISSN: 2037-6677

questi risiederebbero nell'indirizzo (precedente all'attacco bellico di natura informatica) e nel controllo (preventivo e successivo al verificarsi di un fatto). Si tratta di compiti che rischiano di trovare un difficile applicazione per via dei diversi sistemi delle fonti e prima ancora per la struttura stessa del diritto internazionale le cui caratteristiche strutturali impongono una volontaria cooperazione tra gli Stati, in continua tensione tra l'applicazione, da una parte, del principio di sovranità e una sua rinuncia, dall'altra del principio di legalità e il riconoscimento della peculiarità delle fonti nella dimensione transazionale come è quella digitale[48].

Queste tensioni richiederebbero così di affrontare un secondo problema che riguarda la struttura e si articola in due sotto-problemi.

Da una parte l'organizzazione proposta, per acquisire legittimità, dovrebbe assumere la forma di un organo collegiale e plurisoggettivo, nel senso che ai componenti, operando simultaneamente riuniti per il perseguimento di una finalità comune (*unitas actus*), deve essere affidato anche un potere deliberativo. Dall'altra parte, però, all'interno dell'ente dovrebbe essere prevista necessariamente la presenza di un organo esecutivo che esprima una posizione di primazia[49], una coordinazione che si astragga, almeno formalmente, dalle dinamiche statuali e che rappresenti, secondo una logica di massima indipendenza, gli interessi generali della comunità internazionale, vale a dire i suoi scopi.

7. Desecretare e riconoscere il conflitto?

Siamo oggi di fronte ad una situazione internazionale che riprende, per molti versi, quella presente a seguito della pace di Vestfalia (non a caso quest'ultima considerata la "pietra angolare del sistema moderno delle relazioni fra gli Stati")[50], quando la coesistenza di una pluralità di Stati e la politica di potenza di ciascuno di essi cessa di essere limitata e sottoposta ad una autorità superiore, sovrastatuale (l'imperatore), ma solto all'autorità degli altri Stati, cioè ad un potere che opera tra Stati.

La crisi dello *jus publicum europaeum* iniziata con la Prima guerra mondiale[51] e l'attuale crisi dello *jus gentium*, sono crisi in primo luogo dei limiti e richiedono nuove forme di neutralizzazione del conflitto, di limitazione all'esterno da un sistema di equilibrio sulla base di un codice comune, vale a dire sulla base di una definizione dei confini della pace e della guerra.

La sfuggevolezza della guerra informatica può aiutare a scongiurare il conflitto, perché può nascondere l'identità (e quindi le responsabilità) dell'attaccante o gli eventuali danni causati. Tuttavia, un tale modo di procedere rischia di aumentare la conflittualità, poiché pone gli attori statuali in un costante stato di guerra fredda. La definizione di parametri condivisi a

[48] Sul punto R. Bordari, *Diritto sovranazionale punitivo come sistema*, Padova, 2007.
[49] Per una ricognizione sulla nozione di primazia nel diritto pubblico, G. Pepe, *La primazia negli organi pubblici collegiali*, Napoli, 2014, spec. 21 ss.
[50] G. Poggi, *La vicenda dello Stato moderno*, Bologna, Il Mulino, 1978, 136. Sulle difficoltà del paradigma vestfaliano nel contesto del cyberspazio v. S. Mannoni, G. Stazi, *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*, cit., 24.
[51] P. Portinaro, *La crisi dello* jus publicum europaeum, Milano, 1982.

livello globale e di un'organizzazione interstatale che ne garantisca il rispetto, può essere un primo passo per neutralizzare questa nuova minaccia.

Andrea Gatti
Dip.to di Scienze Politiche
Università di Teramo
agatti@unite.it

Matteo Giannelli
Dip.to di Scienze Giuridiche
Università di Firenze
matteo.giannelli@unifi.it

DPCE online
ISSN: 2037-6677