Dottorato di ricerca in Ordine internazionale e diritti umani, Sapienza, Università di Roma - Intercenter, Università di Messina

Ordine internazionale e diritti umani

International Legal Order and Human Rights
Ordenamiento Jurídico Internacional y Derechos Humanos
Ordre juridique international et Droits de l'Homme

PATRICIO IGNACIO BARBIROTTO*

LE DICHIARAZIONI DI OXFORD SULLE CYBEROPERAZIONI E IL DIRITTO INTERNAZIONALE: SVILUPPI RECENTI

1. *Introduzione*

Nell'ultimo decennio l'aumento dell'uso dei mezzi informatici da parte degli Stati come strumento per interferire con gli interessi e negli affari interni di altri Stati (o anche nelle attività delle organizzazioni internazionali), ha rappresentato un elemento dirompente, che pone agli Stati un'enorme sfida e richiede all'intera comunità internazionale un importante sforzo nel tentativo di regolare e di governare tali attività nel quadro delle relazioni internazionali. Il presente lavoro esplora le prospettive per lo sviluppo del diritto internazionale nel cyberspazio, uno "spazio" che ha acquisito sempre più rilevanza negli affari pubblici e privati, con particolare attenzione a quelle operazioni che presentano profili di illiceità. L'analisi parte dalla definizione di quanto previsto dal diritto internazionale per quanto riguarda gli atti illeciti da parte degli Stati in termini classici, vale a dire non portati a termine sul cyberspazio, concentrandosi però su quelle aree che, come si vedrà in seguito, sono rilevanti anche in un quadro di eventuali operazioni di cyberwarfare. Il paragrafo successivo è dedicato a definire, attraverso alcuni dei casi più rilevanti verificatisi negli ultimi anni, ciò che caratterizza gli atti illeciti da parte degli Stati portati a termine mediante operazioni cibernetiche, cosa hanno in comune con gli atti illeciti di tipo tradizionale

* Cultore della materia in Diritto internazionale presso il Dipartimento di Economia dell'Università Ca' Foscari di Venezia, docente a contratto di Immigrazione e Diritti Umani presso il medesimo Ateneo.

commessi dagli Stati e cosa li rende invece unici. I paragrafi secondo e terzo vengono poi messi in relazione nel quarto paragrafo esaminando come alcuni soggetti del diritto internazionale, in questo caso gli Stati e le organizzazioni internazionali, abbiano preso in esame alcune operazioni cibernetiche illecite compiute da parte degli Stati. Sulla base di quanto detto nel quarto paragrafo, il successivo paragrafo prende in considerazione una serie di strumenti ad *hoc,* sviluppati come strumento di assistenza agli Stati, alle organizzazioni internazionali e all'intera comunità internazionale nell'approcciare le operazioni cibernetiche illecite, o che comunque possono risultare tali, in termini di diritto internazionale. Tali strumenti sono il manuale di Tallinn 2.0, presentato brevemente, e le cinque "Dichiarazioni di Oxford", frutto del cosiddetto "*Oxford Process*" redatte nel 2020 le prime tre e nel 2021 (pochi mesi or sono) la quarta e la quinta[1] a cui faremo riferimento nel lavoro. Segue un paragrafo che sposta l'attenzione dal livello internazionale a quello italiano, esaminando brevemente con quali strumenti l'Italia si prepara ad affrontare le minacce provenienti dal cyberspazio. Infine, l'ultimo paragrafo è dedicato alle conclusioni tratte dall'analisi, offrendo alcune riflessioni e spunti per la ricerca futura.

2. *Atti inamichevoli, atti illeciti e diritto internazionale*

Per considerare illecito un atto compiuto da uno Stato e, di conseguenza, invocare la responsabilità dello Stato che lo ha compiuto, lo Stato o l'organizzazione internazionale che lo subisce deve tenere conto di due elementi fondamentali[2]: in primo luogo, l'atto in questione deve essere attribuito ad un altro Stato; in secondo luogo, tale atto deve violare una norma o un principio di diritto internazionale[3]. Poggiando su tali condizioni sono numerosi gli atti che possono costituire illecito internazionale: mentre per quanto concerne gli atti illeciti in generale si rimanda alla vastissima trattazione della materia da parte della dottrina, nel presente lavoro ci si focalizzerà su un limitato numero di particolari illeciti che

[1] Durante la pandemia Covid-19 nel 2020 l'Università di Oxford, insieme ad alcune istituzioni partner, ha riunito virtualmente un vasto gruppo di esperti giuridici internazionali, che ha rilasciato tre dichiarazioni su questioni urgenti:la dichiarazione di Oxford sulla protezione giuridica internazionale contro le operazioni informatiche che mirate al settore sanitario (al sito https://www.elac.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea, consultato il 14 dicembre 2021), la seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini(al sito https://elac.web.ox.ac.uk/article/the-second-oxford-statement, consultato il 14 dicembre 2021), la Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali (al sito https://www.elac.ox.ac.uk/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through#/ , consultato il 14 dicembre 2021), la Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazione (al sito https://www.elac.ox.ac.uk/the-oxford-statement-on-the-regulation-of-information-operations-and-activities#/ , consultato il 14 dicembre 2021) e la Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : la regolamentazione delle operazioni di ransomware (al sito https://www.elac.ox.ac.uk/the-oxford-statement-on-ransomware-operations, consultato il 14 dicembre 2021). V. *infra* par. 5.

[2] Art. 2 del Progetto di articoli sulla responsabilità dello Stato della commissione del diritto internazionale delle Nazioni Unite, al sito https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (consultato il 14 dicembre 2021).

[3] Cfr. tra i molti D. CARREAU, F. MARRELLA, *Diritto Internazionale*, III ed., Milano, 2021, pp. 554-644; N. RONZITTI, *Diritto internazionale*, VI ed.., Torino, , 2019, pp. 399-434 ; R. MONACO, C. CURTI GIALDINO, *Manuale di diritto internazionale pubblico*, III. ed., Torino, 2009, pp. 623-716; M. SCHMITT (Gen. Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cybewarfare*, Londra, 2017, pp. 79-167 ; F. SALERNO, *Diritto Internazionale*, V ed., Milano, 2019, pp. 477-544 .

sono rilevanti trasportati dal contesto tradizionale al contesto delle operazioni cibernetiche[4]. A tal proposito, sarà utile fare riferimento come punto di partenza a fattispecie esistenti prima della comparsa sulla scena delle cyberoperazioni e ai relativi principi e norme di diritto internazionale applicabili a tali fattispecie[5].

Il principale atto illecito considerato è la violazione della sovranità di uno Stato, che avverrebbe, per quanto di interesse per il presente lavoro, tramite atti cibernetici. Nel mondo *offline* il precedente più significativo resta il lodo arbitrale sull'isola di Palmas reso da Max Huber nel 1928[6]. Nel lodo, l'arbitro ha definito la sovranità dello Stato come segue: "la sovranità nei rapporti tra Stati significa indipendenza. L'indipendenza in relazione ad una parte del globo è il diritto di esercitare, escludendo qualsiasi altro Stato, le funzioni dello Stato"[7]. Ne consegue che gli atti che violano l'integrità territoriale di uno Stato nonché gli atti che non consentono allo Stato vittima di svolgere correttamente le funzioni proprie dello Stato sul proprio territorio siano da considerarsi atti illeciti in violazione della regola del rispetto della sovranità statale.

Una seconda possibile violazione del diritto internazionale rilevante per le operazioni cibernetiche è la violazione del divieto di intervento. Tale principio è logicamente correlato al rispetto della sovranità di Stato, come indicato nella sentenza della Corte Internazionale di Giustizia (in seguito: CIG) sulle attività militari e paramilitari in e contro il Nicaragua[8] dove il concetto di intervento va a includere sia gli atti coercitivi compiuti sul territorio di un altro Stato (quindi interessanti la sovranità territoriale) sia gli atti coercitivi che interferiscono con tutte le questioni in cui lo Stato è libero di prendere decisioni sovrane[9]. Entrambi gli aspetti trovano le loro basi nell'art. 2 della Carta delle Nazioni Unite[10], e se il primo aspetto può essere collegato a quanto è stato detto in precedenza sulla violazione della sovranità, il secondo aspetto del principio di non intervento è meglio definito dall'idea di non interferenza negli affari, sia interni che esterni, di un altro Stato.

3.*Cyberoperazioni, l'elemento più dirompente delle relazioni internazionali nel XXI secolo*

Le norme e i principi del diritto internazionale inerenti gli illeciti internazionali si sono evolute nel quadro di atti condotti in modo che potrebbe essere definito "tradizionale", in

[4] N. TSAGOURIAS, R. BUCHAN (EDS.), *Research Handbook on International Law and Cyberspace*, Cheltenham UK & Northampton, MA, USA, 2015.

[5] In merito all'estensione delle fattispecie del mondo fisico e del relativo diritto applicabile al cyberspazio si veda J. D'ASPREMONT, *Cyber Operations and International Law: An Interventionist Legal Thought*, *in Journal of Conflict and Security Law*, vol.21(3), 2016, pp. 575–593.

[6] Lodo Arbitrale sul *Caso dell'Isola di Palmas* (Paesi Bassi, Stati Uniti) // Island of Palmas Case (Netherlands, USA), 4 aprile 1928, in *Reports of International Arbitral Awards*, Vol. II, pp. 829-871, al sito https://legal.un.org/riaa/cases/vol_II/829-871.pdf (consultato il 14 dicembre 2021).

[7] *Ibid,* p. 838.

[8] CIG, *Caso sulle attività militari e paramilitari in e contro il Nicaragua* (Nicaragua c. Stati Uniti // Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. USA), 27 giugno 1986, in I.C.J. *Reports* 1986, p. 14, al sito https://www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (consultato il 14 dicembre 2021). In merito cfr. N. RONZITTI *Diritto internazionale dei conflitti armati*, III ed., Torino, 2006, pp.23-59.

[9] Nella senteza sulle attività militari e paramilitari in Nicaragua la CIG ha dichiarato : « The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference ; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law. », e che « Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free one ». *Ibid.*

[10] Art. 2 della Carta delle Nazioni Unite, al sito https://www.un.org/en/sections/un-charter/un-charter-full-text/ (consultato il 14 dicembre 2021).

quello che è il mondo fisico. Tuttavia, oggetto del presente lavoro sono le operazioni di tipo inamichevole o illecito compiute nel cyberspazio, le cosiddette operazioni informatiche, note anche come *cyberoperations* (o operazioni cibernetiche), ed il loro rapporto con il diritto internazionale. Se, infatti, per quanto riguarda il loro rapporto con il diritto nazionale, questi atti vengono trattati tendenzialmente alla stregua di reati di competenza del giudice nazionale, è sul piano internazionale che si pongono gli interrogativi che portano con sé le maggiori sfide[11].

Questo tipo operazioni ha fatto la sua comparsa durante la Guerra Fredda, per vedere un importantissimo incremento nei numeri a partire dai primi anni del XXI secolo, tanto da rappresentare oggi un campo di azione e di specializzazione autonomo sia per il settore pubblico e sia per il settore privato[12]. La caratteristica principale delle cyberoperazioni è il fatto che, fermo restando che gli effetti possono prodursi nel mondo fisico, vengono eseguite in uno "spazio" digitale, il cyberspazio appunto, dove è possibile compiere atti in modo istantaneo, indipendentemente dalla distanza fisica che separa dall'obiettivo, e dove può risultare estremamente difficoltoso (quando non impossibile) risalire agli autori degli atti stessi.

Le cyberoperazioni nascono in ambito militare e di sicurezza, ma come si vedrà in seguito sono oggi diffuse ben oltre l'ambito originario, complice anche l'informatizzazione di ogni aspetto della vita delle persone. Oltre alle cyberoperazioni attuate in campo militare (per le quali si usa il termine di guerra cibernetica o l'inglese *cyberwafare* e che non rientrano nello spettro delle operazioni prese in analisi nel presente lavoro, rappresentando a loro volta un campo di indagine specialistico meritevole di una trattazione separata), è oggi infatti comune doversi confrontare con cyberoperazioni che interessano tutti i campi dell'attività umana, inclusi quelli dell'economia, della sanità, della società civile, spesso in modo tale da rendere difficoltoso porre un confine tra la pluralità di attività e di interessi coinvolti[13].

4. *Atti illeciti nel XXI secolo: alcuni esempi del comportamento degli Stati nei confronti delle cyberoperazioni svolte da altri Stati*

Una volta definito quali siano gli atti illeciti da parte degli Stati rilevanti nel contesto delle operazioni cibernetiche e quali siano le caratteristiche di tali operazioni, è tempo di tenere conto di come le operazioni cibernetiche dell'ultimo decennio possano essere e siano state considerate alla luce del diritto internazionale vigente. Nel 2013, il gruppo di esperti governativi delle Nazioni Unite sugli sviluppi nel campo dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale ha dichiarato l'applicabilità del diritto internazionale al cyberspazio[14], sottolineandone l'importanza in relazione allo sviluppo del cyberspazio stesso[15]. Anche se tale posizione è la conseguenza di una posizione diffusa, già esistente tra gli Stati, la dichiarazione stessa nel quadro della relazione del gruppo di esperti governativi delle Nazioni Unite rappresenta una pietra miliare nella storia dello sviluppo del

[11] P. LIN, F. ALLHOFF, K. ABNEY, *Is Warfare the Right Frame for the Cyber Debate?*, in L. FLORIDI, M. TADDEO, *The Ethics of Information Warfare*, Londra, 2014, pp. 39-59.
[12] F. LEMIEUX, *Trends in Cyber Operations: An Introduction*, in F. LEMIEUX (Ed.), *Current and Emerging Trends in Cyber Operations Policy, Strategy, and Policy*, Londra, 2015, pp.3-5.
[13] Cfr, tra i molti, P. LIN, F. ALLHOFF, K. ABNEY, *Is Warfare the Right Frame for the Cyber Debate?*, *cit.* alla nota 11.
[14] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Securi*ty del 24 giugno 2013, A/68/98, al sito https://undocs.org/A/68/98 (consultato il 14 dicembre 2021).
[15] *Ibid.*

diritto internazionale e delle relazioni internazionali. Infatti, nei primi due decenni del XXI secolo, le operazioni cibernetiche considerate illecite sono diventate sempre più frequenti nelle relazioni internazionali, e gli Stati si sono trovati a dover sviluppare un *modus operandi* nei confronti di tale novità. Nell'esaminare gli elementi chiave di tali pratiche, sarà necessario fare riferimento a quanto esposto al paragrafo successivo.

Se attribuire un dato atto ad uno Stato è complesso in caso di operazioni tradizionali, lo diventa ancora di più quando si tratta di operazioni cibernetiche. Il filtro offerto dal cyberspazio rende difficile attribuire con certezza un atto ad un soggetto specifico e solo a seguito dell'identificazione del soggetto è possibile procedere alla ricerca di eventuali collegamenti tra il soggetto in questione ed uno Stato[16]. Alcune delle numerose operazioni svolte da organizzazioni di hacker nell'ultimo decennio sono state attribuite in ultima istanza ad uno Stato in seguito ad indagini condotte da parte delle agenzie di *intelligence*: una volta identificato il soggetto che ha materialmente portato a compimento l'atto sul quale era in corso l'indagine, le agenzie responsabili hanno ritenuto che i soggetti identificati seguissero direttive provenienti direttamente da organi di uno Stato, rientrando così nell'ambito di applicazione dell'art. 8 degli Articoli sulla responsabilità dello Stato[17]. Rientrano tra questi casi, ad esempio, le doglianze statunitensi contro la Russia, accusata dalle autorità statunitensi di aver interferito con le elezioni presidenziali del 2016 utilizzando una squadra di *hacker* posta alle dipendenze del GRU, l'agenzia di *intelligence* estera russa[18].

Muovendo il discorso dall'attribuzione alle regole e ai principi del diritto internazionale dei quali vi è il rischio di violazione da parte di operazioni informatiche, la prima questione presa in considerazione è la violazione della sovranità dello Stato. Allo stato attuale, sono molti gli Stati che concordano sul fatto che penetrare nell'infrastruttura informatica di un altro Stato costituisce una violazione della sovranità dello Stato[19]. Tuttavia, pur essendo la posizione più diffusa sulla questione, non c'è consenso unanime in materia, sia tra gli studiosi di diritto internazionale che tra i membri della comunità degli Stati[20]. A questo proposito il Regno Unito nella sua posizione ufficiale in materia, non ritiene che vi siano gli elementi per parlare di violazione della sovranità territoriale per quanto riguarda il cyberspazio (pur certamente riconoscendo l'esistenza del divieto di intervento)[21]. Tale posizione non coincide con quella della NATO[22] (e a questo proposito il Regno Unito ha espresso una riserva[23]) che considera invece l'eventualità di un atto informatico illegale come violazione della sovranità dello Stato[24]. La posizione della NATO sulla questione, e in generale sul rapporto tra diritto internazionale e cyberspazio è particolarmente importante in quanto l'organizzazione ha promosso la redazione del *Tallinn Manual*, il testo di riferimento per coloro che si occupano

---

16 V. *supra*. par. 2.

17 Art. 8 del Progetto di articoli sulla responsabilità dello Stato della commissione del diritto internazionale delle Nazioni Unite, cit. alla nota 2.

18 Commissione Permanente Ristretta del Congresso degli Stati Uniti d'America sull'Intelligence, *Exposing Russia's Effort to Sow Discord Online: The Internet Research Agency and advertisements*, al sito https://intelligence.house.gov/social-media-content/ (consultato il 14 dicembre 2021).

19 F. DELERUE, *Cyber Operations and International Law*, London, 2020, pp. 212-214.

20 *Ibid.*

21 Discorso del Procuratore Generale Jeremy Wright '*Cyber and International Law in the 21st Century*' del 23 maggio 2018, al sito https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (consultato il 14 dicembre 2021).

22 *NATO Allied Joint Doctrine for Cyberspace Operations*, Allied Joint Publication-3.20, Nato Standardisation Office, Gennaio 2020, al sito https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (consultato il 14 dicembre 2021).

23 *Ibid.* p. v

24 *Ibid.* p. 20

di cyberoperazioni[25]. Un interessante interrogativo relativamente all'intera questione è quello inerente al requisito di un danno quando si considera l'atto illecito in termini di sovranità statale. Il summenzionato divieto di violazione della sovranità statale[26] riguarda due aspetti. Il primo aspetto è quello di un'effettiva intrusione nel sistema informatico dello Stato vittima, nelle strutture correlate o, comunque, qualsiasi effetto fisico prodotto sul territorio dello Stato vittima attraverso strumenti digitali; il secondo aspetto è invece quello dell'impossibilità per lo Stato vittima di svolgere le proprie funzioni. Se su quest'ultimo aspetto non vi sono dubbi sul fatto che non è richiesto alcun danno fisico per concretizzare la violazione, sul primo aspetto la dottrina è divisa per quanto concerne quelle operazioni che non producono né danno fisico né perdita di funzionalità del sistema informatico attaccato[27]. Tuttavia, l'adozione di un approccio basato sulla logica dovrebbe considerare come una violazione della sovranità dello Stato qualsiasi penetrazione nel sistema informatico dello Stato vittima, indipendentemente dall'eventuale danno fisico.

La seconda possibile violazione del diritto internazionale di cui al par. 2 del presente scritto è il divieto di intervento. Per essere applicato alle operazioni cibernetiche compiute da uno Stato, è necessario che tale operazione cibernetica di Stato soddisfi le condizioni di coercizione e interferenza sulla capacità di prendere decisioni libere da parte dello Stato che subisce l'atto[28]. La prassi degli Stati è andata nella direzione di considerare come interventi stranieri sia operazioni importanti condotte direttamente contro uno Stato, come è stato il caso degli attacchi informatici contro l'Estonia nel 2007 e che hanno riguardato direttamente le istituzioni statali[29] sia situazioni quali la famosa violazione subita dal Comitato Nazionale del Partito Democratico degli Stati Uniti d'America durante le elezioni statunitensi nel 2016[30]. Tuttavia, l'espressione "intervento straniero" può anche includere operazioni di tipo più subdolo. Infatti, le accuse di intervento straniero sono state spesso sollevate dagli Stati in relazione alle interferenze straniere nei processi elettorali nazionali attraverso vari mezzi, come la diffusione all'opinione pubblica di notizie false o privando gli elettori di informazioni importanti relative ad una votazione[31]. Mentre un tale modo indiretto di influenzare il processo di voto influisce senza ombra di dubbio sulla capacità dello Stato di decidere liberamente, ciò che è in discussione è fino a che punto vi sia un elemento coercitivo. Il principio di "*scales and effects*" di una determinata operazione, risultante dalla sentenza sulle attività militari e paramilitari in e contro il Nicaragua[32], aiuta a determinare se un atto non armato possa essere equiparato all'uso della forza per i suoi effetti, tuttavia il dibattito riguardo alla domanda se le operazioni cibernetiche volte ad esempio ad influenzare le elezioni di un altro Stato mediante la diffusione di informazioni volutamente errate o

[25] V. *infra* par. 5.
[26] V. *supra* par. 2.
[27] Il dibattito dottrinale in materia è ampiamente trattato in M. SCHIMTT , L. VIHUL, *Respect for Sovereignity in Cyberscpace,* in *Texas Law Review*, vol. 95, 2016, p. 1639-1670, *cit.* da F. DELERUE, *Cyber Operations and International Law*, cit. alla nota 19, p .217.
[28] V. *supra* par. 2.
[29] F. DELERUE, *Cyber Operations and International Law*, *cit.* alla nota 19, p. 241.
[30] *Ibid.*, pp. 244-250.
[31] M. SCHMITT, *Foreign Cyber Interference in Elections: An International Law Primer, Part I*, in *EJIL :Talk !*, 16 ottobre 2020, al sito https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-i/ (consultato il 14 dicembre 2021).
[32] Il principio deriva da quanto affermato dalla CIG nella sentenza sulle attività militari e paramilitari in Nicaragua: « The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces », cit. alla nota 8.

incomplete tra gli elettori siano o meno da considerarsi operazioni coercitive è ancora al suo stadio iniziale.

Inoltre, le operazioni cibernetiche pongono sicuramente importanti questioni sotto il profilo dei diritti umani[33]. Valutando il problema sotto questa lente, l'idea che i diritti umani debbano essere garantiti e tutelati nel mondo "virtuale" come in quello reale è stata espressa formalmente dal Consiglio per i Diritti Umani delle Nazioni Unite nel 2012, in relazione alla libertà di parola su Internet[34]. Da allora, alcuni atti dell'ONU hanno esaminato direttamente o indirettamente la questione della protezione dei diritti umani nel ciberspazio, tra cui la risoluzione 68/243 dell'Assemblea Generale delle Nazioni Unite[35] che ha costituito un gruppo di esperti governativi che ha poi adottato una relazione sugli sviluppi nel campo delle tecnologie dell'informazione e della sicurezza internazionale[36]. Nonostante l'ampio consenso sulla questione all'interno della comunità internazionale, non vi è alcun consenso su quali siano i diritti umani che possono essere interessati dalle operazioni cibernetiche[37]. Ciò che appare chiaro è che certamente il diritto alla libertà di espressione e il diritto alla *privacy* sono soggetti al rischio di violazioni attraverso operazioni informatiche. La libertà di espressione è riconosciuta a livello globale dalla Dichiarazione Universale dei Diritti Umani[38] e dal Patto internazionale per i diritti civili e politici[39] e ribadita in strumenti regionali quali la Convenzione europea dei diritti dell'uomo[40]. Per quanto concerne le operazioni cibernetiche, la libertà di espressione viene ad esempio violata in un contesto elettorale, quando un determinato atto informatico impedisce ai candidati di esprimere le proprie opinioni o quando gli elettori sono limitati nell'accesso alle informazioni[41], come rimarcato nei casi di accuse di interferenze straniere nelle elezioni. L'altro diritto certamente interessato da ciò che avviene nel cyberspazio è il diritto alla *privacy*, anche questo espresso a livello globale dalla Dichiarazione universale dei Diritti Umani[42] e dal Patto internazionale per i diritti civili e

---

[33] Sulla tutela dei diritti umani nella realtà contemporanea cfr., tra i molti, L.PANELLA, C. ZANGHÌ, *La protezione internazionale dei diritti dell'uomo*, IV ed., Torino, 2019; R. PISILLO MAZZESCHI, *Diritto internazionale dei diritti umani*, Torino, 2020; con specifico riferimento al rapporto tra Internet e diritti umani si veda G. M. RUOTOLO, *Inernet-ional Law*, Bari, 2012, pp.113-124.

[34] Bozza di Risoluzione del Consiglio per i Diritti Umani delle Nazioni Unite sulla promozione, la protezione ed il godimento dei diritti umani su Internet, 29 giugno 2012, al sito http://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc (consultato il 14 dicembre 2021).

[35] Risoluzione dell'Assemblea Generale dell'ONU n. 68/243 del 27 dicembre 2013, al sito https://undocs.org/A/RES/68/243 (consultato il 14 dicembre 2021).

[36]Relazione di esperti governativi sugli sviluppi nel settore dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale, A/70/174, al sito https://undocs.org/A/70/174 (consultato il 14 dicembre 2021).

[37] F. DELERUE, *Cyber Operations and International Law*, cit. alla nota 19, p. 270.

[38] Art. 19 della Dichiarazione Universale dei Diritti Umani, adottata e proclamata dall'Assemblea Generale delle Nazioni Unite con Risoluzione 217A(III) del 10 dicembre 1948, al sito https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/itn.pdf (consultato il 14 dicembre 2021).

[39] Art. 19 del Patto sui diritti civili e politici, adottato dall'Assemblea Generale delle Nazioni Unite con Risoluzione 2200A(XXI) del 16 dicembre 1966, al sito https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (in lingua inglese; consultato il 14 dicembre 2021).

[40] Art. 10 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, firmata a Roma il 4 novembre 1950, al sito https://www.echr.coe.int/documents/convention_ita.pdf (consultato il 14 dicembre 2021).

[41] M. SCHMITT, *Foreign Cyber Interference in Elections: An International Law Primer, Part II*, in *EJIL :Talk !*, 16 ottobre 2020, al sito https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-ii/ (consultato il 14 dicembre 2021).

[42] Art. 12 della Dichiarazione Universale dei Diritti Umani, cit. alla nota 38.

politici[43], nonché riconosciuto in strumenti regionali come la Convenzione europea dei diritti dell'uomo[44]. Il diritto alla *privacy* è probabilmente quello più colpito dalla rivoluzione informatica, poiché le nuove tecniche di sorveglianza raccolgono un'enorme quantità di dati, potenzialmente esponendo la vita privata dei soggetti intervistati, e questo è vero non solo in caso di attacchi ad enti statali ma anche in caso di attacchi informatici a soggetti, anche privati, legittimamente in possesso di dati sensibili[45].

Infine, si ritiene necessario sottolineare come in caso di violazione dei diritti umani attraverso operazioni cibernetiche, lo Stato che subisce l'attacco potrebbe eventualmente essere ritenuto, quantomeno in parte, responsabile della violazione stessa. Infatti, l'obbligo di rispettare i diritti umani spetta non solo allo Stato che compie l'attacco (e che quindi si deve astenere da azioni contrarie a tale obbligo), ma anche allo Stato che si trova a contrastare un attacco, e le cui azioni devono essere a loro volta conformi all'obbligo di rispettare i diritti umani (per non parlare del caso in cui uno Stato violi i diritti dei propri stessi cittadini, situazione possibile ad esempio nel caso di operazioni di sorveglianza).

5. *Diritto internazionale e cyberoperazioni, nuovi strumenti dalla crisi globale*

Da quanto brevemente esposto finora è possibile osservare come le operazioni cibernetiche illecite da parte degli Stati siano affrontate dagli Stati e dalla comunità internazionale nel suo complesso esattamente come avviene per operazioni illecite (o quanto meno inamichevoli) di tipo più tradizionale. Nel fare ciò, gli Stati e la comunità internazionale basano la loro azione su strumenti pensati per le operazioni tradizionali, adattandoli a nuovi scenari che apparivano impensabili anche solo qualche decennio addietro.

In questa prospettiva, sono particolarmente importanti una serie di strumenti sviluppati con l'obiettivo di cristallizzare ciò che è lo stato attuale dell'arte, o utilizzando le parole della prima edizione del *Tallinn Manual*[46], con l'obiettivo di "riflettere il consenso tra gli Esperti sull'applicabilità della *lex lata*[47]".Tra questi strumenti, si trova appunto il *Tallinn Manual 2.0* evoluzione della citata prima edizione, che è stato ampiamente coperto dalla dottrina giusinternazionalistica e che rappresenta lo strumento più completo ed esteso sul rapporto tra diritto internazionale e cyberspazio, con *focus* particolare sull'aspetto militare[48]. Sviluppato da un gruppo di esperti giuridici internazionali su incarico del NATO CCDCOE, prima nel 2013[49] e successivamente rivisto e ampliato nel 2017[50], il *Tallinn Manual 2.0* affronta un gran numero di questioni che coinvolgono lo spazio informatico e che, pur essendo stato

[43] Art. 17 del Patto sui diritti civili e politici, cit. alla nota 39.
[44] Art. 8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà fondamentali, cit. alla nota 40.
[45] F. DELERUE, *Cyber Operations and International Law*, cit. alla nota 19 , p. 267-268 ; In materia di protezione di dati su Internet cfr. G.M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati*, Bari, 2021.
[46] M. SCHMITT (Gen. ed.), *Tallinn Manual on the International Law Applicable to Cybewarfare*, Londra, 2013.
[47] *Ibid.* p. 5.
[48] In merito al *Tallinn Manual 2.0* si rinvia a E. T. JENSEN, *The Tallinn Manual 2.0: Highlights and Insights*, in *Georgetown Journal of International Law*, vol. 48, 2017, pp. 735-778 ; D. EFRONY, D. SHANY, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, in *American Journal of International Law*, vol. 112 (4), 2018, pp. 583-657, e W. BANKS, *State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0*, in *Texas Law Review*, vol. 95, pp. 1487-1513.
[49] M. SCHMITT (Gen. ed.), *Tallinn Manual on the International Law Applicable to Cybewarfare*, cit. alla nota 46.
[50] M. SCHMITT (Gn. ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cybewarfare*, cit. alla nota 3.

concepito con un marcato orientamento militare, l'ampia portata dei contenuti permette oggi di considerarlo come strumento fondamentale per lo sviluppo dell'intero settore[51].

Se la necessità di organizzare e sistematizzare quanto disposto e previsto dal diritto internazionale in ambito bellico in relazione al cyberspazio ha portato al *Tallinn Manual 2.0*, alcuni degli eventi verificatisi negli ultimi mesi, in particolare le suddette interferenze cibernetiche nelle elezioni estere e la pandemia Covid-19, hanno portato l'*Oxford Institute for Ethics, Law and Armed* Conflict presso la *Blavatnik School of Government* dell'Università di Oxford congiuntamente ai propri partner (vale a dire, Microsoft e il Governo del Giappone), a riunire un gruppo di esperti internazionali in materia di diritto internazionale in quello che è diventato noto come "*Oxford Process on International Law Protections in Cyberspace*" (in breve semplicemente *Oxford Process*), risultato del quale è una serie di cinque (al momento in cui si scrive) strumenti di settore riguardanti le operazioni cibernetiche e il diritto internazionale. Detti strumenti hanno anche in questo caso carattere dottrinale e rappresentano non un'elaborazione di norme ma una disamina su come le norme ed i principi del diritto internazionale debbano essere applicati nel cyberspazio[52].

5.1. *La Dichiarazione di Oxford sulla protezione giuridica internazionale contro le operazioni informatiche mirate al settore sanitario*

Il primo strumento è la Dichiarazione di Oxford sulla protezione giuridica internazionale contro le operazioni informatiche mirate al settore sanitario[53] (in seguito: prima Dichiarazione di Oxford) ed è stata aperta alla firma degli esperti che hanno partecipato alla redazione e dell'intera comunità di studiosi di diritto internazionale il 22 maggio 2020. Il documento è stato elaborato con l'obiettivo di chiarire e precisare quali siano le protezioni esistenti nel diritto internazionale applicabili, come suggerisce il titolo, alle operazioni cibernetiche contro il settore sanitario. Gli eventi che hanno portato all'iniziativa dell'Università di Oxford sono stati gli attacchi informatici subiti da un certo numero di istituzioni sanitarie e operatori del settore, tra cui l'Organizzazione Mondiale della Sanità, durante i primi mesi della pandemia di Covid-19[54]. La dichiarazione inizia con un preambolo in cui, a seguito di alcune considerazioni sulla situazione pandemica, gli esperti osservano che le operazioni cibernetiche sono soggette al diritto internazionale[55] e ricordano, in tal modo, la posizione dell'Assemblea generale delle Nazioni Unite[56]. Gli esperti procedono poi ad enunciare sette norme e principi del diritto internazionale, sui quali vi è consenso sul fatto che essi proteggono le strutture mediche e incoraggiano gli Stati a tener conto di tali norme e principi nelle loro attività[57].

Le sette regole e principi che trovano posto nella prima Dichiarazione di Oxford sono: il principio secondo cui il diritto internazionale si applica alle operazioni cibernetiche

---

[51] E. T. JENSEN, *The Tallinn Manual 2.0: Highlights and Insights*, cit. alla nota 48, p. 778.

[52] *The Oxford Process on International Law Protections in Cyberspace* al sito https://www.elac.ox.ac.uk/the-oxford-process-on-international-law-protections-in-cyberspace#/ (consultato il 14 dicembre 2021).

[53] Dichiarazione di Oxford sulla protezione giuridica internazionale contro le operazioni informatiche mirate al settore sanitario, cit. alla nota 1.

[54] D. AKANDE, D. HOLLIS, D. HONGJU KOH, J. Ò BRIEN, *Oxford Statement on the International Law Protections against Cyber Operations Targeting the Health Care*, in *EJIL :Talk !*, al sito https://www.ejiltalk.org/oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-health-care-sector/ (consultato il 14 dicembre 2021).

[55] Preambolo della Dichiarazione di Oxford sulla protezione giuridica internazionale contro le operazioni informatiche mirate al settore sanitario, cit. alla nota 1.

[56] *Ibid.*

[57] *Ibid.*

condotte dagli Stati; il divieto, ai sensi del diritto internazionale, delle attività statali che possono provocare danni ai servizi sanitari essenziali di altri Stati; l'obbligo, ai sensi del diritto internazionale dei diritti umani, di proteggere la vita di tutti gli esseri umani presenti sul territorio dello Stato; l'obbligo positivo per uno Stato che sia edotto della conduzione di un cyberattacco transnazionale proveniente dal proprio territorio a danno del sistema sanitario di un altro Stato di porre fine all'operazione nociva e di adottare tutte le misure per mitigare i danni; l'obbligo, ai sensi del diritto umanitario internazionale, di non condurre cyberattacchi contro le strutture sanitarie anche durante i conflitti armati; la potenziale considerazione delle operazioni cibernetiche contro le strutture sanitarie come reati internazionali; infine, la potenziale applicazione di tutte le altre norme e principi del diritto internazionale che proteggono il sistema sanitario degli Stati, insieme alle norme e principi già individuati.

5.2. *La seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini*

Il secondo strumento elaborato dal gruppo di esperti, la seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini[58] (in seguito la seconda Dichiarazione di Oxford), discende direttamente dalla prima ed è, ancora una volta, il risultato della reazione dell'Università di Oxford e dei suoi partner ad una serie di eventi: nell'estate del 2020, Canada, Stati Uniti e Regno Unito hanno rilasciato una dichiarazione congiunta in cui accusavano l'*intelligence* russa di cercare di ottenere informazioni riservate sul vaccino Covid-19 attraverso mezzi cibernetici. A ciò è seguita una dichiarazione del Dipartimento di Giustizia degli Stati Uniti che accusa funzionari cinesi di operazioni informatiche dirette a soggetti che lavorano nel trattamento di Covid-19 e nello sviluppo del vaccino[59]. Tali eventi hanno sollecitato una risposta da parte della comunità dei giusinternazionalisti che ha evidenziato la protezione fornita dal diritto internazionale alla ricerca sui vaccini. Il documento redatto dagli esperti riuniti dall'Università di Oxford e aperto alla firma il 7 agosto 2020[60], segue l'approccio metodologico, la struttura e il ragionamento della prima Dichiarazione di Oxford e mira a fornire un elenco di regole e principi del diritto internazionale, sui quali vi è consenso, che tutelano la ricerca scientifica, la produzione e la distribuzione del vaccino Covid-19 contro le operazioni cibernetiche[61]. Nel preambolo della seconda Dichiarazione di Oxford viene descritta la situazione pandemica mondiale al momento della stesura, concentrandosi sulla ricerca sui vaccini, la produzione e la distribuzione, e i firmatari fanno riferimento alla summenzionata prima Dichiarazione di Oxford nel ricordare che qualsivoglia interferenza con le attività sanitarie pone a rischio vite umane[62].

---

[58] Seconda dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini, cit. alla nota 1.

[59] D. AKANDE, A. COCO, T. DE SOUZA, D. HOLLIS, D. HONGJU KOH, J. Ò BRIEN, T. VAN BENTHEM, *The Second Oxford Statement on International Law Protections of the Healthcare Sector During COVID-19: Safeguarding Vaccine Research*, in *EJIL :Talk !*, 11 agosto 2020, al sito https://www.ejiltalk.org/the-second-oxford-statement-on-international-law-protections-of-the-healthcare-sector-during-covid-19-safeguarding-vaccine-research/ (consultato il 14 dicembre 2021).

[60] Seconda dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: Salvaguardia della ricerca sui vaccini, cit. alla nota 1.

[61] Preambolo della Seconda dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: Salvaguardia della ricerca sui vaccini, cit. alla nota 1.

[62] Preambolo della Seconda dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini, cit. alla nota 1.

Il gruppo di esperti ha nuovamente individuato, come nel caso della prima Dichiarazione di Oxford, sette principi di diritto internazionale che proteggono la ricerca, la produzione e la distribuzione dei vaccini COVID-19 e di cui gli Stati dovrebbero tener conto nelle loro attività: i primi due principi enunciati (applicazione del diritto internazionale alle operazioni informatiche e divieto ai sensi del diritto internazionale delle operazioni cibernetiche contro l'assistenza sanitaria) si trovano anche nella prima Dichiarazione di Oxford, ma nella seconda Dichiarazione il campo di applicazione dei principi è esplicitamente esteso alla ricerca, alla sperimentazione, alla produzione e alla distribuzione del vaccino COVID-19, comprendente la protezione dei dati di ricerca e dei risultati delle sperimentazioni lungo le strutture e le relative strutture tecnologiche necessarie allo sviluppo del vaccino COVID-19[63]. Per quanto riguarda i conflitti armati, l'intero processo relativo al vaccino COVID-19 è considerato rientrare nell'alveo delle protezioni concesse alle strutture sanitarie dal diritto internazionale umanitario[64] e si osserva come anche in uno scenario non bellico il diritto internazionale garantisca un'ampia protezione allo sviluppo del vaccino COVID-19[65]. La seconda Dichiarazione di Oxford pone un forte accento sugli obblighi positivi degli Stati derivanti dal principio della *due diligence*, ma anche dall'obbligo di garantire i diritti civili e politici e i diritti sociali, culturali ed economici, anche se tuttavia vi è solo un riferimento generale a tali diritti e nessuna menzione specifica di una convenzione o di un altro strumento specifico del diritto internazionale[66].

5.3. *La Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali*

Il 20 ottobre 2020 è stata adottata dagli esperti giuridici riuniti ad Oxford una terza dichiarazione, incentrata sulle interferenze elettorali attuate con mezzi informatici[67]. La Dichiarazione di Oxford sulla protezione giuridica internazionale contro le interferenze elettorali straniere attraverso mezzi digitali (in seguito: terza Dichiarazione di Oxford) è il risultato di un terzo *workshop* organizzato dall'Università di Oxford e dai suoi partner, in seguito alle esperienze di successo di cui sopra. Il *workshop* è stato reso necessario dalle notizie in costante aumento di interferenze straniere, che vedono tra gli accusati in particolare Russia, Cina e Iran, nei processi elettorali di un gran numero di Stati europei e degli Stati Uniti[68]. Ancora una volta, gli esperti internazionali riuniti dall'Università di Oxford affermano con chiarezza quali sono le regole e i principi del diritto internazionale sui quali vi è consenso relativamente alla loro applicabilità ai processi elettorali. Nel Preambolo della terza Dichiarazione di Oxford, i firmatari vanno direttamente alle fondamenta dell'ordinamento giuridico internazionale contemporaneo: in primo luogo, vengono menzionate la Carta delle Nazioni Unite e "l'indipendenza politica di ciascuno Stato come elementi cardine del sistema

[63] Punti 1-2 della Seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini, cit. alla nota 1.
[64] Punto 3 della Seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini, cit. alla nota 1.
[65] Punto 4 della Seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini, cit. alla nota 1.
[66] Punti 5-7 della Seconda Dichiarazione di Oxford sulla protezione giuridica internazionale del settore sanitario durante Covid-19: salvaguardia della ricerca sui vaccini, cit. alla nota 1.
[67] Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali, cit. alla nota 1.
[68] D. AKANDE, A. COCO, T. DE SOUZA, D. HOLLIS, D. HONGJU KOH, J. Ò BRIEN, T. VAN BENTHEM, *The Oxford Statement on International Law Protections against Foreign Electoral Interference through Digital Means*, in *EJIL :Talk* !, 28 ottobre 2020, al sito https://www.ejiltalk.org/the-oxford-statement-on-international-law-protections-against-foreign-electoral-interference-through-digital-means/ (consultato il 14 dicembre 2021).

internazionale"[69] seguita dalle posizioni dell'Assemblea Generale delle Nazioni Unite e della Corte internazionale di giustizia in materia[70]. L'aspetto della questione relativo ai diritti umani si trova immediatamente di seguito, quando i firmatari richiamano l'art. 25 del Patto sui diritti civili e politici[71] e le convenzioni regionali africane, americane ed europee sui diritti umani, le quali riconoscono e tutelano il diritto delle persone di scegliere liberamente i loro rappresentanti[72]. Vengono anche richiamati gli articoli sulla responsabilità degli Stati quando si afferma come gli Stati siano responsabili anche di azioni svolte da privati se queste sono riconducibili agli Stati stessi[73]. Prima di passare all'elencazione dei principi e delle norme applicabili individuate dai firmatari, vengono infine richiamate una serie di dichiarazioni e strumenti relativi al comportamento degli Stati nel cyberspazio[74].

La prima questione esaminata è quella dell'applicabilità del diritto internazionale alle operazioni informatiche con conseguenze negative sul processo elettorale di un altro Stato. Si osserva che il processo elettorale non è dato solo dalla votazione in senso stretto, ma si estende anche al conteggio ed alla veridicità dei voti ed anche al fornire agli elettori tutte le informazioni necessarie sull'intero processo. Come conseguenze negative sono da considerarsi gli atti che intervengono sia sullo svolgimento del processo elettorale sia sul minare la fiducia degli elettori sul processo stesso o sui suoi risultati[75]. Pertanto, gli Stati devono astenersi dal condurre, sponsorizzare o prestare assistenza in operazioni che possono interferire con il processo elettorale, così come descritto al punto precedente[76]. I firmatari affermano poi come gravi sugli Stati anche un onere considerevole in termini di prevenzione e protezione dei processi elettorali sia all'estero che a livello nazionale. La *due diligence* obbliga gli Stati ad agire contro le operazioni cibernetiche provenienti dai loro territori e che possono provocare conseguenze negative sul processo elettorale di un altro Stato, e allo stesso tempo gli Stati hanno l'obbligo di adottare tutte le misure necessarie per garantire che le elezioni nazionali siano protette dalle interferenze straniere[77].

5.4. *La Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazione*

[69] Preambolo della Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali, cit. alla nota 1.
[70] *Ibid.*
[71] L'art. 25 del Patto sui Diritti civili e politici stabilisce che "il cittadino molto ha il diritto e l'opportunità, senza restrizioni irragionevoli [a] di partecipare allo svolgimento degli affari pubblici, direttamente o attraverso rappresentanti liberamente scelti;[b] di voto e da eleggere in occasione di vere e proprie elezioni periodiche che hanno luogo a suffragio universale e paritario e sono tenute a scrutinio segreto, garantendo la libera espressione della volontà degli elettori ; [c] di accedere, in condizioni generale di eguaglianza, ai pubblici impieghi del proprio paese", cit. alla nota 39.
[72] Preambolo della Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali, cit. alla nota 1.
[73] V. *supra* paragrafi 2 e 4.
[74] In particolare i principi guida delle Nazioni Unite sulle imprese e i diritti umani, la dichiarazione congiunta sulla libertà di espressione e le elezioni nell'era digitale, adottata dal relatore speciale delle Nazioni Unite per la libertà di opinione e di espressione, dal rappresentante dell'OSCE per la libertà dei media e dal relatore speciale dell'OAS sulla libertà di espressione e l'appello di Parigi a favore della fiducia e della sicurezza nel cyberspazio.
[75] Punto 1 della Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali, cit. alla nota 1.
[76] Punti 2-3 della Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali, cit. alla nota 1.
[77] Punti 4-6 della Dichiarazione di Oxford sulla protezione del diritto internazionale contro le interferenze elettorali straniere attraverso mezzi digitali, cit. alla nota 1.

Nei primi mesi del 2021 è stata elaborata ed aperta alla firma una quarta dichiarazione avente a oggetto la regolamentazione delle operazioni e le attività di informazione[78]. I motivi che hanno portato a tale sviluppo all'interno dell'*Oxford Process* sono da ricondursi alla risonanza che informazioni false o comunque incomplete hanno acquisto negli ultimi tempi e che sono sfociate, ad esempio, negli attacchi al popolo Rohingya, frutto di una campagna di odio circolata sulla rete, o nei fatti di Capitol Hill, che annoverano tra le concause anche la campagna di informazione estremamente polarizzante seguita alle elezioni del 2020 negli Stati Uniti[79]. Nel caso di questa quarta Dichiarazione, la questione che ha guidato la comunità scientifica non era tanto se il diritto internazionale si applichi alle tecnologie di informazione e comunicazione, fatto pacifico a livello internazionale, quanto in quale modo il diritto internazionale si applichi alle operazioni ed alle attività di informazione su internet[80]. La Dichiarazione inizia con un preambolo dove si richiamano le precedenti tre Dichiarazioni e le dichiarazioni dei principali organi a tutela della libertà di espressione sia su scala globale (Special Rapporteur delle Nazioni Unite sulla libertà di opinione ed espressione) sia su una dimensione regionale (OCSE, OAS e Commissione africana sui diritti dell'uomo e dei popoli). Di particolare interesse infine il fatto che vengano richiamati direttamente gli artt. 11 e 12 dei Principi Guida ONU su imprese e diritti umani e la responsabilità degli operatori privati di rispettare i diritti umani, responsabilità che nelle parole del gruppo di lavoro si estende anche all'impatto delle attività e delle operazioni di informazione condotte utilizzando i servizi degli operatori privati stessi[81].

Affermata nel primo punto della Dichiarazione l'applicabilità del diritto internazionale a tutte le attività condotte con l'uso di tecnologie di informazione e comunicazione, gli esperti affermano l'esistenza di obblighi per gli Stati sia quando operano direttamente, sia nel regolare e controllare le attività di informazione sulla rete. Gli Stati devono condurre le proprie attività nel rispetto della sovranità degli altri Stati e del principio di non interferenza negli affari interni di uno Stato, ma devono impegnarsi anche sul proprio territorio non solo a non essere coinvolti ma bensì a proibire quelle attività di informazione che diano luogo a discorsi d'odio o discriminatori ed a non partecipare in o supportare qualunque attività di informazione che possa violare i diritti degli individui che si trovino sotto la giurisdizione dello Stato stesso[82]. Vengono anche delineati i principi che gli Stati devono rispettare nel proteggere i diritti umani degli individui che si trovano sotto la propria giurisdizione e nell' adottare misure a protezione di questi, con attenzione particolare al fatto che nel regolamentare le attività di informazione gli Stati non possono arbitrariamente limitare la libertà di espressione o altri diritti garantiti dall'ordinamento internazionale e che vi debba essere un'attività di sorveglianza da parte degli Stati sulla capacità di operare in pieno rispetto dei diritti umani da parte delle società private che forniscono servizi informatici[83]. La Dichiarazione prosegue poi con il rimarcare come le operazioni e le attività di informazione

[78] Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazione cit. alla nota 1.

[79] D. AKANDE, A.COCO, T. DE SOUZA DIAS, D. HOLLIS, J. O'BRIEN, T. VAN BENTHEM, *The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities*, in *EJIL :Talk* !, 02 giugno 2021 al sito https://www.ejiltalk.org/the-oxford-statement-on-international-law-protections-in-cyberspace-the-regulation-of-information-operations-and-activities/ (consultato il 14 dicembre 2021).

[80] *Ibid.*

[81] Preambolo della Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazionem cit. alla nota 1.

[82] Punti 1-4 della Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazionem cit. alla nota 1.

[83] Punti 5-7 della Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazione, *cit.* alla nota 1.

debbano essere conformi al diritto internazionale umanitario e possano costituire elemento di crimini internazionale qualora dovessero averne le caratteristiche[84].

5.5. *La Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio: regolamentazione delle operazioni di ransomware*

Infine, una quinta Dichiarazione di Oxford relativa agli attacchi *ransomware* è stata aperta alla firma nell'autunno del 2021[85]. Tale dichiarazione non si discosta come impostazione dalle precedenti, che vengono richiamate nel preambolo della stessa. Nel preambolo, inoltre, si fa riferimento a come la pandemia di Covid-19, aumentando la dipendenza delle attività umane dalle reti informatiche, abbia aperto a nuove opportunità di sfruttamento dei *ransomware* e di *malware* in generale, con conseguenti ingenti danni arrecati a soggetti sia pubblici che privati[86]. Caratteristica dell'attacco *ransomware* è infatti quella di bloccare l'accesso ai dati colpiti fino a quando non vengono accolte le richieste, solitamente il pagamento di una somma di denaro, del soggetto che ha portato a compimento l'attacco. Sebbene tali operazioni vengano nella maggior parte dei casi compiute da soggetti criminali per fini meramente economici, è evidente come si ponga la questione di quegli Stati che tollerano o comunque non contrastano tali operazioni soprattutto quando originatesi sul proprio territorio[87].

In seguito all'affermazione che puree le operazioni *ransomware* rientrano tra quelle coperte dal diritto internazionale, gli esperti si focalizzano proprio sulla condotta degli Stati, che devono in primo luogo astenersi dal compiere e dal prestare assistenza a chi compie operazioni *ransomware*, in particolare quando queste rappresentino una violazione della sovranità di Stati terzi, del principio di non intervento negli affari di uno Stato terzo, quando possano configurarsi come uso della forza o quando l'attacco *ransomware* risulti in una violazione dei diritti umani[88]. Al contempo, gli Stati devono non solo non permettere l'originarsi di tali operazioni sul proprio territorio ma anche adottare tutte le misure che sono in loro potere per mettervi fine nel più breve tempo possibile una volta emerse. Inoltre, gli Stati sono tenuti a porre in essere tutte le misure necessarie, anche di tipo legislativo, per proteggere i propri cittadini da possibili ed eventuali violazioni dei diritti umani causate da operazioni *ransomware*[89]. Anche in un contesto bellico, infine, l'utilizzo di *ransomware* rimane soggetto al rispetto del diritto internazionale umanitario ed il loro utilizzo potrebbe contribuire al configurarsi di crimini internazionali[90].

Ciò che le cinque Dichiarazioni di Oxford hanno in comune è che trattanoquestioni molto specifiche e che sono orientate esclusivamente ad un determinato contesto, non

---

84 Punti 8-9 della Dichiarazione di Oxford sulla protezione giuridica internazionale nel cyberspazio : regolamentazione delle operazioni e delle attività di informazione, cit. alla nota 1.

85 Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : regolamentazione delle operazioni di r*ansomware*, cit. alla nota 1.

86 Preambolo della Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : regolamentazione delle operazioni di *ransomware*, cit. alla nota 1.

87 D. AKANDE, A. COCO, T. DE SOUZA DIAS, D. HOLLIS, J. O'BRIEN T. VAN BENTHEM, *The Oxford Statement on International Law Protections in Cyberspace: The Regulation of Ransomware Operations*, in *EJIL :Talk* !, 4 ottobre 2021 al sito https://www.ejiltalk.org/the-oxford-process-on-international-law-protections-in-cyberspace-the-regulation-of-ransomware-operations/ (consultato il 14 dicembre 2021)

88 Punti 1-3 della Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : regolamentazione delle operazioni di *ransomware*, cit. alla nota 1.

89 Punti 4-5 della Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : regolamentazione delle operazioni di *ransomware*, cit. alla nota 1.

90 Punti 6-7 della Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : regolamentazione delle operazioni di ransomware, cit. alla nota 1.

mirando ad affrontare l'intera relazione tra il diritto internazionale e le operazioni informatiche. Sono inoltre "aperte", nel senso che non mirano a delineare una disciplina specifica ma si focalizzano sui principi fondamentali che non possono essere un freno o arrecare pregiudizio alcuno all'applicazione di altre norme che abbiano rilevanza per la questione affrontata[91]. La comunità degli esperti giuridici internazionali invita gli Stati a tenere conto di un numero relativamente limitato di principi accettati sui quali vi è ampio consenso circa la loro applicazione a specifiche operazioni informatiche. Una dichiarazione così chiara e inequivocabile del ruolo e della forza del diritto internazionale nel cyberspazio, pur affrontando specifiche circostanze storiche, ha un peso enorme: in primo luogo, perché riafferma e porta all'attenzione del mondo il ruolo che la legge ha anche in tempi duri e caotici per l'intero pianeta, anche nel contesto di eventi che accadono, almeno in parte, "al di fuori" del mondo fisico; in secondo luogo, perché pone le basi per un ulteriore sviluppo del diritto internazionale nel cyberspazio, andando oltre i confini di una serie di principi teorici che specificano come tali regole e principi devono essere intesi in un contesto specifico. Queste riflessioni portano alle conclusioni del presente lavoro e ad alcune ipotesi e prospettive per il futuro. Per meglio affrontare la parte conclusiva tuttavia è utile fare qualche considerazione su come la questione della cybersicurezza venga affrontata dal legislatore italiano e come questo sia influenzato dal dibattito globale.

6. *La risposta dell'Italia: l'Agenzia per la cybersicurezza nazionale*

Anche l'Italia infatti, come tutti gli attori della società internazionale, si trova a dover fare i conti con la dimensione del cyberspazio e nel farlo non può prescindere da quelli che sono gli sviluppi a livello europeo ed internazionale. Non potrebbe d'altra parte essere altrimenti vista la partecipazione dell'Italia all'Unione europea ed alla vita della comunità internazionale e considerato che anche l'Italia è oggetto di attacchi cibernetici. Particolare risalto ha avuto l'attacco del 30 luglio 2021 indirizzato contro i sistemi informatici della Regione Lazio e che ha interessato il sistema di prenotazione dei vaccini contro il Covid-19 nel pieno della campagna vaccinale[92]. Pochi giorni dopo anche la Regione Toscana, in particolare l'agenzia sanitaria regionale, è stata vittima di un caso simile che ha avuto minore visibilità mediatica e nel quale si sono verificati danni più ridotti[93]. Interessante segnalare come questi attacchi possano ricondursi a quegli attacchi contro il sistema sanitario di cui alla prima Dichiarazione di Oxford[94], vista la assoluta priorità che i Governi hanno attribuito alla campagna vaccinale tanto da poterla ragionevolmente considerare come servizio medico essenziale e rientrino al contempo sotto la definizione di attacco *ransomware* di cui alla quinta Dichiarazione di Oxford[95].

Allo scopo di accentrare e di rendere più efficaci le misure di contrasto alle minacce provenienti dalla rete, l'Italia ha recentissimamente istituito con il decreto-legge 14 giugno

[91] Si veda in questo senso il punto conclusivo di ognuna delle dichiarazioni dell'*Oxford Process*, cit. alla nota 1.
[92] Comunicato della Regione Lazio sull'attacco del 30 luglio 2021, al sito https://www.regione.lazio.it/notizie/attacco-hacker (consultato il 14 dicembre 2021).
[93] Comunicato della Regione Toscana sull'attacco del 17-18 agosto 2021, al sito https://www.toscana-notizie.it/web/toscana-notizie/-/ars-virus-informatico-dati-epidemiologici-e-statistici-in-via-di-totale-recupero (consultato il 14 dicembre 2021).
[94] Punto 2 della Dichiarazione di Oxford sulla protezione giuridica internazionale contro le operazioni informatiche mirate al settore sanitario, cit. alla nota 1.
[95] Dichiarazione di Oxford sulle protezioni del diritto internazionale nel cyberspazio : regolamentazione delle operazioni di *ransomware*, cit. alla nota 1.

2021, n. 82[96], convertito con modificazioni dalla legge 4 agosto 2021, n. 109[97], l'Agenzia per la cybersicurezza nazionale, ente intorno al quale si dovrà incardinare il sistema di sicurezza informatica italiano. La realizzazione di tale ente è inoltre da collocarsi nel quadro della strategia UE di cybersecurity che prevede già da più di un decennio un'agenzia europea di cybersicurezza (ENISA)[98] e mira attivamente ad un'armonizzazione del quadro normativo degli Stati membri in materia. Di particolare importanza in tale contesto è la direttiva (UE) 2016/1148 del Parlamento e del Consiglio[99], attuata dall'Italia con il decreto legislativo 18 maggio 2018, n. 65[100], con la quale si stabiliscono livelli di sicurezza delle reti informatiche comuni per tutti gli Stati membri. In quest'ottica toccherà all'Agenzia per la cybersicurezza nazionale disporre e strutturare quello che sarà il sistema nazionale di cyberdifesa, da incentrarsi su sei pilastri: lo sviluppo di una strategia nazionale, lo sviluppo della tecnologia e dei mezzi necessari alla cyberdifesa, lo sviluppo delle risorse umane, lo sviluppo dell'organizzazione tra gli enti che prendono parte alla cyberdifesa, l'opera di formazione e la cooperazione internazionale[101]. La dimensione internazionale dell'attività dell'Agenzia per la cybersicurezza nazionale è d'altronde naturale viste sia la citata partecipazione dell'Italia alla vita della comunità internazionale sia l'essenza delle minacce provenienti dal cyberspazio, transnazionali ed aterritoriali per definizione. A questo proposito, è proprio il decreto-legge istitutivo ad attribuire all'Agenzia per la cybersicurezza nazionale il compito di definire e mantenere aggiornato il quadro normativo nazionale in materia tenendo in considerazione quanto avviene a livello internazionale[102]. Ed in questo alveo appare necessario fare riferimento, da parte di chi si troverà ad operare nell'Agenzia per la cybersicurezza nazionale, all'opera svolta dalla dottrina, in particolare alle Dichiarazioni di Oxford ed al *Tallin Manual 2.0*, trattandosi di opere di sistematizzazione che delineano delle linee guida per il settore sulle quali concordano i più importanti esperti di diritto internazionali al mondo.

7. *Conclusioni*

Ciò che emerge sinora dall'analisi del rapporto tra diritto internazionale e cyberoperazioni compiute da Stati e dalle Dichiarazioni di Oxford è che lo spazio informatico non è un'area selvaggia, come viene spesso affermato. Naturalmente, la natura del cyberspazio pone alcune sfide agli Stati e alla comunità internazionale soprattutto per quanto riguarda l'attribuzione della condotta allo Stato autore dell'illecito. Se l'eventuale violazione di un obbligo di diritto internazionale può essere accertata quantomeno ponendo l'attenzione

96 Decreto-legge 14 giugno 2021, n. 82, al sito https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/sg (consultato il 14 dicembre 2021).
97 Legge 4 agosto 2021, n. 109, al sito https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg (consultato il 14 dicembre 2021).
98 *European Agency for Cybersecurity* (ENISA), profilo al sito https://europa.eu/european-union/about-eu/agencies/enisa_en (consultato il 14 dicembre 2021).
99 Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione, al sito https://eur-lex.europa.eu/eli/dir/2016/1148/oj/ita/pdf (consultato il 14 dicembre 2021).
100 Decreto legislativo 18 maggio 2018, n. 65, al sito https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg (consultato il 14 dicembre 2021).
101 Sui sei pilastri alla base del lavoro dell'Agenzia per la cybersicurezza nazionale si veda A. L. SCIACOVELLI, *L'Agenzia per la cybersicurezza nazionale: un approccio olistico multi tasking? I 6 pilastri* , in *CybersecurityItalia*, 6 agosto 2021, al sito https://www.cybersecitalia.it/lagenzia-per-la-cybersicurezza-nazionale-un-approccio-olistico-multi-tasking-i-6-pilastri/13462/ (consultato il 14 dicembre 2021).
102 Art. 7, c. 1, lett. p) del Decreto-legge 14 giugno 2021, n. 82, *cit* alla nota 96.

sugli effetti dell'atto compiuto, è innegabile che per quanto riguarda l'attribuzione, l'agire fuori dallo spazio fisico, utilizzando tecnologie che consentono di rendere al limite dell'impossibile l'identificazione dell'identità di compie l'atto, ponga una sfida di proporzioni epocali. Tuttavia, le posizioni assunte dall'Assemblea Generale delle Nazioni Unite, dagli Stati e dalla comunità degli esperti di diritto internazionale chiariscono che le caratteristiche del cyberspazio non ne fanno uno spazio libero, e che le regole e i principi del diritto si applicano nel mondo cibernetico così come nel mondo fisico. La digitalizzazione di gran parte degli aspetti pubblici e privati della vita delle persone (si pensi a strumenti quali lo SPID o la firma digitale, solo per restare in ambito italiano) rende il cyberspazio un'area sulla quale gli Stati e le organizzazioni internazionali sono chiamati a prestare una crescente attenzione. La portata delle cyberoperazioni è infatti tale da obbligare gli Stati e le organizzazioni internazionali (ma come si è accennato oramai la questione interessa anche i privati) non solo a sviluppare tecniche di difesa dalle cyberoperazioni inamichevoli o illecite (attività che rientrano nel campo della cybersicurezza) ma anche, nel contesto di dette tecniche, di implementare la capacità di attuare a propria volta cyberoperazioni difensive che saranno a loro volta oggetto di studio e di regolamentazione. Su queste premesse, il compito che attende la neonata Agenzia per la cybersicurezza italiana appare decisamente impegnativo visto che le viene affidata la costruzione e lo sviluppo dell'intero sistema di cyberdifesa nazionale, a sua volta da incardinarsi nel sistema dell'Unione europea e che dovrà per forza di cose, come detto, relazionarsi con ciò che avviene su scala globale. Appare evidente come ci si trovi di fronte ad un'autentica rivoluzione, già in corso da almeno vent'anni e sulla quale le crisi globali di un anno che passerà indubbiamente alla storia quale il 2020 hanno acceso i riflettori. Quello che resta come insegnamento delle esperienze del biennio 2020-2021 è che coloro che sono chiamati a governare i processi che avvengono su scala globale devono affrontare ciò che avviene nel cyberspazio con la stessa priorità di ciò che avviene al di fuori di esso e in questo la comunità scientifica rappresenta uno dei principali alleati. Le Dichiarazioni emerse dall'*Oxford Process* sono certamente strumenti di carattere dottrinale, al pari del *Tallinn Manual 2.0*, che tuttavia, dato il ruolo che la dottrina riveste nello sviluppo del diritto internazionale, rappresentano dei fondamentali punti di riferimento per tutti gli attori coinvolti nelle relazioni internazionali[103].

[103] D. CARREAU, F. MARRELLA, *Diritto Internazionale*, cit. alla nota 3, p. 344.