UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II

DIPARTIMENTO DI GIURISPRUDENZA

DOTTORATO DI RICERCA IN DIRITTO DELL'ECONOMIA

XXXII CICLO

CYBERSPAZIO E DIRITTO INTERNAZIONALE

Governance, attacchi informatici e diritto alla *privacy*

Tutor
Prof. Fulvio Maria Palombino

Candidato
Alessandro Stiano

Anno Accademico 2019/2020

SOMMARIO

INTRODUZIONE E PIANO DEL LAVORO 1

CAPITOLO I

DAL PROBLEMA DELLA GOVERNANCE DI INTERNET ALLA RICERCA DELLE NORME INTERNAZIONALI APPLICABILI AL CYBERSPAZIO

1. La nascita di internet ed il suo sviluppo: alcune precisazioni tecniche e terminologiche 6

2. Le regole applicabili al cyberspazio: dall'anarchia al problema della *governance* di internet 12

2.1 La *governance* di internet 16

2.2 L'ICANN e la World Conference International Telecommunication del 2012 22

3. Il (limitato) ruolo degli Stati nell'individuazione delle norme di diritto internazionali applicabili al cyberspazio e il fallimento dei negoziati intrapresi dall'Assemblea Generale 29

4. L' impulso da parte di soggetti diversi dallo Stato per la 'creazione' di regole internazionali applicabili al cyberspazio 47

5. Il valore delle iniziative degli attori non statale nella formazione di regole internazionali applicabili al cyberspazio 55

CAPITOLO II

LE NORME DI DIRITTO INTERNAZIONALE APPLICABILI AL CYBERSPAZIO: IL PROBLEMA DEGLI ATTACCHI INFORMATICI

1. Il principio di sovranità e la sua possibile applicazione al cyberspazio 59

2. La nozione di patrimonio comune dell'umanità 67

2.1 La nozione di Patrimonio comune dell'umanità in relazione al cyberspazio 71

3. La definizione di attacco informatico rilevante per il diritto internazionale 77
3.1 Divieto dell'uso della forza e attacchi informatici 84
3.1.1. Il caso *stuxnet* 104
3.1.2. L'attacco informatico statunitense nei confronti dell'Iran del 20 giugno 2019 109
4. Il principio del non intervento negli affari interni di uno Stato 112
4.1. Attacchi informatici e violazione del principio del non intervento 117
5. Il problema dell'attribuzione allo Stato del fatto illecito compiuto da soggetti privati 125
5.1. La possibile attribuzione ad uno Stato di un attacco informatico 131
5.2. *Segue:* 134
5.2.1. L' (inversione dell') onere della prova 137
5.2.2. Standard di prova: il caso delle elezioni statunitensi del 2016 e l'affare *Stuxnet* 142
5.3. Il possibile ricorso a criteri alternativi: il regime della responsabilità oggettiva 149
6. Il principio di *due diligence* e la sua rilevanza nel contesto degli attacchi informatici 152

CAPITOLO III

LA SORVEGLIANZA DI MASSA E LA TUTELA DEL DIRITTO ALLA *PRIVACY*

1. La nascita del concetto di *privacy* e la sua evoluzione. 158
2. Lo sviluppo del diritto alla *privacy* nel diritto internazionale 164
2.1. Brevi cenni al caso Datagate 171
3. La sorveglianza di massa e l'intelligence sharing nella cornice dell'art. 8 CEDU 176
4. La sentenza sul caso Big Brother Watch e altri c. Regno Unito 187
4.1. La questione della sorveglianza di massa 191
4.2. La questione dell'*intelligence sharing* 199

CONCLUSIONI.....207
BIBLIOGRAFIA.....215

INTRODUZIONE E PIANO DEL LAVORO

Negli ultimi 250 anni il mondo ha conosciuto tre grandi rivoluzioni capaci di incidere, condizionare e modificare le nostre vite[1]. La prima, riconducibile al periodo che va tra il 1760 e il 1830, si caratterizza principalmente per l'introduzione di nuovi metodi di lavorazione del ferro e dell'acciaio, nonché per gli sviluppi che hanno portato alla produzione di nuovi prodotti e a nuove scoperte scientifiche. Si pensi, ad esempio, ai nuovi metodi per trasportare le merci (le ferrovie) e alle specializzazioni nella lavorazione dei materiali[2].

La seconda grande rivoluzione, databile tra il 1875 e il 1930, ha visto invece la nascita di alcune invenzioni come l'elettricità, i mezzi di comunicazione come il telefono e i meccanismi di combustione che hanno poi dato vita ai motori delle automobili. Queste migliorie sono state possibili grazie sia all'utilizzo di capitale senza precedenti sia in virtù della creazione di una moderna organizzazione di impresa[3].

Infine, la terza rivoluzione, in corso proprio in questi anni, è segnata dalla nascita e dallo sviluppo di internet. Questo passaggio è stato reso possibile grazie ai progressi tecnologici compiuti in alcuni settori come l'*hardware* e il *software* dei computer, nonché nelle telecomunicazioni. Internet ha portato le aziende di tutto il mondo a reinventare il modo di fare impresa, determinando uno stravolgimento nel mondo delle comunicazioni e in quello degli affari. Tale trasformazione ha determinato un cambiamento senza precedenti nella produttività delle aziende,

[1] SMITH, *The Third Industrial Revolution: Law and Policy for the internet,* in *Recueil des cours, 2000,* p. 241.

[2] *Ibidem.*

[3] *Ibidem.*

portandole ad una maggiore efficienza e alla creazione di nuovi mercati digitali[4].

Al di là delle considerazioni di carattere economico, la nascita di internet ha senza dubbio influenzato e continua a farlo quasi tutti i settori della nostra vita quotidiana.

Tuttavia, per comprendere in che modo ciò sia stato possibile è necessario approfondire alcuni aspetti storici.

Le origini storiche della Rete sono riferibili ai primi anni sessanta del secolo scorso. In particolare nel 1962, allorquando un gruppo di studiosi iniziava a discutere della creazione di un sistema di comunicazione tra computer che permettesse a ogni terminale di connettersi con gli altri[5]. La base su cui poggiava questa idea era sostanzialmente quella di creare un sistema complesso di comunicazione che non fosse dipendente da un singolo computer (o nodo). In questo modo quindi anche il malfunzionamento di uno dei nodi – sia perché compromesso sia perché leso – non avrebbe determinato la cessazione delle trasmissioni di informazioni, potendo garantire quindi il costante funzionamento delle comunicazioni.

Il contesto storico in cui si inserisce questa iniziale ricerca com'è noto è quello della guerra fredda. È altrettanto noto che in quegli anni era fortemente sentita la concorrenza, soprattutto nel campo dell'innovazione tecnologica, tra i due grandi blocchi composti dagli Stai Uniti d'America (USA) e dall'Unione delle Repubbliche Socialiste Sovietiche (URSS). Da un lato, infatti, l'URSS pochi anni prima aveva lanciato il primo satellite artificiale nello spazio, lo *Sputnik*, dall'altro lato il Presidente degli USA, Eisenhower, aveva creato una speciale agenzia destinata a svolgere un

[4] *Ibidem*.

[5] Cfr. DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018, p. 32.

ruolo centrale nei primi anni di sviluppo della Rete, l'*Advanced Research and Development Agency* (ARPA)[6].

L'agenzia, nata originariamente con lo scopo di approfondire alcuni aspetti dell'innovazione tecnologica in campo militare, al suo interno ospitava un ufficio specializzato sui temi delle interconnessioni informatiche, l'*Information Processing Techniques Office* (IPTO)[7]. È proprio in questo contesto che per la prima volta nel 1969 veniva realizzata una connessione tra i terminali dell'Università di Los Angeles e l'Istituto di Ricerca di Stanford.

Si può dire dunque che da queste iniziali intuizioni e con le successive ricerche teorico-pratiche sia nata quella che oggi conosciamo come Rete.

La breve disamina circa la storia della nascita di internet si profila particolarmente importante per comprendere come l'idea iniziale di stampo marcatamente informale e localizzata sia stata con il passare degli anni abbondantemente superata. E infatti nell'ultimo trentennio, in ragione della crescita esponenziale e diffusa della Rete, si è assistito allo sviluppo del complesso tema della regolamentazione[8] e, in particolare, della regolamentazione internazionale.

---

[6] Sul tema della storia di internet si veda, tra gli altri, LEINER, CERF, CLARK, KAHN, KLEINROCK, LYNCH, POSTEL, ROBERTS, WOLFF, *Brief History of the internet*, consultabile online al seguente indirizzo www.internetsociety.org; BING, *Building a Cyberspace: History of internet*, in *BYGRAVE, BING, internet Governance: Infrastructure and Istitution*, Oxford, 2009, p. 8 ss.; GILLIES, CAILLIAU, *How the Web Was Born*, Oxford, 2000; NAUGHTON, *The Evolution of the internet: from military experiment to General Purpose Technology*, in *Journal of Cyber Policy*, 2016, p. 5 ss..

[7] DELLA MORTE, *op.cit.*, p. 33.

[8] In dottrina è stato correttamente sostenuto che all'origine della Rete vi erano dei meccanismi di coordinamento che non avevano un carattere giuridico, ma che funzionavano in modo adeguato rispetto all'esigenze della Rete stessa. A ciò è stato aggiunto che «ad un certo punto, nello sviluppo di internet, questi meccanismi di autoregolamentazione entrano in crisi, a causa di alcuni fattori principali, in primo luogo, la crescita esplosiva della Rete. Cfr. SARTOR, *La rivoluzione informatica e la globalizzazione*, in TORRESETTI (a cura di), *Diritto, polita e realtà sociale nell'epoca della globalizzazione – Atti del XXII Congresso della Società Italiana di filosofia giuridica e politica*, Macerata, 2008, p. 161.

Questi aspetti saranno affrontati nel corso del primo capitolo ove verranno anzitutto offerte delle considerazioni di carattere terminologico e tecnico, per poi affrontare le problematiche sottese al complesso tema della *governance* di internet. In particolare si individueranno i momenti più importanti che hanno caratterizzato il tentativo da parte degli Stati di trovare una soluzione negoziale al problema della regolamentazione. Tuttavia, preso atto delle difficoltà, si individueranno le iniziative poste in essere da soggetti diversi dagli Stati e ci si interrogerà circa il loro valore da un punto di vista giuridico.

Nel secondo capitolo, invece, si analizzeranno le norme e i principi del diritto internazionale preesistenti alla nascita di internet e si affronterà la tematica relativa alla loro possibile applicazione al contesto virtuale. Più nel dettaglio, verrà esaminato dapprima il principio di sovranità e la sua declinazione in relazione al cyberspazio. Si costaterà che nonostante il principio in questione esplicichi i suoi effetti sulle infrastrutture informatiche situate su un dato territorio, non può giungersi alle medesime conclusioni in relazione al cyberspazio inteso come spazio virtuale e senza confini. Preso atto di queste difficoltà, si cercherà di capire se al contesto virutale sia applicabile il regime giuridico del patrimonio comune dell'umanità. Partendo da quest'ulimo, si estenerà l'analisi più dettagliatamente ad una delle sue caratteristiche principali, vale a dire all'uso pacifico degli spazi sottoposti a tale regime. Più nel dettaglio, verranno esaminiti il divieto di uso della forza, del non intervento negli affari interni di uno Stato, nonché gli aspetti inerenti l'attribuzione di operazioni informatiche ad uno Stato.

Infine, nell'ultimo capitolo si prenderanno le mosse dal tema della tutela della *privacy* e, dopo una sua breve ricostruzione, si approfondiranno alcuni aspetti relativi al ruolo svolto dalla Corte Europea dei diritti dell'uomo. In particolare, si analizzeranno le sentenze che hanno

avuto ad oggetto il tema della sorveglianza di massa e il rispetto dell'art. 8 CEDU, con particolare riferimento ad una delle più recenti e controverse decisioni in materia.

CAPITOLO I

DAL PROBLEMA DELLA *GOVERNANCE* DI INTERNET ALLA RICERCA DELLE NORME INTERNAZIONALI APPLICABILI AL CYBERSPAZIO

SOMMARIO: 1. La nascita di internet ed il suo sviluppo: alcune precisazioni tecniche e terminologiche. - 2. Le regole applicabili al cyberspazio: dall'anarchia al problema della *governance* di internet. - 2.1 La *governance* di internet. - 2.2 L'ICANN e la World Conference International Telecommunication del 2012. - 3. Il (limitato) ruolo degli Stati nell'individuazione delle norme di diritto internazionali applicabili al cyberspazio e il fallimento dei negoziati intrapresi dall'Assemblea Generale. - 4. L' impulso da parte di soggetti diversi dallo Stato per la 'creazione' di regole internazionali applicabili al cyberspazio. - 5. Il valore delle iniziative degli attori non statali nella formazione di regole internazionali applicabili al cyberspazio.

1. La nascita di internet ed il suo sviluppo: alcune precisazioni tecniche e terminologiche

Lo studio del fenomeno teso alla regolamentazione della Rete richiede, prima di essere più opportunamente approfondito, alcune brevi riflessioni sulle caratteristiche tecniche di internet nonché alcune precisazioni di carattere terminologico.

Per quanto concerne il primo aspetto, un importante punto da analizzare riguarda la distinzione tra nozione di rete distribuita e la trasmissione dei dati a pacchetto.

Partendo dal primo concetto, bisogna ricordare che in origine la Rete aveva una struttura di tipo centralizzato e cioè ogni entità era connessa ad

un nodo centrale e affinché un'informazione potesse essere trasferita da un'entità all'altra era necessario che la comunicazione, partita da un nodo periferico, raggiungesse il nodo centrale e che quest'ultimo la trasmettesse ad una altro nodo periferico, destinatario dell'informazione[9].

I problemi di un tale sistema erano essenzialmente due: il primo concerneva la lunghezza in termini di percorso che doveva compiere un'informazione per poter essere trasmessa; il secondo, invece, indubbiamente più rilevante, riguardava la vulnerabilità del nodo centrale, che se compromesso avrebbe determinato una possibile paralisi dell'intero sistema.

Al fine di prevenire ed evitare tale fragilità, l'idea innovativa è stata quella di passare da un sistema 'centralizzato' ad un sistema 'distribuito' in cui l'informazione contenuta all'interno della comunicazione viene trasferita dal nodo di partenza a quello più vicino e da quest'ultimo a quello successivo fino a giungere al destinatario finale[10].

È proprio quest'ultimo modello ad essere stato utilizzato nel sistema ARPANET. Più precisamente, da quel modello, inteso come di tipo 'distribuito' puro, oggi si è passati ad un sistema semplicemente 'decentralizzato' in cui i fornitori di servizi mettono a disposizione (gratuitamente o a pagamento) le proprie infrastrutture che fungono da possibili centri di una serie di sotto-reti[11]. Al di là degli elementi tecnici in quanto tali, quello che in questa sede si vuole sottolineare – che sarà utile per il prosieguo della nostra ricerca – è che l'intero sistema è strutturato in modo tale da essere privo di un vero e proprio centro, dato

[9] DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2918, p. 35. Per considerazioni di carattere più generale sul tema degli aspetti tecnici relativi alla Rete si veda, tra tutti, GODON, *Considération techniques à destination des juristes*, in Société Francaise pour le Droit International, *internet et le droit international – Colleque de Rouen*, Parigi, 2014.

[10] *Ibidem*.

[11] *Ibidem*, p. 36.

che ogni entità può scegliere liberamente a quale altra entità trasmettere una particolare informazione.

Oltre a ciò occorre prendere in considerazione un ulteriore elemento dal punto di vista dell'evoluzione tecnologica, ovvero quello relativo alla 'trasmissione per pacchetto'. Con questa espressione si suole far riferimento a quel meccanismo secondo cui non è necessario che l'informazione da trasmettere sia inoltrata nella sua interezza, ma è ben possibile che questa venga trasferita per piccoli segmenti che verranno rimessi insieme direttamente una volta raggiunta la destinazione finale. Il concetto che c'è dietro il cd. Protocollo internet è proprio questo. E infatti i protocolli, insieme ai cd. indirizzi IP e il sistema dei nomi a dominio (DNS)[12] rappresentano nel loro insieme la struttura portante e principale di internet così come oggi lo conosciamo.

Le precisazioni di carattere tecnico fin qui esposte non hanno solo una valenza teorica, ma incidono su alcuni degli aspetti giuridici che interessano direttamente le regole applicabili al cyberspazio.

Com'è stato sostenuto, uno dei terreni su cui queste precisazioni acquistano particolare rilevanza sono quello della 'neutralità della Rete' e quello della cybersicurezza[13].

Quanto al primo aspetto, esso si fonda sull'idea di una rete internet neutrale per cui i dati a pacchetto che vengono trasmessi devono essere trattati tutti allo stesso modo e dunque nessun utente in particolare né servizio deve essere favorito rispetto ad un altro[14].

---

[12] Secondo alcuni, invero, il corretto funzionamento dei DNS è di importanza assoluta dal momento che esso garantisce l'esistenza della Rete stessa. Sul punto si veda RUOTOLO, *internet-ional Law. Profili di diritto internazionale pubblico della Rete*, 2012, Bari, p. 48.

[13] DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, cit., p. 37.

[14] Cfr. SOLUM, *Models of internet Governance*, in L.A. BYGRAVE, J. BING (a cura di) *internet Governance. Infrastructure and Institutions*, Oxford University Press, 2009, p.88

Relativamente invece alla cybersicurezza, essa dovrebbe essere garantita grazie alla resilienza di internet[15]. La capacità di adattamento quindi dovrebbe essere finalizzata a garantire il cd. *disaster recovery*, cioè quei processi volti a salvaguardare dati e infrastrutture necessarie all'erogazione dei servizi più importanti nei casi di gravi emergenze[16].

Passiamo ora all'ulteriore aspetto preliminare, e cioè quello relativo alle considerazioni di carattere terminologico.

A tal proposito, anzitutto va precisata la differenza tra il termine 'cyberspazio' e 'internet', sovente erroneamente utilizzati come sinonimi. Il termine internet[17], che configura una «una tecnica di trasmissione di dati»[18], non è altro che un settore del cyberspazio che invece, in prima approssimazione, può dirsi evocare uno spazio, una dimensione, come lo sono aria, mare, terra e spazio esterno. internet, invece, è un meccanismo di comunicazione tra una molteplicità di reti, definibile come una sorta di 'rete delle reti' che, secondo quanto riportato dalla *Max Planck Encyclopedia of Public International Law*, «comprises phisically the entitrety of the global interconnected computer networks, which colloquially is equated with the information, cummunication, and other services available therin»[19].

[15] DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, p. 37.

[16] *Ibidem*.

[17] Secondo altri autori il termine internet fa riferimento «ad un sistema complesso di apparecchi in origine coincidenti coi soli computer, ma negli ultimi tempi anche di diverso tipo come televisioni, smartphone o consolle per i videogiochi, distribuiti in maniera disomogenea sulla superficie del pianeta». A ciò va aggiunto che «internet è una infrastruttura […] priva di organizzazione gerarchica. Al suo interno, infatti, non esiste alcun punto, né centrale né di vertice dal quale si diramano tutti i percorsi, né è possibile individuare una macchina alla quale tutte le altre devono essere collegate per comunicare tra loro. Si veda RUOTOLO, *internet (diritto internazionale)*, in *Enciclopedia del diritto – Annali vol. VII*, 2014, p. 545 e p. 547.

[18] CAROTTI, *Il sistema di governo di internet*, Milano, 2016, p. XIII

[19] WOLTAG, *internet*, in *Max Planck Encyclopedia of Public International Law*, 2010.

Passando invece alla locuzione cyberspazio, è necessario sottolineare come l'individuazione degli elementi che lo costituiscono non è compito facile. La sua costante evoluzione – dettata dal crescente utilizzo di internet – ha infatti determinato il susseguirsi di una molteplicità di definizioni che di volta in volta hanno cercato di affrontare la maggiore importanza che tale spazio assumeva nella nostra vita quotidiana[20].

In linea generale possiamo dire che il termine cyberspazio –composto dalle parole cyber(netica) e spazio – trova le sue radici nella parola greca *kybernan* (ossia colui che detiene il comando; capitano). La sua origine nell'accezione moderna, tuttavia, è da rintracciarsi nel pensiero dello scrittore William Gibson che lo intese come uno spazio digitale nel quale gli individui interagiscono e si scambiano informazioni, etichettandolo come «un'allucinazione consensuale sperimentata quotidianamente da milioni di operatori legittimi, in ogni nazione (…) una rappresentazione grafica di dati astratti da banche dati presenti in ogni computer del sistema umano»[21].

A tale primordiale accezione si sono susseguite poi diverse definizioni, sia di carattere normativo che dottrinale, sicuramente più attinenti al nostro campo d'indagine.

Tra queste va anzitutto richiamata quella emanata dal Dipartimento di Difesa americano il quale delinea il cyberspazio come «un dominio globale all'interno dell'ambiente informativo costituito dalla rete

[20] Per un approfondimento di carattere più generale si rimanda a BRYANT, *What Kind of Space is Cyberspace*, in *internet Journal of Philosophy*, 2001, p 138-155; KOESPELL, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property*, Londra, 2003; COHEN, *Cyberspace as/and Space*, in *Columbia Law Review*, 2007, p. 210-256.

[21] GIBSON, *Neuromante*, Milano, 1986, p. 69. Per la versione originale si veda, ID, *Neuromancer*, Regno Unito, 1984, p. 51.

interdipendente di infrastrutture informatiche, tra cui internet, reti di telecomunicazione e sistemi informatici»[22].

Questo assunto, sebbene non sia il più completo ed esaustivo, in ragione di un mancato riferimento al lato *software*, è stato ritenuto un adeguato punto di partenza in considerazione dell'utilizzo in dottrina e in altri e differenti documenti ufficiali[23] degli elementi in esso individuati. E infatti, partendo dalle indicazioni fornite dal Dipartimento di Difesa americano, l'autore Daniel Kuehl ha suggerito una rappresentazione del cyberspazio che vada al di là di un insieme di computer e informazioni digitali, sostenendo che ci troviamo dinanzi a un «dominio globale all'interno dell'ambiente informativo il cui carattere distintivo è dato dall'uso dell'elettronica e dello spettro elettromagnetico al fine di creare, archiviare, modificare e scambiare informazioni attraverso reti indipendenti e interconnesse»[24].

Anche la NATO ha descritto il cyberspazio come «uno spazio globale, non fisico e concettuale che include componenti fisiche e tecniche come internet, 'la memoria pubblica globale' contenuta nei siti Web accessibili al pubblico, nonché tutte le entità e gli individui connessi a internet»[25].

Ebbene, dalle definizioni poc'anzi menzionate è possibile individuare gli elementi che accomunano il modo in cui il cyberspazio viene inteso, sia in dottrina sia dagli Stati. Si può ritenere infatti che esso sia composto

---

[22] Traduzione dell'Autore, per la versione originale si veda DoD Dictionary of Military and Associated Terms, novembre 2010, Joint Chiefs and Staff, Joint pubblications.

[23] TSAGOURIAS, *The legal status of Cyberspace*, in TSAGOURIAS e BUNCHAN (a cura di), *Research Handbook on International Law and Cyberspace,* Cheltenham, 2015, p. 13 ss.; VON HEINEGG, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013

[24] Traduzione dell'Autore, per la versione originale si veda KUEHL, *From Cyberspace to Cyberpower: Defining the Problem*, in KRAMER, STARR e WENTS (a cura di) *Cyberpower and National Security*, Nebraska, 2009, p. 28.

[25] Traduzione dell'Autore, per la versione originale si veda ZIOLKOWSKI, *Confidence Building Measures for Cyberspace - Legal Implications*, Tallin, 2013, p. 5.

da almeno tre livelli: il primo, più concreto, costituito dalle infrastrutture fisiche (computer, cavi, server, antenne); il secondo costituito dal *software*, programmi attraverso i quali è possibile controllare il livello precedente; il terzo livello costituito dai dati, contenuti nelle macchine, che generano a loro volta le informazioni informatiche[26].

L'ulteriore elemento che può dedursi è che il cyberspazio, oltre ad essere formato da uno spazio virtuale, a-territoriale e per sua stessa natura senza confini, è 'sorretto' da elementi fisici, collegati ad uno spazio reale senza i quali l'intera struttura non esisterebbe[27]. È quindi necessario distinguere gli aspetti fisici da quelli virtuali in ragione delle differenti regole di diritto internazionale ad essi applicabili.

2. Le regole applicabili al cyberspazio: dall'anarchia al problema della *governance* di internet

Dopo questa breve disamina sulle caratteristiche infrastrutturali della Rete, appare adesso necessario tracciare gli elementi che hanno portato alla nascita della problematica relativa alla cd. *governance* di internet[28] e in particolare ai profili di una *governance* internazionale.

---

[26] TABANSKI, *Basic Concenpts in Cyber Warfare*, in *Military and Strategic Affairs*, 2011, p. 77.

[27] A ben vedere, tuttavia, potrebbe sostenersi che dei confini 'infrastrutturali' siano esistenti, in particolar modo laddove l'accesso ad internet non viene riconosciuto a tutti in egual modo. Si fa riferimento al concetto di *digital divide*, e cioè alla limitazione concreta di accedere alle tecnologie dell'informazione e delle telecomunicazioni, incluso quindi internet. Tale problema può derivare da cause strutturali come l'arretratezza delle infrastrutture o le difficoltà economiche in cui versa un Paese, ma non è esclusa la sua esistenza anche all'interno del medesimo Stato, configurando – ad esempio – una disparità di accesso tra le diverse regione. Il tema è stato da ultimo affrontato dall'*Human Rights Council*, il quale ha sottolineato che «the global and open nature of internet as a driving force in accelerating progress towards development in its various forms», auspicando quindi un sempre maggiore accesso alla Rete da parte dell'intera Umanità. Cfr. Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the internet*, 29 June 2016, UN Doc A/HRC/20/L. 13, 2.

[28] In linea generale, con il termine *governance*, la cui traduzione dall'italiano non appare possibile, e pertanto verrà mantenuta la locuzione inglese, si intende qualsiasi forma di organizzazione dell'azione collettiva. Più dettagliatamente, il termine si riferisce a un processo

Sin dalla nascita di internet, e del connesso nuovo spazio (virtuale), è sorto un intenso dibattito circa il modo in cui esso dovesse essere considerato da un punto di vista giuridico. La domanda (in questa prima parte del nostro lavoro) alla quale proveremo a rispondere è essenzialmente questa: il cyberspazio può essere considerato alla stregua di un luogo in cui le regole giuridiche – e per quello che a noi interessa, le regole di carattere internazionale – possono essere applicate oppure, al contrario, questo deve intendersi come uno spazio libero paragonabile ad una sorta di terra *nullius* virtuale?[29]

---

di regolamentazione, su base orizzontale, che coinvolge attori di natura diversa (sia pubblici che privati) con il fine di conseguire obiettivi di carattere politico. Si tratta di 'reti' che funzionano principalmente su base consensuale e che utilizzano come metodo per la risoluzione di eventuali controversie la negoziazione e il confronto. Com'è stato osservato, proprio in virtù di tali metodologie risolutive, «è più probabile lo stallo e il rinvio che la vittoria di una parte sull'altra» (cfr. BOBBIO, *Invece dello Stato: reti,* in *Parole chiave – nuova serie di 'Problemi del socialismo',* 2005, p. 34. Lo stesso autore aggiunge «non è un caso che il termine *governance* sia diventato di moda. Esso riassume in modo sintetico una circostanza che si caratterizza per la 'diffusione e la dispersione dell'autorità politica lungo una pluralità di percorsi verticali e orizzontali che non hanno più lo Stato come epicentro politico'. Non è più il governo a governare. Sono piuttosto le reti in cui gli stessi governi si trovano a confrontarsi (o scontrarsi) con altri soggetti». Per un'analisi più dettagliata si veda G. DELLA MORTE, *op.cit.*, p. 39, nota 39.

[29] In dottrina è stata paventata l'idea secondo cui il regime giuridico applicabile agli spazi internazionali abbia radici abbastanza lontane, e segnatamente al diritto romano. In particolare, secondo questa idea, gli spazi internazionale potrebbero essere divisi in due macro categorie: *res nullius* e *res communis*. La prima fonda le proprie basi sull'idea che una determinata 'cosa' non sia di proprietà di nessuno e, di conseguenza, qualsiasi Stato potrebbe farla propria. In linea con questo approccio, basato sul concetto legale di attribuzione, Jhon Locke ha sviluppato la nozione di diritto naturale. Per quanto attiene alla seconda categoria, invece, essa sta ad indicare le cose che sono di dominio pubblico e che non sono di proprietà di nessuno Stato/soggetto. Di conseguenza, tutti possono avere accesso a quel determinato bene/spazio. In realtà, prima dello sviluppo dell'era tecnologica e di internet, gli Stati dibattevano sulla questione se alcuni spazi come ad esempio le acque internazionali, l'Antartica, la luna o gli altri corpi celesti erano da considerare *res nullius* ovvero *res communis*. Senza addentrarci troppo all'interno della questione (che verrà poi affrontata nel corso dell'elaborato, in questa sede ci pare opportuno solo indicare che può ritenersi ormai pacifica l'idea secondo cui tali spazi non sono sottoposti al principio di sovranità degli Stati e quindi nessuno di essi può esercitare il proprio potere in modo unilaterale senza permettere agli altri di poter usufruire delle risorse presenti. Cfr. WEBER, *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles*, Berlino, 2015, p. 5-6.

Invero, il problema relativo alle regole giuridiche applicabili al cyberspazio è tutt'altro che nuovo. Le difficoltà nel tracciare un regime giuridico ad esso applicabile si sono manifestate sin da quando la Rete, liberandosi della sua connotazione marcatamente militaristica tipica degli inizi anni sessanta, ha raggiunto negli anni novanta la sua definitiva affermazione su base globale, e da quel momento diversi sono stati gli approcci al problema.

Se agli albori di internet si professava la sua totale indipendenza, definendo il cyberspazio come uno spazio del tutto autonomo e lontano da qualsiasi intervento governativo[30], ad oggi la strada intrapresa sembra muoversi in una direzione diametralmente opposta: l'interesse degli Stati per le attività svolte con l'uso dei mezzi informatici, nonché per le operazioni, soprattutto di carattere economico, è divenuto sempre più intenso[31].

Da un lato, un primo filone inquadrava il cyberspazio come uno spazio virtuale, privo di confini territoriali e pertanto differente rispetto agli spazi reali. Esponenti di tale corrente erano per lo più autori statunitensi di metà

[30] Celebre in tal senso è la Dichiarazione di Indipendenza del Cyberspazio redatta da J. Barlow. Secondo l'Autore infatti «[g]overnments of Industrial World (…) you are not welcome among us. You have no sovereignty where we gather… I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions… Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This *governance* will arise according to the conditions of our world, not yours. Our world is different». Siffatte affermazioni indicavano la chiara volontà di percepire tale nuovo 'spazio' in modo del tutto indipendente dalla sovranità degli Stati.

[31] Sono molteplici infatti i documenti statali che si sono interessati ed hanno affrontato direttamente o meno questioni relative al cyberspazio. Si pensi, ad esempio, all' *International Strategy for Cyberspace* emanato nel 2011 dal governo americano oppure alla *National Strategic Framework for cyberspace security* emanato nel 2013 dalla presidenza del consiglio dei ministri italiano.

anni novanta, i quali ritenevano non solo che internet non fosse sottoponibile alle tradizionali regole di diritto, ma addirittura che per un suo corretto funzionamento il cyberspazio *dovesse* autoregolarsi[32]. Tale visione (cd. *cyber libertarian*), in ragione della primaria importanza riconosciuta all'elemento territoriale, individuava una diretta corrispondenza tra le norme applicabili e l'esistenza di confini ben determinati. Lo Stato pertanto poteva esercitare al suo interno la propria sovranità e giurisdizione[33]. Di conseguenza, essendo il cyberspazio per sua stessa natura uno spazio senza confini – inteso intrinsecamente come un fenomeno globale – gli Stati non potevano né dovevano esercitare alcuna sovranità su di esso[34]. In altre parole, in ragione della sua intrinseca natura a-territoriale, l'unico modo per poter regolare il cyberspazio era quello di una *self-govenance* attuata dagli utenti della Rete, e ciò per almeno tre ordini di ragioni. In primo luogo perché in questo modo si sarebbe garantita una maggiore efficienza rispetto a qualsiasi altro sistema di *governance*; secondariamente perché la "comunità digitale" avrebbe necessitato di un insieme di regole e procedure differenti rispetto a quelle stabilite dagli Stati; infine perché solo attraverso l'autoregolamentazione sarebbe stato possibile promuovere una *voluntary compliance*[35].

Ad una tale concezione si è ben presto contrapposta la visione di chi, paragonando la *self-governance* ad una forma di anarchia (tanto da utilizzare il termine *cyberanarchy*), inquadrava il cyberspazio in modo non dissimile rispetto al "mondo reale": le transazioni che avvengono attraverso il

[32] In questi termini, JHONSON, POST, *Law and Borders-The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, p. 1367-1402.

[33] JHONSON, POST, *op.cit.*, 1369. Secondo gli autori, la corrispondenza tra norme applicabili e delimitazione territoriale è sorretta da diverse circostanze come *power; effects, legitimacy* e *notice*.

[34] JHONSON, POST, *op.cit.*.

[35] PERRITT, *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism*, in *Berkley Technology Law Journal*, 1997, 424.

cyberspazio non sono differenti rispetto a quelle che intercorrono normalmente tra due diverse nazioni[36]; le azioni poste in essere avvengono sempre tra soggetti appartenenti al mondo reale e sono sottoposti alla sovranità dello Stato e alla sua giurisdizione[37]. A queste obiezioni inoltre se ne aggiungevano altre di carattere più pragmatico. Veniva sottolineato infatti che per il corretto funzionamento di internet – potremmo dire per la sua stessa esistenza – è necessaria la presenza di infrastrutture fisiche che inevitabilmente si troveranno sul territorio di un determinato Stato e di conseguenza saranno sottoposte alla sua sovranità e giurisdizione.

Senonché, la questione qui brevemente rappresentata lungi dall'avere un carattere meramente teorico-dottrinale, nel corso degli anni infatti essa ha assunto un significato sempre più rilevante anche sul piano pratico. L'effetto tangibile di quanto si sta dicendo è rintracciabile proprio nel complesso tema della *governance* di internet, questione da cui bisogna prendere sin da subito le mosse e che sarà oggetto della prima parte di questo capitolo.

2.1 La *governance* di internet

Come si è avuto modo di vedere, può ormai ritenersi superato il paradigma relativo all'applicabilità o meno di alcune regole, anche internazionali, ad internet. È indubbio infatti che la risposta a questa domanda debba essere positiva. A dar manforte a questa tesi ci ha pensato in primo luogo l'Organizzazione delle Nazioni Unite (ONU), la quale attraverso una delle sue agenzie specializzate, l'International Telecommunications Union (ITU), ha dato vita a diverse conferenze internazionali, con ad oggetto proprio il

[36] GOLDSMITH, *Against Cyberanarchy*, in *University of Chicago Law Occasional Paper*, 1999, 1

[37] *Ibidem*, p. 2

tema di cui stiamo parlando, che sono comunemente conosciute con il nome di *World Summit on the Information Society* (WSIS).

I modelli di *governance* tuttavia affinché potessero essere efficienti dovevano tenere in considerazione la struttura particolare di internet. Come abbiamo visto infatti la trasmissione dei dati e quindi delle informazioni non avviene attraverso un sistema centralizzato, ma si avvale del cd. sistema a pacchetti. Una simile architettura rende quindi particolarmente difficile l'istituzione di un unico centro di imputazione decisionale capace di esercitare funzioni normative in maniera univoca e generalizzata[38]. Da qui nasce la complessità che caratterizza gli aspetti regolativi di internet.

È possibile avere contezza di questi aspetti allorquando si allarga lo sguardo sul piano internazionale.

Il tema della *governance* infatti ha assunto rilievo in occasione del *World Summit on the Information Society* (WSIS), ovvero una serie di conferenze internazionali organizzate dall' International Telecommunications Union (ITU)[39], agenzia specializzata operante sotto l'egida delle Nazioni Unite, a cui hanno preso parte Stati, società civile e aziende.

---

[38] Cfr. NATOLI, *La internet governance nel sistema internazionale*, in *Federalismi*. *Rivista di diritto pubblico, comparato ed europeo*, 2014, p. 7.

[39] Com'è noto, trattasi di una delle agenzie specializzate dell'ONU il cui atto costitutivo ha subito diverse modifiche nel corso degli anni fino al 1992, anno in cui è stata adottata 'la costituzione' unitamente ad una convenzione e a due regolamenti amministrativi: uno riguardante le telecomunicazioni e l'altro le radiocomunicazioni, entrambi periodicamente aggiornati ed emendati. Le revisioni periodiche dei regolamenti amministrativi vincolano tutti gli Stati membri fatti salvi i casi in cui questi non manifestano la loro opposizione nel momento dell'adozione o entro un certo periodo di tempo. Particolarmente importante è il regolamento delle radiocomunicazioni in quanto tende a disciplinare e coordinare l'uso delle frequenze radio e dell'orbita geostazionaria. Oltre al settore delle radiocomunicazioni, la struttura organizzativa dell'ITU prevede due settori ulteriori: uno volto alla standardizzazione delle telecomunicazioni e l'altro al loro sviluppo. Inoltre, i membri che compongono l'Unione possono essere distinti tra quelli statali e di settore. I primi sono attualmente 193 e rappresentano gli Stati; i secondi invece, che ammontano a 700, rappresentano le diverse categorie di attori coinvolti nel settore delle telecomunicazioni, incluse le organizzazioni regionali e internazionali come la internet Society e il *Groupe Speciale Mobile* (GSM). Cfr. CONFORTI, *Diritto Internazionale,* XI edizione, a cura di M. IOVANE, Napoli, 2018, p. 165; WALDEN, *International*

Il summit internazionale costa di due differenti fasi. La prima, tenutasi a Ginevra nel 2003 e conclusasi con l'adozione di una Declaration of Principles[40] e un Action Plan, aveva come obiettivo lo sviluppo negli Stati di una maggiore consapevolezza circa la necessità di adottare delle regole comuni di disciplina della cd. società dell'informazione. La Dichiarazione, in particolare, fissava alcuni principi inerenti una corretta *governance* di internet, che dovrebbe ispirarsi al multilateralismo e alla trasparenza nonché al principio democratico, garantendo l'accesso diffuso alle informazioni e alla conoscenza. Senonché uno dei problemi principali che non permetteva l'avanzata un dialogo costruttivo sui temi indicati era propria la mancanza di una definizione programmatica della internet *governance*. Per questa ragione l'allora Segretario Generale delle Nazioni Unite, Kofi Annan, venne

Telecommunications Law, the internet and the Regulation of Cyberspace, in ZIOLKOWSKI (a cura di), *Peacetime Regime for State Activities in Cyberspace Interantional Law, International Relations and Dipomacy*, Tallinn, 2013.

[40] Data la rilevanza della Dichiarazione, il cui titolo è esplicativo degli obiettivi in essa preposti (Building the Information Society: a global challenge in the new Millennium), se ne riportano alcuni passaggi salienti: «A. Our Common Vision of the Information Society 1. We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights (…) 8. We recognize that education, knowledge, information and communication are at the core of human progress, endeavour and well-being. Further, Information and Communication Technologies (ICTs) have an immense impact on virtually all aspects of our lives. The rapid progress of these technologies opens completely new opportunities to attain higher levels of development. The capacity of these technologies to reduce many traditional obstacles, especially those of time and distance, for the first time in history makes it possible to use the potential of these technologies for the benefit of millions of people in all corners of the world (…) 20. Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders». Cfr. World Summit on Information Society, *Declaration of Principles Building the Information Society: a global challenge in the new Millennium*, Document WSIS-03/GENEVA/DOC/4-E 12 dicembre 2003.

incaricato di promuovere la creazione di un organo di studio, il *Working Group on internet Governance* (WGIG)[41], il cui scopo primario era quello di chiarire alcuni aspetti fondamentali e di riferire i risultati raggiunti nel corso della seconda fase del Summit. Più nel dettaglio, il WGIG era stato incaricato di sviluppare una definizione programmatica di internet *governance*, di indentificare i profili problematici della politica pubblica in materia di *governance* e, infine, di inquadrare i rispettivi ruoli e responsabilità degli Stati, delle organizzazioni intergovernative, delle organizzazioni internazionali, della società civile e del settore privato[42]. Il lavoro del WGIG si concludeva con l'emanazione di un rapporto che escludeva il riconoscimento in capo a qualsiasi governo di un ruolo preminente nella *governance di internet* e mirava ad una maggiore internazionalizzazione della stessa. Esso inoltre proponeva l'istituzione di un nuovo organismo consultivo, su base internazionale e globale, l'internet *Governance* Forum (IGF) al quale è oggi assegnato il compito di discutere le politiche pubbliche connesse agli elementi chiave della *governance* di internet al fine di incentivarne la sostenibilità e mantenere un dibattito aperto tra tutti gli organismi che direttamente ed indirettamente se ne occupano[43]. Infine, sempre l'IGF svolge un ruolo di promotore *ex ante* e valutatore *ex post* circa l'implementazione da parte degli Stati dei principi adottati nel corso del

[41] Il gruppo era creato da 40 persone rappresentative dei diversi attori coinvolti nella *governance* di internet. Per un approfondimento del funzionamento e delle dinamiche interne al WGIG si rimanda, tra tutti, a DRAKE (a cura di), *Reforming internet Governance: Perspectives from the Working Group on internet Governance* (WGIG), New York: United Nations Information and Communication Technology Task Force, 2005.

[42]World Summit on Information Society, *Plan of Action*, Doc. WSIS-03/GENEVA/DOC/5-E, dicembre 2003, pp. 6-7.

[43] In questi termini si veda RUOTOLO, *Il sistema dei nomi a dominio alla luce delle recenti tendenze dell'ordinamento internazionale*, in *Il diritto dell'informazione e dell'informatica*, 2016, p. 36.

WSIS nei processi di *governance*, affrontando le questioni relative alle risorse critiche della Rete come, ad esempio, gli indirizzi IP[44].

Il report finale della prima fase del WSIS proponeva quattro differenti modelli regolati per la Rete, due dei quali prevedevano la creazione di organismi collegati alle Nazioni Unite[45]. Più nel dettaglio, il primo modello prevedeva una parziale riforma dell'*internet Corporation for Assigned Names and Numbers* (d'ora in poi ICANN) – di cui parleremo più diffusamente *infra* – con la sostituzione del ruolo sino ad allora svolto dal dipartimento del commercio americano con l'IGF. In tal modo l'ICANN avrebbe assunto natura più strettamente internazionale e avrebbe svolto le proprie funzioni sotto l'egida delle Nazioni Unite[46]. Il secondo modello invece non aveva come scopo una riforma dell'ICANN, ma piuttosto tendeva a limitare il ruolo svolto dai governi al suo interno riconoscendo una maggior peso alla rappresentanza della società civile[47]. La terza proposta di riforma aveva come obiettivo l'indebolimento del ruolo svolto dai paesi industrializzati a fronte di una maggior peso riconosciuto ai paesi in via di sviluppo. A tal fine era stato proposto un rafforzamento del ruolo dell'IGF all'interno del comitato governativo presente nella struttura organizzativa dell'ICANN[48]. Infine, l'ultimo modello, senz'altro quello più radicale, proponeva una riforma totale dell'ICANN attraverso la creazione di un nuovo ente denominato *World internet Corporation for Assigned Names and Numbers* (WICANN), che avrebbe sostituito l'ICANN e sarebbe stato guidato da un *Global internet Governance Forum*[49].

---

[44] *Ibidem*.

[45] *Ibidem*.

[46] Cfr. MURRAY, *The Regulation of Cyberspace: Control in the online environment*, New York, 2007, p. 122.

[47] *Ibidem*.

[48] *Ibidem*.

[49] *Ibidem*.

Come si può agilmente notare almeno tre delle proposte qui brevemente analizzate miravano ad una totale o parziale riforma dell'ICANN.

Le conclusioni della prima fase del Summit avrebbero dovuto costituire le basi per il secondo incontro – svoltosi a Tunisi nel 2005 – che aveva uno scopo più specifico, e al tempo stesso ambizioso: la promozione di un accordo internazionale relativo alla *governance* di internet, nonché la creazione di un forum negoziale che permettesse nel corso del tempo di apportarvi migliorie attraverso l'adozione di protocolli addizionali. Tuttavia, va sin da subito notato come questa fase sarebbe culminata in un parziale fallimento. Il negoziato, infatti, si concluderà con l'adozione di un atto di carattere meramente politico, il Tunis Commitment, il cui contenuto è volto quasi esclusivamente a reiterare il supporto degli Stati alle dichiarazioni adottate nel corso della prima fase[50]; e con la cd. Agenda di Tunisi attraverso la quale veniva fatta richiesta al Segretario Generale delle Nazioni Unite di istituire un gruppo di lavoro che avesse come focus specifico quello della *governance* di internet che coinvolgesse diversi attori (sia dei paesi industrializzati che quelli in via di sviluppo) come governi, società civile e il settore privato.

L'unico aspetto positivo nonché l'unico obiettivo raggiunto nel corso dell'incontro di Tunisi è stato l'adozione di una definizione programmatica della internet *Governance*. Secondo quest'ultima, con tale termine si indicherebbe «the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms,

[50] Più nel dettaglio, uno degli aspetti più rilevanti che veniva fatto presente all'interno del documento riguardava la possibilità di riconoscere l'accesso alle informazioni, alla condivisione e alla creazione di ulteriori conoscenze come strumenti per contribuire significativamente al rafforzamento dello sviluppo economico, sociale e culturale. In questo modo si permetteva a tutti gli Stati di raggiungere gli obiettivi di sviluppo programmati a livello internazionale nonché gli obiettivi di sviluppo del Millennio. Cfr. WSIS-05/TUNIS/DOC/7-E, 18 novembre 2005. È possibile consultare il documento integralmente al seguente indirizzo online https://www.itu.int/

rules, decision-making procedures, and programmes that shape the evolution and use of the internet»[51].

Tuttavia, come anticipato, la seconda fase del summit non ha avuto esito positivo. Uno dei motivi principali di tale epilogo è stato senz'altro il differente approccio adottato dagli Stati in relazione alle proposte di riforma di uno degli enti maggiormente problematici in relazione alla gestione e alle regole da applicare ad internet. Il riferimento è chiaramente rivolto all' *internet Corporation for Assigned Names and Numbers* (ICANN), la cui importanza nel discorso relativo alla *governance* di internet è di fondamentale importanza e per questo, prima di procedere oltre, non può farsi riferimento alla sua struttura e alle sue proposte di riforma.

2.2 L'ICANN e la World Conference International Telecommunication del 2012

L'ICANN, fondata nel 1998, è una organizzazione senza scopo di lucro di natura interna in cui sono presenti il settore pubblico (i governi) e i soggetti privati (società civile e individui) che trova la sua base giuridica nella *Non-profit Public Benefit Corporation Law*, una legge dello Stato californiano. La sua funzione principale è quella di gestire la *governance* di internet attraverso tre differenti attività: l'amministrazione dei protocolli di internet (TCP/IP), l'amministrazione degli indirizzi IP e la gestione dei *root server*[52]

[51] Report of the Working Group on internet *Governance*, giugno 2005, p. 4.

[52] Il modo attraverso cui internet funziona dipende in buona sostanza dai *root* server (server radice). In totale ce ne sono tredici e la loro funzione è essenzialmente quella di fungere da *database* per tutti i nomi a dominio. In altre parole, ogni qualvolta ci sia una domanda di accesso ad un determinato punto della Rete, i root server reindirizzano la richiesta verso i server specifici e quest'ultimi a loro volta forniscono le informazioni. È chiaro quindi che la gestione dei root server determina in ultima analisi la gestione di internet inteso come 'rete di reti'. Ebbene, gli Stati Uniti, in particolare la *National Telecommunications and Information Administration* (NTIA), per il tramite di ICANN e IANA detiene il potere esclusivo di autorizzare qualsiasi modifica al contenuto del *database*. Tale esercizio di potere esclusivo

e dei cd. nomi a dominio (DNS). Il ruolo svolto dall'ICNN è quindi di fondamentale importanza non solo per il corretto funzionamento dell'intera Rete, ma anche per garantirne la sicurezza e l'affidabilità[53].

Il motivo principale per cui all'ICANN sono riconosciuti i poteri poc'anzi menzionati è da rintracciarsi essenzialmente in una ragione storica. Come abbiamo visto la nascita di internet ha radici statunitensi, il che ha giustificato sia la sua posizione geografica sia la sua natura giuridica di ente privato nonché – e di certo l'aspetto più importante – il controllo da parte degli Stati Uniti[54]. Questa situazione invero è stata sin dall'origine dell'ICANN oggetto di pesanti critiche e divergenze da parte degli attori coinvolti, sia statali che non governativi, tanto da richiedere in diverse occasioni una sua riforma che permettesse di limitare il ruolo unilaterale svolto dagli Stati Uniti.

Il momento di maggiore tensione si è concretizzato in occasione della *World Conference on International Telecommuncations* (WCIT-12) tenutasi a Dubai nel 2012 sotto l'egida dell'ITU. La conferenza si prefissava come obiettivo principale l'aggiornamento delle *International Teleccomunications Regulations* (ITRs) risalenti ormai al 1988 epoca in cui l'enorme potenziale innovativo di internet era sostanzialmente inespresso, motivo per cui il testo adottato in quel contesto aveva come scopo quello di offrire un quadro flessibile per la cooperazione internazionale in tema di interconnessione e di

viene esercitato dal governo statunitense anche per qui *root server* che sono situati sui territori di altri Stati. La giustificazione per l'applicazione extraterritoriale del potere di governo statunitense, in assenza di norme di diritto internazionale che gli riconoscano tale facoltà, sembrerebbe risiedere in una sorta di *acquiescenza* degli Stati su cui i *root server* sono dislocati. Cfr. RUOTOLO, *internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012, p. 51-60.

[53] Cfr. CARRILLO, *La reforma de la corporacion para la asignacion de nombres y numeros de internet (ICANN): un analisis en terminos de legitimidad,* in *Revista espanola de derecho internacional*, 2018, p. 156.

[54] Per un approfondimento sulla relazione tra l'ICANN e l'Amministrazione statunitense si veda, tra gli altri, HYBRID *Net: the regulatory framework of ICANN and the DNS*, in *International Journal of Law and Technology*, 2014, pp. 49-73.

interoperabilità dei servizi di comunicazione[55]. Lo sviluppo di internet com'è noto è avvenuto al di fuori di tale cornice normativa, attraverso un processo multi rappresentativo in cui attori non statali, e per lo più di nazionalità statunitense, hanno sviluppato gli *standard* tecnici che hanno permesso una crescita esponenziale dei cd. nomi a dominio che di internet rappresentano l'ossatura principale[56].

Da questi motivi è scaturita la decisione dell'ITU di emendare le ITRs al fine di adeguarle al mutato contesto internazionale delle telecomunicazioni. Il nodo principale della Conferenza pertanto ha riguardato proprio la paventata possibilità di applicare le ITRs alla Rete, attraverso modifiche testuali e strutturali all'accordo.

Va preliminarmente detto che l'intera fase preliminare della Conferenza è stata caratterizzata da un forte clima di agitazione; a pochi mesi dal suo inizio infatti una serie di segnali non propriamente positivi sono stati emessi da parte di istituzioni internazionali[57], le quali esprimevano profonde

[55] In questi termini si veda ODDENINO, *Diritto individuali, sicurezza informatica e accesso alla conoscenza in rete: la revisione delle International Telecommunication Regulations dell'ITU*, in *Diritti Umani e Diritto Internazionale*, 2013, p. 532

[56] *Ibidem*.

[57] Ad esempio, Il Parlamento Europeo, attraverso la Risoluzione del 22 novembre 2012 relativa alla WCIT-12, esprimeva preoccupazione per la mancanza di trasparenza nelle negoziazioni che precedevano la Conferenza e dichiarava: «it does not believe that the ITU, or indeed any other single, centralised international institution, is the appropriate body to assert regulatory authority over either internet *governance* or internet traffic flows. It regrets the lack of transparency and inclusiveness surrounding the negotiations for WCIT 12, given that the outcomes of this meeting could substantially affect the public interest» aggiungendo che «some of the ITR reform proposals would negatively impact the internet, its architecture, operations, content and security, business relations and *governance*, as well as the free flow of information online, and draw attention to the consequences of some of the proposals presented: the ITU itself could become the ruling power over aspects of the internet, which could end the present bottom-up, multi-stakeholder model. If adopted, these proposals could seriously affect the development of, and access to, online services for end users, as well as the digital economy as a whole; the establishment of new profit mechanisms could seriously threaten the open and competitive nature of the internet, driving up prices, hampering innovation and limiting access. Parliament recalls that the internet should remain free and open». Cfr. Parlamento Europeo, Risoluzione 2012/2881 (RSP), 22 novembre 2012.

preoccupazione per gli esiti della Conferenza. La preoccupazione maggiore invero era legata alla possibilità che il processo di aggiornamento delle ITRs – obiettivo principale della Conferenza – potesse incidere in maniera diretta sul tema della *governance* di internet.

Sulla base di queste premesse, durante la Conferenza le posizioni dei delegati si sono orientate intorno a due principali modelli di riferimento, che possono essere sintetizzati nei termini che seguono.

Da un lato vi erano coloro i quali erano a favore di una concezione di internet come mezzo incompatibile con gli assetti delle telecomunicazioni tradizionali e di conseguenza sottratto dalla cornice normativa dell'ITU; dall'altro lato invece, e in senso diametralmente opposto, vi erano i fautori di una possibile applicazione alla Rete della disciplina prevista per le telecomunicazioni in senso classico. Seguendo questo schema, un primo gruppo di Stati (capeggiati dagli Stati Uniti e seguiti dall'Unione Europea nonché da un gran numero di Stati occidentali) era favorevole al mantenimento dello *status quo* e in particolare del ruolo svolto dall'ICANN come soggetto investito della gestione dei nomi a dominio, offrendo un modello di *goverannce* cd. informale[58]. Siffatto modello avrebbe come pregi il mantenimento della Rete come risorsa aperta e globale, nonché una certa flessibilità nel riconoscere la capacità di auto-svilupparsi della Rete. In caso contrario invece – e cioè ogni tentativo di racchiudere internet in un modello di *governance* più rigido e gerarchizzato – comporterebbe il rischio di compromettere la crescita della Rete e la sua natura aperta[59]. Questo modello organizzativo, oltre che dagli Stati, era appoggiato dai grandi fornitori di

[58] Sul concetto richiamato si veda, tra tutti, WEINBERG, *Non State Actors and Global Informal Governance: the case of ICANN*, in T. CHRISTIANSEN, C. NEUHOLD (a cura di), *International Handbook on Informal Governance*, Cheltenham, 2012, p. 292 ss.

[59] Cfr. ODDENINO, *Diritto individuali, sicurezza informatica e accesso alla conoscenza in rete: la revisione delle International Telecommunication Regulations dell'ITU*, in *Diritti Umani e Diritto Internazionale*, 2013, p. 534.

servizi globali su internet, i cd. *Over the top* (OTT), quali Google, Facebook che, in ultima analisi, sostenevano il mantenimento dello *status quo* per ragioni prettamente economiche e commerciali avendo strutturato il proprio modello imprenditoriale sugli assetti di un internet globale con scarsa interferenza da parte degli Stati e dei fornitori di servizi di telecomunicazioni tradizionali.

D'altro canto, un nutrito gruppo di Stati, come Cina, Russia, nonché paesi in via di sviluppo, propendeva per un radicale cambiamento degli assetti regolativi sino a quel momento in vigore. In particolare, si ricercavano modelli nuovi e più equilibrati volti soprattutto al superamento del legame privilegiato intercorrente tra l'ICANN e gli Stati Uniti e, in ultima analisi, alla regolazione di internet attraverso la cornice normativa delle ITRs.

Le ragioni alla base di tale cambiamento erano da ricercare sia nella valorizzazione di alcuni aspetti legati alla sicurezza (come ad esempio il contrasto al *cybercrime*, al *cyberterrorismo* e alla *cyberwar*), sia alla creazione di una cornice istituzionalizzata, più sicura e prevedibile per gli sviluppi futuri, nonché la possibilità di utilizzare tale cornice per il superamento del divario digitale[60] che ancora oggi affligge i paesi meno industrializzati[61].

Ebbene dinanzi a tale spaccatura di vedute, l'esito dell'WCIT-12 non poteva che essere compromissorio, non raggiungendo affatto lo scopo che inizialmente si era prefissato. L'atto finale della Conferenza infatti è stato sottoscritto solo da 89 Stati a fronte dei 144 partecipanti e tra gli assenti si

[60] Sul tema si rimanda a AARONSON, LEBLOND, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law*, 2018, pp. 245-272; SHACKELFORD, CRAIG, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in internet Governance and Enhancing Cybersecurity*, in *Stanford Journal of International Law*, 2004, p. 119 ss.

[61] ODDENINO, *Diritto individuali, sicurezza informatica e accesso alla conoscenza in rete: la revisione delle International Telecommunication Regulations dell'ITU*, in *Diritti Umani e Diritto Internazionale*, 2013, p. 534.

registrano diversi Paesi come gli Stati Uniti, il Giappone, l'Australia, il Canada e l'Unione Europea[62]. Per quanto riguarda poi il nuovo testo delle ITRs, va da subito notato come da un punto di vista strettamente formale l'auspicio di far chiaramente riferimento ad internet non ha avuto esito positivo, non essendo stato inserito il termine in nessuna delle parti che compongono il nuovo accordo. Qualche novità più interessante, invece, è possibile scorgerla nel Preambolo e, più precisamente, attraverso il riferimento agli obblighi in materia di diritti umani che gli Stai intendono rispettare[63]. Il riferimento non va inteso come fine a sé stesso, ma rappresenta senza dubbio un tentativo di consolidare le posizioni degli Stati circa una visione libera ed aperta di internet volta altresì a contrastare i tentavi di censura da parte di alcuni regimi dittatoriali[64].

Le contrapposizioni più significative però si sono avute in relazione all'emendato art. 1.1 b) dell'accordo, dedicato allo scopo e all'oggetto del trattato. Nel citato articolo infatti si può leggere «[t]hese Regulations also contain provisions applicable to those operating agencies, authorized or recognized by a Member State, to establish, operate and engage in international telecommunications services to the public, hereinafter referred as "*authorized operating agencies"*». Il riferimento alle 'agenzie operative autorizzate', e soprattutto la mancanza di una loro adeguata definizione, ha suscitato non poche perplessità circa la possibile estensione degli obblighi derivanti dal trattato anche agli enti tecnici gestionali come l'ICANN.

In conclusione, non può non sottolinearsi, come d'altronde già fatto all'inizio di questo paragrafo, che il testo finale delle nuove ITRs appare assolutamente compromissorio e volutamente equivoco, il che non mancherà

[62] WALDEN, *op.cit.,* p. 274.

[63] Secondo il testo dell'Accordo «[m]ember States affirm their commitment to implement these Regulations in a manner that respects and upholds their human rights obligations».

[64] Cfr. NATOLI, *op.cit.,* p. 21.

di creare disagi per la futura *governance* di internet. A ciò va aggiunto un ulteriore aspetto che emerge con disarmante chiarezza e cioè l'esistenza di vedute diametralmente opposte che coincidono con la separazione geografica degli Stati: da un lato, un gruppo di Paesi occidentali che seppur numericamente più esiguo è rappresentativo di circa i due terzi degli utenti globali di internet e, dall'altro, un nutrito insieme di governi, tra i quali spiccano Russia e Cina, i quali offrono una visione di internet completamente inconciliabile rispetto ai primi.

In dottrina, a fronte di tale spaccatura di vedute, si sono venuti a creare due orientamenti parzialmente diversi tra loro. Infatti, secondo una parte, gli approcci discordanti mantenuti dagli Stati Uniti e dalla Cina nel corso della Conferenza avrebbero dato vita ad una versione tecnologica della guerra fredda in cui gli attori coinvolti tendono sempre di più a condizionare le scelte in materia di *governance* secondo una propria visione del futuro di internet[65]. In questo senso depone anche la tesi sostenuta da altri autori, secondo cui il mancato consenso sul nuovo testo delle IRTs sarebbe esplicativo di una tendenza volta ad una costante crescita della cd. frammentazione di internet, che in ultima analisi potrebbe essere descritta come l'inizio di una vera e propria guerra fredda digitale[66].

Secondo altra parte della dottrina, invece, la situazione di stallo creatasi nel corso della Conferenza non sarebbe qualificabile come una guerra, ma piuttosto andrebbe identificata nei termini di una dichiarazione di conflitto tra le diverse potenze mondiali[67].

A noi sembra invero che la situazione possa essere qualificata nei termini da ultimo utilizzati, e cioè identificando tale situazione di blocco come

---

[65] Cfr. GOLDSMITH, *WCIT-12: An Opinionated Primer and Hysteria-Debunker*, in *Lawfare blog*, 30 novembre 2012, consultabile online al seguente indirizzo www.lawfareblog.com.

[66] Cfr. ODDENINO, *op.cit.*, p. 537

[67] Cfr. ROSENZWEIG, *WCIT Treaty Breakdown – A summary and Some Analysis*, in *Lawfare blog*, 14 dicembre 2012, consultabile online al seguente indirizzo www.lawfareblog.com

l'inizio di un possibile conflitto (economico) e non invece nei termini di una vera e propria guerra. A suffragio di tale affermazione si può pensare alla recentissima situazione tra Stati Uniti e Cina circa il blocco delle vendite di forniture informatiche tra aziende statunitensi e l'azienda cinese Huawei[68].

3. Il (limitato) ruolo degli Stati nell'individuazione delle norme di diritto internazionali applicabili al cyberspazio e il fallimento dei negoziati intrapresi dall'Assemblea Generale

Dopo aver individuato ed analizzato alcuni elementi della *governance* di internet, appare ora necessario volgere lo sguardo ad una questione affine, o potremmo dire ad essa subordinata, e cioè all'individuazione delle regole di diritto internazionale applicabile al cyberspazio. In altri termini, bisogna domandarsi se il diritto internazionale è applicabile al cyberspazio e nel caso di risposta positiva individuare quali siano le regole che ad esso possano essere applicate e in che modo vadano interpretate per meglio conciliarsi con la natura *sui generis* di questo nuovo spazio.

Sotto il profilo strettamente dogmatico, l'approccio secondo cui lo studio di fattispecie giuridiche di carattere internazionale connesse al cyberspazio possa essere condotto tenendo in considerazione categorie e concetti tradizionali dell'ordinamento internazionale è stato criticamente definito come *interventionist approach*[69], proprio allorquando conduca all'applicazione analogica a fattispecie *online* di norme di diritto internazionale precedentemente sviluppate per disciplinare situazioni reali. Secondo questo approccio, l'applicazione analogica sarebbe infatti una

[68] A tal proposito si veda LOHR, *U.S. Moves to Ban Huawei From Government Contracts*, in *New York Times*, 7 agosto 2019.

[69] Cfr. D'ASPREMONT, *Cyber Operations and International Law: An Interventionist Legal Thought*, in *Journal of Conflict and Security Law*, 2016, p. 11 ss.

conseguenza ingiustificata del fatto che, al fine di rimediare all'assenza di una cornice normativa specificamente concepita, la dottrina internazionalistica verrebbe spinta ad affrontare le questioni con i propri strumenti al fine di assicurarsi che le fattispecie informatiche siano regolate mediante norme di cui essa è pienamente a conoscenza, nel tentativo di 'intervenire' nei problemi del mondo e gestirli[70].

Senonché, è agevole affermare che tale orientamente non sia pienamente applicabile a quei casi, come appunto il contesto in esame, in cui via stata un'esplicita attività normativa di diritto internazionale da parte di Stati o di organizzazioni internazionali[71].

Invero, i termini di questo problema, già a partire dal 2006, erano stati affrontati dalla Commissione del Diritto Internazionale (d'ora in poi anche CDI), la quale ha elaborato una serie di riflessioni sul tema, poi trasfuse in un documento intitolato *Protection of Personal Data in Transborder Flow of Information.* Quanto suggerito dalla CDI può essere schematizzato attraverso tre differenti approcci: il primo prevede i casi in cui il diritto esistente venga applicato direttamente a situazioni nuove; il secondo invece riguarda quelle ipotesi in cui il diritto vivente non risulti pienamente adeguato e necessiti, per la sua applicazione, di alcune modifiche; infine l'ultimo riguarda la circostanza in cui la produzione di nuove norme giuridiche è indispensabile per affrontare nuovi problemi[72].

Il primo problema da affrontare quindi è quello dell'applicabilità al cyberspazio delle regole di diritto internazionale. Sul punto, nonostante si possa già anticipare una risposta in senso positivo, non sono mancati

[70] *Ibidem.*

[71] Così RUOTOLO, *Il ruolo del consenso del sovrano territitoriale nel transborder data access tra obblighi di diritto internazionale e norme interne di adattamento*, in *La Comunità internazionale*, 2016, p. 185.

[72] Si veda *Report of the International Law Commission on the Work for the Fifty-eighth Session* (2006), allegato D, dal titolo *Protection of Personal Data in Transborder Flow of Information*, 490

elementi che hanno messo in crisi il ruolo che il diritto internazionale possa e debba effettivamente assumere.

In senso positivo invero depongono sia circostanze fattuali che giuridiche. È infatti chiaro che l'uso – e talvolta l'abuso – di tale nuovo spazio abbia delle ripercussioni tangibili nella vita concreta e nelle politiche statali che riguardano ad esempio la sicurezza nazionale, la pubblica sicurezza e lo sviluppo economico di un Paese. Gli interessi sottesi a tale spazio vanno dunque ben al di là rispetto a quelli circoscritti sul piano meramente interno di uno Stato[73].

Dal punto di vista giuridico, e più precisamente per ciò che attiene al diritto internazionale, possiamo dire che sulla questione vi sia stato un consenso solo a partire dal 2013.

Il rapido sviluppo delle tecnologie dell'informazione e delle telecomunicazioni aveva catturato l'attenzione delle Nazioni Unite, e segnatamente di uno dei suoi organi principali, ovvero l'Assemblea Generale, già a partire dal 1998. È in quell'anno infatti che la Russia propose una bozza di Risoluzione all'Assemblea Generale nella quale si indicava che le nuove tecnologie potevano essere usate per destabilizzare e minacciare la sicurezza degli Stati. Per questo motivo sollecitava gli altri Stati membri di informare il Segretario Generale al fine di provvedere ad uno sviluppo dei principi internazionali affinché si raggiungesse uno standard di sicurezza per tali tecnologie e si riuscisse a combattere la criminalità e il terrorismo internazionale informatico[74]. Negli anni immediatamente successivi la solerzia della Russia, attraverso la presentazione simili proposte[75], fece sì che

[73] In tal senso si veda PERRITT, *The internet as a Threat to Sovereignty? Thoughts on the internet's Role in Strengthening National and Global Governance*, in *Indiana Journal of Global Legal Studies*, 1998, p. 429; ZIOLKOWSKI, *Confidence Buildings Measures for Cyberspace: legal implication*, 2013, p. 164; MACAK, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers*, in *Leiden Journal of International Law*, 2017, p. 879.

[74] Cfr. A/RES/53/70, 1999.

[75] Si vedano A/RES/54/49 del 1999, A/RES/55/28 del 2000 e A/RES/56/19 del 2001.

nel 2002 l'Assemblea Generale chiedesse al Segretario Generale di istituire un gruppo di Governi allo scopo di riferire sulle regole di diritto internazionale per «strengthening the security of global information and telecommunications system»[76]. Nonostante i migliori auspici sui quali poggiava l'istituzione di un gruppo di diversi governi preposto allo scopo di trovare un punto di incontro sull'applicabilità del diritto internazionale al cyberspazio, il primo incontro del gruppo, denominato *Group of Government Experts* (UN GGE), composto da 15 Membri rappresentativi dei diversi Paesi sulla base di una equa distribuzione geografica, non ebbe un esito positivo: il consenso per adottare l'atto finale non fu raggiunto e il report quindi non fu mai emanato[77].

Malgrado l'epilogo negativo a cui si è giunti nel corso del primo incontro, a partire da quell'anno con frequenza regolare il GGE si è riunito in cinque diverse occasioni[78]. Le più importante delle quali sono state senz'altro quelle

[76] Cfr. A/RES/56/19, del 2002.

[77] Sul punto si veda HENRIKSEN, *The End of the road for the UN GGE process: The future regulation of cyberspace*, in *Journal of cybersecurity*, 2019, p. 2.

[78] Il secondo incontro è stato stabilito con apposita Risoluzione dell'Assemblea Generale del 2005 in cui si chiedeva al GGE di continuare a studiare le minacce che l'uso delle nuove tecnologie potevano determinare, con l'auspicio di trovare misure più intense di cooperazione tra gli Stati partecipanti. La peculiarità dell'incontro è stata determinata dal fatto che pochi anni prima si era verificato uno dei più rilevanti attacchi informatici sul piano internazionale (precisamente, quello avverso l'Estonia e quello successivo intercorso durante la guerra tra Russia e Georgia). L'avvenimento non ha avuto un rilevo esclusivamente teorico, ma ha messo in luce come l'assenza di un accordo sulle regole internazionali da applicare al cyberspazio potesse portare a sferrare attacchi e, di conseguenza, istaurare conflitti senza che questi fossero disciplinati. Il report finale dunque sottolineava che gli Stati avevano usato le nuove tecnologie come uno strumento di *intelligence* al solo fine di favorire i loro scopi politici. Esso quindi richiedava agli Stati di sviluppare una visione comune sui comportamenti da assumere al fine di evitare ulteriori rischi di instabilità. In ultima analisi, il Report, pur mancando di un assetto giuridico determinato e stabile per il prosieguo dello studio, ha certamente avuto il pregio di dimostrare un consenso generale da parte dei partecipanti per il futuro sviluppo delle regole internazionali applicabili al cyberspazio. E infatti è proprio grazie ad esso che nel 2011, l'Assemblea Generale ha organizzato il terzo incontro al fine di discutere lo specifico tema "*norms, rules or principles of responsible behaviour of States* (cfr. A/RES/66/24, 2011). Anche in questa occasione, l'incontro era stato preceduto da un ulteriore attacco informatico, cd. *Stuxnet*, che ha inevitabilmente condizionato l'andamento dei negoziati. All'interno del Report

del 2015 e del 2017, entrambe saranno esaminate nel prosieguo della nostra analisi.

Nel dicembre del 2013, l'Assemblea Generale ha istituito il quarto GGE e nel 2015 il Gruppo ha adottato per consenso un ulteriore Report in cui vengono chiariti ed approfondite diversi aspetti.

In primo luogo, viene chiarito che gli Stati, al fine di tutelare la sicurezza internazionale delle attività svolte tramite l'utilizzo di tecnologie informatiche e i diritti umani, sono tenuti a rispettare la Risoluzione dell'Assemblea Generale riguardante 'il diritto alla privacy nell'era digitale'[79] (sul punto si rimanda al cap. 3, par. 2). A ciò si aggiungono una

si può leggere, per la prima volta, che il diritto internazionale – e in particolare la Carta delle Nazioni – e precipuamente il principio di sovranità si applicano alle condotte assunte dagli Stati nel cyberspazio. Le conclusioni a cui giunge l'atto finale, seppur ancora in uno stato primordiale, sono particolarmente rilevanti perché esse riflettono l'emergente consenso nel considerare il cyberspazio uno spazio sottoposto alle medesime regole di diritto internazionale che governano gli ulteriori domini fisici. Cfr. HENRIKSEN, *op.cit.*, p. 3.

[79] Il documento è stato inteso da parte della dottrina come uno spartiacque rispetto al passato e un punto di partenza ideale per un'effettiva salvaguardia della privacy nell'era di internet. La Risoluzione, adottata per consenso nel dicembre del 2013, rappresenta il più importante documento emanato dall'Assemblea Generale in materia di diritto alla privacy e sorveglianza di massa da parte degli Stati e mira all'applicazione degli *standard* di tutela previsti in materia di diritti umani anche alle attività di intercettazione delle comunicazioni e di archiviazione dei dati personali. La risoluzione inoltre ha avuto un ruolo di catalizzatore per le attività delle Nazioni Unite in tema di sorveglianza e diritto alla privacy, demandando all'Alto Commissario per i diritti umani il compito di fornire un report sulla protezione e promozione del diritto alla privacy "*in the context of domestic and extraterritorial surveillance and/or interception of digital communications and the collections of personal data, including on mass scale* (…)". Ebbene, all'esito delle consultazioni, il report redatto dall'Alto Commissario fornisce diverse indicazioni sul rapporto intercorrente tra sorveglianza di massa e diritto alla privacy, giungendo altresì a conclusioni di non poca importanza.

Più dettagliatamente, il documento definisce come potenziale interferenza con il diritto alla privacy la mera possibilità che una comunicazione sia intercettata e non solo dunque quando tale comunicazione sia stata effettivamente sottoposta a intercettazioni. Inoltre, il report sottolinea come la perdurante differenza tra il contenuto delle comunicazioni e i *metadata* deve ritenersi ormai superata, in quanto del tutto anacronistica ed irrilevante rispetto all'attuale contesto in cui si sviluppano le comunicazioni. Questa affermazione ha non poca rilevanza se si considera che la caratteristica insita dei metadata è proprio quella di non rivelare il contenuto delle comunicazioni. Infine, il report, nonostante qualifichi il diritto alla privacy come un diritto derogabile, indica altresì che per stabilire se una interferenza con il diritto alla privacy possa essere considerata arbitraria o illecita è necessario far riferimento ai principi di legalità,

serie di raccomandazioni rivolte agli Stati circa il modo in cui il diritto internazionale deve essere applicato al cyberspazio. Anzitutto, viene ribadito che gli obblighi derivanti dal diritto internazionale e in particolare quelli della Carta delle Nazioni Unite rappresentano la cornice giuridica essenziale per le azioni intraprese nel mondo virtuale nonché rappresentano il punto di partenza per esaminare il modo in cui il diritto internazionale deve essere applicato[80]. Partendo da quest'ultimo aspetto, il GGE identifica alcuni principi di diritto internazionale che avrebbero effetti anche in relazione al nuovo spazio virtuale, vengono infatti espressamente menzionati il principio di sovranità, il divieto dell'uso della forza, il rispetto dei diritti umani e delle libertà fondamentali e il divieto di ingerenza negli affari interni degli altri Stati[81]. A ciò si aggiunge che la sovranità statale e le norme ad essa connesse vengono applicate a tutte le attività che lo Stato svolge nel cyberspazio, inoltre le infrastrutture tecniche che compongono la Rete (quelle che sono state identificate come il primo livello che compone il cyberspazio) sono soggette alla giurisdizione dello Stato territoriale sul quale esse si trovano[82]. Oltre agli aspetti relativi all'uso pacifico del cyberspazio, la Risoluzione affronta altresì alcuni aspetti connessi alla responsabilità degli Stati[83]. A tal proposito viene imposto agli Stati di non utilizzare *proxies* al fine di commettere illeciti internazionali e di assicurarsi che il loro territorio non venga usato da attori non statali al fine di commettere le medesime condotte.

---

necessità e proporzionalità così come definiti e sviluppati nel diritto internazionale dei diritti umani. Cfr. NINO, *La risoluzione dell'Assemblea Generale delle Nazioni Unite sulla tutela della privacy nell'era digitale: importanti luci, ma non poche ombre*, in *Diritto del commercio internazionale*, 2014, p. 768.

[80] Cfr. General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/150, 22 luglio 2015, p. 12.

[81] *Ibidem.* Di questo aspetti si darà conto più diffusamente nei capitoli successivi dell'elaborato.

[82] *Ibidem*.

[83] Sul tema della responsabilità degli Stati e sulla possibile attribuzione degli attacchi informatici ad uno Stato si veda il capitolo 2.

Il GGE affronta anche, seppur sempre in maniera concisa, il delicato tema dell'attribuzione delle condotte illecite, commesse per mezzo di strumenti informatici, agli Stati. A tal proposito chiarisce che il *Progetto di Articoli sulla Responsabilità Internazionale degli Stati* è applicabile anche al contesto cibernetico, tuttavia sottolinea come la semplice indicazione che un'attività sia originata dal territorio di un determinato Stato non sia di per sé sufficiente ad attribuire quella data condotta allo Stato medesimo[84].

Nella parte conclusiva del Report, ove vengono fatte considerazioni per gli sviluppi futuri sul tema, il GGE ribadisce che gli Stati sono gli attori responsabili per il mantenimento di un ambiente tecnologico pacifico e sicuro, ma allo stesso tempo riconosce che una effettiva cooperazione internazionale sia necessaria affinché si possano individuare i meccanismi per permettere la concreta partecipazione anche agli altri attori interessanti come il settore privato, gli studiosi e la società civile[85]. L'intento ultimo sotteso al Report è dunque quello di proseguire nello studio delle problematiche connesse al settore tecnologico al fine di costruire un cyberspazio aperto, sicuro ed accessibile a tutti[86].

Senonché, nonostante il consenso unanime ottenuto nel corso dell'incontro del 2015, va registrato un notevole cambio di tendenza avutosi nel corso dell'ultimo incontro, nel 2017[87], in cui non è stato raggiunto il

[84] Per ulteriori considerazioni sul tema si rimanda al cap. II.

[85] *General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, p. 12.

[86] Secondo il Report infatti «[t]he Group recommends that Member States give active consideration to the recommendations contained in the present report on how to help to build an open, secure, stable, accessible and peaceful ICT environment and assess how they might be taken up for further development and implementation».

[87] Attualmente gli Stati rappresentati all'interno del gruppo sono 20 e sono i seguenti: Antigua and Barbuda, Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russia, Spain, the United Kingdom and the United States. Brazil is the group's chair.

consenso per approvare il relativo Report[88]. I motivi sottesi a tale fallimento possono essere ricondotti essenzialmente al mancato accordo relativamente al paragrafo 34 della bozza finale del Report, all'interno del quale si faceva riferimento alla potenziale applicazione al cyberspazio delle norme relative alla legittima difesa, alle contromisure che gli Stati potevano adottare nel caso di un attacco e più in generale all'applicazione del diritto internazionale umanitario[89].

Tra gli Stati che si sono opposti con maggiore forza si annoverano Cuba, Russia, e Cina[90]. Particolarmente rilevante appare la posizione assunta dai rappresentati dello Stato cubano che attraverso la presentazione di un documento ufficiale hanno spiegato i motivi per i quali non è stato possibile raggiungere un accordo sul testo finale del Report. Secondo quanto si legge nel documento, il tenore del paragrafo 34 avrebbe determinato una conversione del cyberspazio in uno scenario militare ed avrebbe legittimato azioni punitive unilaterali, incluse azioni militari nei confronti degli Stati che lamentavano di essere state vittime di illeciti internazionali perpetrati attraverso l'uso delle tecnologie informatiche[91]. Lo stesso delegato cubano

---

[88] SUKUMAR, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, in Lawfare blog, 2017, reperibile online al seguente indirizzo www.lawfareblog.com; SEGAL, *The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What*?, in *Council on Foreign Relations*, 2017, reperibile on line al seguente indirizzo www.cfr.org; HENRIKSEN, *op.cit.*; SCHMITT, VIHUL, *International Cyber Law Politicized: The Un Gge's Failure To Advance Cyber Norms*, in justsecuriy, 2017, reperibile online al seguente indirizzo https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/

[89] *Ibidem*.

[90] HENRIKSEN, *op.cit.* p. 3.

[91] Cfr. *Declaration by Miguel Rodríguez, Representative of Cuba, At The Final Session of Group Of Governmental Experts On Developments In The Field Of Information And Telecommunications In The Context Of International Security*. New York, giugno 23, 2017, secondo cui «I must register our serious concern over the pretension of some, reflected in paragraph 34 of the draft final report, to convert cyberspace into a theater of military operations and to legitimize, in that context, unilateral punitive force actions, including the application of sanctions and even military action by States claiming to be victims of illicit uses of ICTs».

sottolineava altresì come l'equiparazione degli attacchi informatici a dei veri e propri «attacchi armati», secondo quanto previsto dall'art. 51 della Carta delle Nazioni Unite[92], in modo da giustificare nel contesto cibernetico il ricorso alla legittima difesa, non poteva essere condivisa[93]. Anche in relazione al termine 'contromisure' – che secondo il testo va inteso come il 'diritto degli Stati di rispondere ad un illecito internazionale commesso attraverso strumenti informatici' – non si è raggiunta una visione comune. Il motivo principale di tale disaccordo sarebbe da rintracciare nella temuta spaccatura che potrebbe crearsi tra gli Stati tecnologicamente più avanzati e quelli invece che ancora non hanno sviluppato tecnologie tali da poter stare al passo con gli altri Paesi.

Infine, l'ultimo aspetto che ha determinato il mancato accordo e il definitivo fallimento del GGE è quello relativo all'applicazione dell'insieme di norme del diritto internazionale umanitario al cyberspazio. Sul tema invero già in passato la Cina aveva espresso alcune perplessità, constatando che da tale applicazione sarebbe derivato un legittimo uso militare del cyberspazio[94]; allo stesso modo lo Stato cubano aveva rigettato tale

[92] Com'è noto l'art. 51 della Carta delle Nazioni Unite disciplina il diritto degli Stati di agire in legittima difesa. Secondo il dettato dell'articolo infatti «[n]essuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale».

[93] *Declaration by Miguel Rodríguez, Representative of Cuba, At The Final Session of Group Of Governmental Experts On Developments In The Field Of Information And Telecommunications In The Context Of International Security*. New York, June 23, 2017, «[w]e consider unacceptable the formulations contained in the draft, aimed to establish equivalence between the malicious use of ICTs and the concept of "armed attack", as provided for in Article 51 of the Charter, which attempts to justify the alleged applicability in this context of the right to self-defense».

[94] SUKUMAR, *op.cit.*.

evenienza in quanto capace di legittimare uno scenario bellico e azioni militari nello spazio virtuale[95]. Evenienza quest'ultima che avrebbe determinato, anche in questo caso, una sostanziale disparità tra gli Stati (come gli Stati Uniti) che hanno già da tempo ampliato e fortificato le proprie capacità tecnologiche e quelli invece che hanno un livello di sviluppo nettamente inferiore (come, ad esempio, Cuba). A ciò va aggiunta una considerazione di carattere più generale, e cioè la difficile applicazione al contesto cibernetico di alcuni principi cardini del diritto internazionale umanitario come ad esempio quello relativo alla distinzione tra civili e obiettivi militari.

Ebbene, l'analisi fin qui condotta ha messo in luce le concrete difficoltà nel raggiungere un accordo circa le norme di diritto internazionale applicabili e anche il modo in cui queste vanno interpretate per meglio adattarsi allo spazio cibernetico. È possibile allora svolgere alcune riflessioni, che si articoleranno su tre distinti aspetti, sui motivi per cui si è giunti a tale conclusione.

In primo luogo, appare chiaro che nonostante i diversi tentativi svolti nelle varie sedi internazionali la possibilità di adottare un trattato multilaterale vincolante per tutti gli Stati, che disciplini in modo esaustivo le diverse declinazioni internazionali del cyberspazio, è un'impresa particolarmente ardua. E ciò in realtà non è imputabile ad una mancata ovvero una scarsa iniziativa da parte degli Stati, ma piuttosto al difficile raggiungimento di una visione comune che possa mettere d'accordo i diversi Stati coinvolti. Infatti, solo per fare qualche esempio, oltre alle già citate Conferenze, summit e Gruppi di esperti, già nel 1996 la Francia emanò una iniziale proposta dal

[95] *Declaration by Miguel Rodríguez, Representative of Cuba, At The Final Session of Group Of Governmental Experts On Developments In The Field Of Information And Telecommunications In The Context Of International Security.* New York, June 23, 2017.

titolo *Charter for International Cooperation on the internet*[96]. La proposta francese mirava alla creazione di un accordo internazionale equiparabile a quanto avutosi per il diritto internazionale del mare[97].

[96] MACAK, *op.cit.*, p. 880. La proposta francese è stata richiamata dal Consiglio dei Ministri dell'Unione Europea all'interno della risoluzione sul tema *on illegal and harmful content on the internet*, ove si può leggere «the council of the european union and the representatives of the governments of the member states, meeting within the council, having regard to the Treaty establishing the European Community, Having regard to the request to the Commission following the informal meeting of Ministers of Telecommunications and Ministers of Culture and Audiovisual Affairs held in Bologna on 24 April 1996 to produce a summary of problems posed by the rapid development of internet, and to assess, in particular, the desirability of Community or international regulation, Having regard to the informal meeting of Ministers of Justice and Home Affairs on 26 and 27 September 1996 in Dublin which discussed further cooperation between Member States to combat trade in human beings and sexual abuse of children, and stressed the importance of three action projects, Having regard to the conclusions on paedophilia and the internet of the Council held on 27 September 1996, which agreed to the extension of the Working Party established following the Bologna meeting to representatives of Ministers of Telecommunications as well as to access and service providers, content industries and users with a view to presenting concrete proposals/possible measures taking account also of United Kingdom measures to combat the illegal use of internet or similar networks, in time for the Council of 28 November, Having regard to the proposal for a charter for international cooperation on the internet placed before the OECD by France, Having regard to the session of the Council of 8 October, at which the need for further analysis of the issues underlying development of information society policy internationally and the need for coordination between initiatives relating to the subject was recognized, and the German proposal to host an international conference dedicated to this end to be prepared in close cooperation with the Commission and Member States was welcomed, Having regard to the declaration of the Council and of the Ministers for education meeting within the Council of 20 December 1996 on protection of children and countering paedophilia, Having regard to the Commission's undertaking to submit to the Dublin European Council in December 1996 an updated version of the 'Europe's way to the information society` action plan in order to clarify the coherence of the various steps undertaken, Noting the recent communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions on illegal and harmful content on the internet, and the Commission Green Paper on the protection of minors and human dignity in audiovisual and information services, both of which will have to be considered in greater detail, Recalling the positive benefits offered by the internet in particular in education, by empowering citizens, lowering the barriers to the creation and distribution of content and offering wide access to even richer sources of digital information, Recalling the need to combat illegal use of the technical possibilities of internet in particular for offences against children, 1. Welcome the report of the Commission Working Party on illegal and harmful content on the internet and undertake to consider the proposals in that report taking into account further discussions on the Commission communication on illegal and harmful content on the internet and on the Green Paper on the protection of minors and human dignity in audiovisual and information services; 2. Take into account the work accomplished in the field of justice and home affairs; 3. Suggest that special

Successivamente, altre proposte sono state avanzate unitamente dalla Cina e dalla Russia e si sono concretizzate nella presentazione dell'*International Code of Conduct for Information Security* all'Assemblea Generale rispettivamente nel 2011 e nel 2015[98].

attention continue to be paid by the Commission and Member States to coordination of the efforts of groups working in all the relevant fields; 4. Invite the Member States to start with the following measures: encourage and facilitate self-regulatory systems including representative bodies for internet service providers and users, effective codes of conduct and possibly hot-line reporting mechanisms available to the public; encourage the provision to users of filtering mechanisms and the setting up of rating systems; for example the PICS (platform for internet content selection) standard launched by the international World-Wide-Web consortium with Community support should be promoted; participate actively in the International Ministerial Conference to be hosted by Germany and encourage attendance by representatives of the actors concerned; 5. Request the Commission, as far as Community competences are concerned, to: ensure the follow-up and the coherence of work on the measures suggested in the abovementioned report, taking into account other relevant work in this field and to reconvene the Working Party as necessary to monitor progress and take further initiatives if appropriate; foster coordination at Community level of self-regulatory and representative bodies; promote and facilitate the exchange of information on best practice in this area; foster research into technical issues, in particular filtering, rating, tracing and privacy-enhancing, taking into account Europe's cultural and linguistic diversity; consider further the question of legal liability for internet content; 6. Recommend that the Commission, in the framework of Community competences, and Member States take all necessary steps to enhance the effectiveness of the measures referred to in this resolution through international cooperation building on the results of the International Ministerial Conference and in discussions in other international forums». Cfr. *Resolution of the Council and of the Representatives of the Governments of the Member States, meeting within the Council of 17 February 1997 on illegal and harmful content on the internet.*

[97] WU, *Cyberspace Sovereignty? The internet and the International System*, in *Harvard Journal of Law and Technology*, 1997, p. 660

[98] La proposta russa-cinese è senz'altro suggestiva nonostante gli Stati promotori siano stati più volte definiti come 'nemici di internet', in virtù dello stretto controllo governativo da loro esercitato nel cyberspazio, ed infatti in essa si possono leggere le seguenti proposte «1. To comply with the UN Charter and universally recognized norms governing international relations, which enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all states, respect for human rights and fundamental freedoms, as well as respect for diversity of history, culture, and social systems of all countries. 2. Not to use ICTs including networks to carry out hostile activities or acts of aggression and pose threats to international peace and security. Not to proliferate information weapons and related technologies. 3. To cooperate in combating criminal and terrorist activities which use ICTs including networks, and curbing dissemination of information which incites terrorism, secessionism, and extremism or undermines other countries' political, economic, and social stability, as well as their spiritual and cultural environment. 4. To endeavor to ensure the supply chain security of ICT products and services, prevent other states from using their resources,

Senonché nessuna delle suddette proposte è stata accolta con particolare entusiasmo né dagli altri Stati[99] né tantomeno dalla dottrina. Alcuni Autori infatti hanno definito l'eventualità di un trattato multilaterale sul tema come un'ipotesi prematura e al momento del tutto trascurabile[100].

critical infrastructures, core technologies, and other advantages, to undermine the right of the countries, which accepted this Code of Conduct, to independent control of ICTs, or to threaten other countries' political, economic and social security. 5. To reaffirm all states' rights and responsibilities to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage 6. To fully respect the rights and freedom in information space, including rights and freedom of searching for, acquiring and disseminating information on the premise of complying with relevant national laws and regulations. 6. To promote the establishment of a multilateral, transparent, and democratic international management of the internet to ensure an equitable distribution of resources, facilitate access for all, and ensure a stable and secure functioning of the internet. 7. To lead all elements of society, including its information and communication private sectors, to understand their roles and responsibilities with regard to information security, in order to facilitate the creation of a culture of information security and the protection of critical information infrastructures. 8. To assist developing countries in their efforts to enhance capacity building on information security and to close the digital divide. 9. To bolster bilateral, regional, and international cooperation, promote the United Nations' important role in formulation of international norms, peaceful settlement of international disputes, and improvement of international cooperation in the field of information security, and enhance coordination among relevant international organizations. 10. To settle any dispute resulting from the application of this Code through peaceful means and refrain from the threat or use of force».

[99] Si veda, ad esempio, la posizione espresso dal Regno Unito nel document intitolato 'Response to General Assembly resolution 68/243 'Developments in the field of information and telecommunications in the context of international security', del Maggi 2014, in cui viene sottolieato che 'attempts to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would [not] make a positive contribution to enhanced international cybersecurity'; KALJURAND, *United Nations Group of Governmental Experts: The Estonian Perspective*, in OSULA, RÕIGAS (a cura di), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, 2016, p. 123.

[100] Si veda a tal proposito GOLDSMITH, *Cybersecurity Treaties: A Skeptical View*, in BERKOWITZ (a cura di), *Future Challenges in National Security and Law*, 2011, p. 2 consultabile online al seguente indirizzo www.hoover.org/sites/default/files/research/docs/futurechallenges_goldsmith.pdf; WAXMAN, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011, p. 425–426; HATHAWAY, *The Law of Cyber-Attack*, in *California Law Review*, 2012, p. 882; EICHENSEHR, *The Cyber-Law of Nations*, in *Georgetown Law Journal*, 2015, p. 356; SCHMITT, VIHUL, *The Nature of International Law Cyber Norms*, in Osula, Rõigas (a cura di), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, 2016, p. 39.

Ebbene, oltre alla difficile ipotesi di raggiungere una visione comune, sorretta da un accordo internazionale, va aggiunto che molto spesso gli Stati si sono dimostrati poco propensi allo sviluppo di norme internazionali consuetudinarie specificamente attinenti al cyberspazio. Il problema invero si pone soprattutto a causa della poca trasparenza con cui gli Stati decidono di affrontare i problemi connessi alla realtà virtuale, e quindi con la conseguente difficile ricostruzione di una prassi in materia[101]. Ciò è dovuto essenzialmente alla reticenza che gli Stati mostrano nel rivelare le proprie strategie nel cyberspazio a causa delle possibili conseguenze e ricadute sulla loro sicurezza nazionale[102]. A ciò si aggiunge una altrettanta complessa individuazione dell'elemento soggettivo della consuetudine[103]. A ben vedere infatti le dichiarazioni degli Stati emanate per il tramite di documenti ufficiali non sembrano assumere quel carattere *di obbligatorietà* richiesta dall'elemento soggettivo della consuetudine.

Ciononostante va rilevato che se si escludono dal novero delle norme tutte quelle relative ai conflitti che possono sorgere tra gli Stati − e quindi l'insieme dei vincoli che discendono dalla connessa responsabilità internazionale e le relative conseguenze[104] − è possibile individuare diversi

[101] Cfr. MACAK, *op.cit.*, p. 881.

[102] Cfr. SCHMITT, VIHUL, *The Nature of International Law Cyber Norms*, in A.M. OSULA, H. ROIGAS (a cura di), *op.cit.*, p. 43.

[103] *Ibidem*.

[104] Questo specifico aspetto verrà trattato in maniera più approfondita nel corso del secondo capitolo. In questa sede però pare opportuno riprendere un recente esempio che dimostra proprio le difficoltà nel trovare il modo in cui alcuni aspetti del diritto internazionale debbano interfacciarsi con il cyberspazio. Il riferimento va al *US Law of War Manual*, adottato nel 2015 ed aggiornato nel 2016, un manuale che tra i diversi aspetti trattati fa esplicito riferimento alle *cyber operations*. Al suo interno infatti si può leggere «[t]his Chapter addresses the law of war and cyber operations. It addresses how law of war principles and rules apply to relatively novel cyber capabilities and the cyber domain. As a matter of U.S. policy, the United States has sought to work internationally to clarify how existing international law and norms, including law of war principles, apply to cyber operations.1 Precisely how the law of war applies to cyber operations is not well-settled, and aspects of the law in this area are likely to continue to develop, especially as new cyber capabilities are developed and States determine their views in response to such development» (Cfr. DEPARTMENT OF DEFENSE, *Law of War Manual*, 2016, p.

Stati che, attraverso documenti ufficiali, hanno manifestato la loro volontà nell'applicare il diritto internazionale al cyberspazio e ciò può risultare particolarmente utile non tanto per la ricostruzione di norme consuetudinarie, ma piuttosto per il modo in cui gli Stati decidono di declinare il diritto internazionale nel contesto cibernetico. A tal proposito diversi sono gli esempi che possono essere presi in considerazione.

In primo luogo, è ormai nota la dichiarazione emanata dal Governo statunitense in merito al rapporto tra diritto internazionale e il cyberspazio. In essa infatti si può leggere come lo sviluppo delle norme di condotta degli Stati nel cyberspazio non richieda la creazione di nuove norme di diritto

1011 ss). Il manuale, nonostante l'apprezzabile tentativo volto a fornire alcune indicazioni circa il modo in cui alcune norme del diritto internazionale vadano declinate in relazione al cyberspazio, appare del tutto includente su alcuni aspetti particolarmente problematici ed ostici. Ad esempio in relazione al problema dell'attribuzione degli attacchi informatici agli Stati, oppure gli aspetti relativi all'individuazione delle infrastrutture critiche da poter attaccare. In dottrina infatti è stato adeguatamente sottlineato come «[a]s an indication of a major power's willingness to submit to meaningful international regulation of its cyber operations, especially during armed conflict, the *Manual* offers mixed signals. On one hand, the *Manual* includes a number of statements that suggest strong US interest in refining and clarifying norms applicable to states' cyber operations. These observations and seeming commitments offer hope to those interested in resorting to international law and norms to regulate cyberspace. Moreover, the *Manual*'s cyber operations chapter is a resounding rejection of the Exceptionalist view on the relationship between international law and cyberspace. The *Manual* unequivocally regards existing international law as a source of binding norms on states' conduct of cyber operations. To a limited extent and on limited subjects, the *Manual* also follows up on US purported commitment to further cyber law development and refinement. The *Manual*'s sections on neutrality, proportionality, and precautions against civilian harm offer constructive guidance and seeming *opinio juris* on important ambiguities. Each section offers simultaneously clear expressions of applicable legal standards and useful illustrations of how those standards are understood to operate with respect to modern cyber operations. On the other hand, the *Manual* does little of its own accord to resolve many of the unsettled and developing provisions it notes as problematic. For instance, the *Manual* resists adopting a specific analytical methodology for sorting the legal significance of cyber operations that produce effects short of destruction or violence. The *Manual* might, in relatively short order, have announced a clear position with respect to what particular cyber operations or consequences thereof relate to the *ratione materiae* of the law of war». Per una ricostruzione più approfondita del tema si rimanda WATTS, *Cyber Law Development and the United States Law of War Manual*, in OSULA, ROIGAS (a cura di) *International Cyber Norms: Legal, Policy and Industry Perspectives*, CCDCOE, Tallin, 2016, p. 49ss.

internazionale consuetudinario, né tanto meno il nuovo spazio cibernetico rende il diritto internazionale esistente obsoleto. Secondo gli Stati Uniti le norme di diritto internazionale che veicolano i comportamenti degli Stati − sia in tempo di pace che in guerra − sono applicabili anche al cyberspazio. Ciononostante, però, le peculiarità e le caratteristiche tecniche di quest'ultimo rendono necessari ulteriori approfondimenti sia per chiarire *come* tali norme debbano essere concretamente applicate e sia per individuare quali ulteriori comportamenti gli Stati devono adottare affinché si possano eventualmente integrare tali norme. A tal fine bisogna continuare a lavorare sul piano internazionale allo scopo di raggiungere un maggiore consenso da parte degli altri Stati membri della comunità internazionale, partendo da un assunto di base e cioè dall'idea che la norma da applicare è quella relativa al mantenimento della pace[105].

[105] Cfr. *International Strategy for Cyberspace*. *Prosperity, Security and Openess in a Neteworked World*, maggio 2011, p. 9. Per quello che a noi interessa, vale la pena sottolineare come all'interno del documentro, tra le altre cose, si può altresì leggere «[r]ules that promote order and peace, advance basic human dignity, and promote freedom in economic competition are essential to any international environment.These principles provide a basic roadmap for how states can meet their traditional international obligations in cyberspace and, in many cases, reflect duties of states that apply regardless of context.The existing principles that should support cyberspace norms include: •Upholding Fundamental Freedoms: States must respect fundamental freedoms of expression and association, online as well as off. • Respect for Property: States should in their undertakings and through domestic laws respect intellectual property rights, including patents, trade secrets, trademarks, and copyrights. • Valuing Privacy: Individuals should be protected from arbitrary or unlawful state interference with their privacy when they use the internet. • Protection from Crime: States must identify and prosecute cybercriminals, to ensure laws and practices deny criminals safe havens, and cooperate with international criminal investigations in a timely manner. • Right of Self-Defense: Consistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace. Deriving from these traditional principles of interstate conduct are responsibilities more specific to cyberspace, focused in particular on preserving global network functionality and improving cybersecurity.Many of these responsibilities are rooted in the technical realities of the internet.Because the internet's core functionality relies on systems of trust (such as the Border Gateway Protocol), states need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader internet. Likewise, in designing the next generation of these systems, we must advance the common interest by supporting the soundest technical standards and *governance* structures, rather than those that will simply enhance national

Volgendo lo sguardo ai Paesi europei non mancano casi che depongono nello stesso senso. La Francia ad esempio ha adottato il *French National Digital Security Strategy*, all'interno del quale viene sottolineato che il governo francese riconosce l'applicazione del diritto internazionale già esistente al cyberspazio, inoltre viene aggiunto che al fine di rinforzare la fiducia tra i membri della comunità internazionale la Francia si impegnerà a perpetrare un dialogo costruttivo e pacifico con gli ulteriori attori coinvolti nel cyberspazio[106].

Anche l'Olanda ha adottato il documento intitolato *Building Digital Bridges: International Cyber Strategy Towards an Integrated International Cyber Policy* in cui si fa espresso riferimento all'applicabilità dell'insieme di norme del diritto internazionale al cyberspazio. Il governo, tuttavia, aggiunge che il suo scopo primario è chiarire il modo in cui queste norme devono essere applicate e favorire la conclusione di un accordo non vincolante su *standard* di condotta che gli Stati devono assumere al fine di favorire un uso pacifico del cyberspazio e lo sviluppo della sicurezza internazionale[107].

---

prestige or political control. Emerging norms, also essential to this space, include: • Global Interoperability: States should act within their authorities to help ensure the end-toend interoperability of an internet accessible to all. • Network Stability: States should respect the free flow of information in national network configurations, ensuring they do not arbitrarily interfere with internationally interconnected infrastructure. • Reliable Access: States should not arbitrarily deprive or disrupt individuals' access to the internet or other networked technologies. • Multi-stakeholder *Governance*: internet *governance* efforts must not be limited to governments, but should include all appropriate stakeholders. • Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse».

[106] Cfr. *French National Digital Security Strategy*, p. 8, 38 e 40.

[107] La dichiarazione propone ulteriori elementi interessanti che per completezza vale la pena riportare in questa sede. In particolare, il paragrafo 4 del documento, rubricato *Policy priorities of an international cyber strategy*, definisce in modo chiaro la visione del governo olandese nella materia *de qua*. Al suo interno infatti si può leggere «[t]he vision for the international cyber strategy has been fleshed out into the following policy priorities: Economic growth and sustainable development of the internet; Effective internet *governance*; Further enhancement of cybersecurity; Effective efforts to stop cybercrime; International peace, security and

Infine, anche l'Italia ha emanato una dichiarazione nel corso del G7 'sul comportamento responsabile degli Stati nel cyberspazio'. La dichiarazione affronta diverse problematiche, tra cui la responsabilità internazionale degli Stati per attacchi informatici[108]; i problemi relativi all'attribuzione delle

stability; rights and online freedom. Più dettagliatamente, il punto relativo ai futuri sviluppi in materia di cybersicurezza è quello che ci sembra essere il più rilevante. Nel testo, a tal proposito, si può leggere « Security, freedom and social growth exist in a dynamic balance. It is not possible to guarantee an open and free digital domain without security. With that in mind the government is actively working to promote and enhance cybersecurity – bilaterally, regionally and multilaterally. In this way, both the Netherlands and the digital domain can be kept safe and secure. As the CSBN has noted in its annual reports, the cyber threat posed by states, criminals and nonstate actors to the Netherlands' political, economic and social interests is real and growing. The government has therefore been working for some time on enhancing security in cyberspace, as stated in the strategic objectives laid down in NCSS 2. These objectives, which also apply internationally, include boosting resilience to cyberattacks and protecting vital interests in cyberspace; public-private partnership; detection, response and awareness-raising; and education. The Netherlands also endeavours to lend its guidance to relevant initiatives at international level, given that cyberspace has no borders and security can only be achieved through joint efforts to address the weakest links». Cfr. *Building Digital Bridges: International Cyber Strategy Towards an Integrated International Cyber Policy*, *passim.* Per una disamina giuridica sia interna che internazionale sulle politiche del governo olandese in material si veda CLAVER, *Governance of cyber warfare in the Netherlands: an exploratory investigation*, in *The International Journal of Intelligence, Security, and Public Affairs*, 2018, p. 155 ss.

[108] Si può leggere infatti «[r]ibadiamo la responsabilità degli Stati di astenersi, nelle relazioni internazionali, dal ricorso alla minaccia o all'uso della forza contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato o in qualunque altra maniera incompatibile con gli scopi delle Nazioni Unite; Rileviamo che, ai fini della prevenzione dei conflitti e della pacifica risoluzione delle controversie, il diritto internazionale fornisce anche un quadro per le risposte degli Stati a illeciti che non assumono le proporzioni di un attacco armato – e che possono comprendere cyber attività con intento doloso. Tra le altre risposte legittime, uno Stato che sia vittima di un atto illecito a livello internazionale, può, in talune circostanze, adottare contromisure proporzionate, anche di natura informatica, nei confronti dello Stato che si è reso responsabile dell'illecito, per indurlo ad assolvere agli obblighi internazionali».

cyber attività (tra cui gli attacchi informatici) ad uno Stato[109]; il rispetto dei diritti umani e dei relativi trattati anche per le attività svolte su internet[110].

Oltre a ciò, e per quello che a noi interessa, anche nelle dichiarazioni dell'Italia è possibile notare la volontà dello Stato di impegnarsi a promuovere un quadro strategico per le prevenzione dei conflitti, la cooperazione e la stabilità nel cyberspazio, «tramite il riconoscimento dell'applicabilità del diritto internazionale esistente al comportamento degli Stati nel cyberspazio»[111]; inoltre al fine di accrescere la predicibilità e la stabilità del cyberspazio viene richiesto agli altri Stati di chiarire pubblicamente le rispettive posizioni in merito al *modo* in cui il diritto internazionale deve essere applicato al fine «di migliorare la trasparenza e disegnare un quadro di attese di comportamento da parte degli altri Stati»[112].

4. L' impulso da parte di soggetti diversi dallo Stato per la 'creazione' di regole internazionali applicabili al cyberspazio

Come si è avuto modo di vedere finora, gli Stati hanno avuto non poche difficoltà nel raggiungere una comune visione circa le regole da applicare al cyberspazio. Ad essere più precisi, va rilevato come gli Stati non sono stati

[109] Sul tema si afferma «[r]ileviamo che il diritto consuetudinario internazionale in materia di responsabilità di Stato indica gli standard per l'attribuzione di atti agli Stati, che possono applicarsi alle attività nel cyberspazio. A tale riguardo, gli Stati non possono sottrarsi alla responsabilità legale per cyber illeciti perpetrati a livello internazionale tramite *proxy*. In sede di attribuzione di un illecito internazionale a un altro Stato o di adozione di azioni di risposta, lo Stato dovrà agire in conformità al diritto internazionale. In questo quadro, lo Stato valuterà i fatti e sarà libero di maturare una decisione in linea con il diritto internazionale, con riferimento all'attribuzione di un cyber illecito a un altro Stato».

[110] In questo caso viene affermato «[r]iaffermiamo altresì che gli stessi diritti di cui gli individui godono quando non sono in Rete, debbano essere tutelati in Rete e ribadiamo l'applicabilità nel cyberspazio del diritto internazionale in materia di diritti umani, compresa la Carta delle Nazioni Unite, il diritto consuetudinario internazionale ed i pertinenti trattati».

[111] Cfr. *Dichiarazione del G7 sul Comportamento Responsabile degli Stati nel Cyberspazio*, Lucca, 11 aprile 2017, p. 2.

[112] *Ibidem*.

capaci di raggiungere né un accordo internazionale sullo specifico tema[113] né tantomeno individuare in maniera omogenea in che modo le norme di diritto

[113] Con questa affermazione non si vuole sostenere che non esistano alcuni trattati regionali o settoriali che prendano in considerazione lo specifico tema delle attività compiute nel cyberspazio. A tal proposito sono note, ad esempio, la Convenzione del Consiglio d'Europa sulla Criminalità informatica (anche conosciuta come Convenzione di Budapest) e la Convenzione dell'Unione Africana in materia di Cybersicurezza. È utile riportarne brevemente alcune parti sicché si possano svolgere alcune veloci considerazioni. Per quanto concerne la Convezione di Budapest nel preambolo è possibile leggere «The member States of the Council of Europe and the other States signatory hereto, Considering that the aim of the Council of Europe is to achieve a greater unity between its members; Recognising the value of fostering co-operation with the other States parties to this Convention; Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation; Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks; Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks; Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies; Believing that an effective fight against cybercrime requires increased, rapid and wellfunctioning international co-operation in criminal matters; Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation; Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy; Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (…)». Ebbene, appare chiaro che nonostante il riferimento all'interno del preambolo alla locuzione 'primo accordo internazionale', la Convenzione non è altro che la trasposizione di alcune norme di diritto penale applicate all'ambito degli illeciti internazionali. Non vengono annoverati invece i problemi più rilevanti né viene chiarito il loro ambito di applicazione. Discorso parzialmente diverso va fatto in relazione alla Convenzione adottata dall'Unione Africana. In questo caso infatti la Convenzione affronta tre diversi aspetti particolarmente rilevanti soprattutto nel contesto di alcuni paesi africani, che da molti vengono considerati come '*safe haven for cyber criminals'*: *i)* trasmissioni elettroniche; *ii)* protezione dei dati personali; *iii)* cyber sicurezza e

internazionale consuetudinario già esistenti debbano essere applicate al nuovo dominio.

Preso atto di questa situazione, a noi sembra che nel contesto del cyberspazio si stia assistendo a quell'ipotesi che nella teoria generale del diritto è stata definita come 'the pluratization of international law making'[114], che si caratterizza perché «only a limited part of the exercise of public authority at the international level nowadays materializes itself in the creation of norms which can be considered international legal rules according to a classical understanding of international law»[115].

Secondo questa teoria infatti la creazione delle norme di diritto internazionale non sarebbe più esclusivamente riconosciuta in capo a coloro che esercitano il potere di governo, ma piuttosto essa avverrebbe attraverso una più complessa procedura che involge anche gli attori non statali[116]. Questo modo di procedere è stato definito da parte della dottrina come 'un processo di verticalizzazione'[117], secondo cui appunto la creazione delle norme di diritto internazionale, non essendo più riconducibile all'esercizio

crimini informatici. Anche in questo caso, tuttavia, è agevole constatare la presenza di alcuni punti critici. In primo luogo, la Convenzione non si riferisce al diritto internazionale, anche se le va di certo riconosciuto il pregio di aver affrontato il tema in un contesto particolarmente difficile; in secondo luogo, ed è sicuramente l'aspetto più rilevante, essa non è stata ratificata da nessuno Stato. Per un sintetico approfondimento si veda ROIGAS, *Mixed Feedback on the African Union Convention on Cyber Security and Personal Data Protecion*, in *CCDCOE Incyder Database*, febbraio 2015, consultabile online al seguente indirizzo https://ccdcoe.org/incyder-articles/mixed-feedback-on-the-african-union-convention-on-cyber-security-and-personal-data-protection/

[114] D'ASPREMONT, *Formalism and the Sources of International Law. A Theory of the Ascertainment of Legal Rules*, Oxford, 2011, p. 222.

[115] *Ibidem*, p. 2.

[116] *Ibidem*. A tal proposito si veda Palombino, secondo il quale la prassi dei movimenti insurrezionali può contribuire alla formazione di nuove norme di diritto internazionale consuetudinario. Cfr. PALOMBINO, *Introduzione al diritto internazionale*, Bari, 2019, p. 135.

[117] KLABBERS, *Setting the Scene*, in KLABBERS, PETERS, e ULFSTEIN (a cura di), *The Constitutionalization of International Law*, Oxford, 2009, p. 14. Circa lo specifico ruolo degli attori-non statali si veda, *ex multis*, D'ASPREMONT (a cura di), *Partecipans in the International Legal System − Multiple Perspectives on Non State Actors in International Law*, Londra, 2011.

del potere pubblico da parte degli Stati indipendenti e sovrani, andrebbe altresì ricondotta ad altri attori come organizzazioni internazionali, movimenti di liberazione nazionali, organizzazioni internazionali non governative e anche (o soprattutto) dalla società civile[118].

Ebbene, va precisato sin da subito che non è nostra intenzione esaminare tale fenomeno dal punto di vista della teoria generale del diritto, ma piuttosto si vuole sottolineare come questo processo di commistione di diversi attori direttamente interessati a 'creare' fonti internazionali è particolarmente evidente quando si parla di cyberspazio. A suffragio di tale affermazioni è possibile richiamare due iniziative particolarmente rilevanti, entrambe provenienti non solo da attori non statali ma anche da due diversi settori della società, e cioè quella proposta da Microsoft (una delle aziende *leader* nel settore informatico) e quella che si è concretizzata con l'adozione del cd. Manuale di Tallinn.

La proposta di Microsoft − resa pubblica nel dicembre 2014 attraverso l'adozione di un documento intitolato *International Cybersecurity Norms: Reducing Conflict in an internet-Dependent World* − non è la prima in senso assoluto nel suo genere[119]. Ad essa tuttavia va riconosciuto il primato per essere stata la prima a ricomprendere una serie di specifiche condotte da tenere nel cyberspazio e per essere esclusivamente rivolta agli Stati, nonostante la sua natura privata. Lo scopo principale della proposta era quello di ridurre la possibilità che il cyberspazio fosse usato dagli Stati per condurre azioni militari[120]. A tal fine venivano proposte sei distinte 'norme', attraverso le quali veniva richiesto agli Stati di migliorare le loro capacità

[118] KLABBERS, *op.cit.*, p. 14.

[119] Va riconosciuto infatti che circa quindici anni prima già un'altra rilevante azienda operante nel settore informatico aveva esortato gli Stati a rivedere il loro ruolo e aveva spinto per l'adozione di 'international standard' al fine di regolare alcuni aspetti della vita on line come la sicurezza, la privacy e la tassazione. Cfr.MACAK, *op.cit.*, p. 888.

[120] Cfr. MCKAY e altri, *International Cybersecurityu Norms: Reducing Conflict in an internet-Dependent World*, 2014

difense sul cyberspazio e allo stesso tempo di limitare l'uso di operazioni offensive nei confronti degli altri Stati.

Le norme si articolavano nel seguente modo: *i)* States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services[121]; *ii)* States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them[122]; *iii)* States should exercise

[121] Nella prima norma viene specificato che « The global technology industry is founded on trust, in that consumers, enterprises, and governments depend on ICT for critical functions. Although the private sector can and does invest considerably in efforts to advance and demonstrate the assurance and integrity of products and services, states have the unique capability to direct disproportionately larger resources to exploit these products or services and to taint the broad ICT supply chains by which they are delivered. Exploiting of commercial off-the-shelf (COTS) products and services—which puts at risk every computer user dependent on that technology, even if that user is of no interest to a government—would be an action with the potential to create unacceptable impacts globally, since the degradation of trust in ICT would threaten innovation and economic security. Sophisticated state-resourced tradecraft targeting ICT companies to place backdoors or vulnerabilities in COTS products—or compromising signing keys to enable government to misrepresent the provenance of software—may exceed the commercially reasonable limits of the private sector operational security and integrity controls. Governments should also refrain from undermining international security standards efforts to benefit their own interests». Cfr. *Ibidem*, p. 11.

[122] La seconda norma sottolinea che «It is well-documented that governments around the world are active participants in the cyber vulnerability market and that they exploit gray and black markets.5 The Heartbleed vulnerability, discovered in 2014, fueled additional speculation as to how governments stockpile vulnerabilities in ICT products rather than disclosing them to vendors to fix before they are exploited. In April 2014, in response to specific allegations against the US government, the White House published its framework approach to addressing if or when the federal government may withhold knowledge of a vulnerability from the public: "This administration takes seriously its commitment to an open and interoperable, secure and reliable internet, and in the majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. This has been and continues to be the case."6 The White House further noted that building up a "huge stockpile of undisclosed vulnerabilities" while leaving the internet vulnerable and people unprotected would not be in the national security interest of the United States.

Although the White House reserved the right to use vulnerabilities as a method of intelligence collection, this approach does reflect a positive analysis that short-term gains to advance one objective could also create impacts that threaten other objectives, such as economic growth, technological innovation, and trust in government. We recommend that other governments similarly develop and publicly publish their policies on vulnerability handling and

restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable[123]; *iv)* States should commit to nonproliferation activities related to cyber weapons[124]; *v)* States should limit their engagement in cyber offensive operations to avoid creating a mass event[125]; *vi)* States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace[126].

---

that they have a partiality for reporting vulnerabilities to vendors. When doing so, they should adhere to the principles of Coordinated Vulnerability Disclosure (CVD)». Cfr. *Ibidem,* p. 12.

[123] Nella terza norma, invece, Microsoft fa riferimento a « recognizes that governments will develop cyber weapons and protocols for their own use. When governments do build them, therefore, they should ensure that they are building cyber weapons that are controllable, precise, and not reusable by others, consistent with the concepts of distinction, discrimination, and distribution previously discussed, to limit the impacts associated with these actions». Cfr. *Ibidem*.

[124] Nella quarta si può leggere « As states increase investments in offensive cyber capabilities, care must be taken to not proliferate weapons or techniques for weaponizing code. States should establish processes to identify the intelligence, law enforcement, and financial sanctions tools that can and should be used against governments and individuals who use or intend to use cyber weapons in violation of law or international norms. Furthermore, states should agree to control the proliferation of cyber weapons in cooperation with international partners and, to the extent practicable, private industry. Implementing this norm will not only help limit state actions that could have unacceptable impacts but also will help reduce the possibility that cyber weapons could be used by non-state actors». Cfr. *Ibidem*, p. 13.

[125] Nella penultima norma viene precisato che gli Stati «hould review and update their current policy positions with an appreciation for the unintended consequences or impacts in cyberspace that could escalate conflict, incite war or disproportionately harm civilian ICT. During an armed conflict, as regulated by the law of war, any attack must be justified by military necessity, intended to help in the military defeat of the enemy, with a military objective. Furthermore, the harm caused to civilians or civilian property must be proportional in relation to the concrete and direct military advantage anticipated. In other words, the action should be to advance defined and accepted military objectives and should not create disproportional impacts. These strictures can and should be applied to offensive cyber operations. States should recognize that attacks targeting the confidentiality, integrity, or availability of ICT systems, services, and data can have a mass effect beyond any reasonable sense of proportionality and required global action». Cfr. *Ibidem*.

[126] Infine, nell'ultima norma si può leggere « Although governments play an increasingly important role in cyberspace, the first line of defense against cyber attacks remains the private sector, with its globally distributed telemetry, situational awareness, and well-established incident response functions. There has not been evidence of governmental interference with private sector recovery efforts following a severe cyber attack, but governments should commit to not interfere with the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs), individual response personnel, and technical response systems. Intervening in private sector response and recovery would be akin

Senonché, come era facilmente prevedibile, la proposta di Microsoft non è stata accolta nel migliore dei modi. Infatti, veniva criticato che le norme in essa previste erano rivolte esclusivamente agli Stati e non considerassero invece il ruolo altrettanto importante svolto dal settore privato, e in particolare dalle grandi multinazionali del settore.

A fronte di tali critiche, nel 2016 Microsoft ha proposto un nuovo *White Paper − From Articulation to Implementation: Enabling Progress on Cybersecurity Norms −* nel quale, da un lato, venivano ribadite le norme previste nel documento precedente e, dall'altro lato, veniva fatto riferimento anche al ruolo del settore privato. Quest'ultimo aspetto, nonostante fosse stato menzionato all'interno del documento, veicolava la partecipazione delle aziende, che attraverso le loro capacità tecniche avrebbero contribuito a rendere il dialogo più costruttivo[127], sempre attraverso gli Stati.

Da ultimo, lo sviluppo finale della proposta si è avuto allorquando nel 2017 Microsoft ha richiesto agli Stati di includere le norme da lei proposte in un trattato internazionale intitolato 'Digital Geneve Convention'[128].

La seconda iniziativa da analizzare invece è quella che si è conclusa con l'adozione delle due versioni del Manuale di Tallinn: la prima nel 2013 e la seconda nel 2017. Il processo che ha condotto a tale esito è durato sette anni

---

to attacking medical personnel at military hospitals. Additionally, governments should go one step further and, when asked by the private sector, commit to assist with recovery and response needs that have global and regional implications. For example, repairing cuts in underwater sea cables often requires permits and cross-border movement of technical equipment or experts, and governments can help ensure that those actions are expedited. Alternatively, a cyber event with large-scale impacts, such as the Shamoon attacks in 2012, could require the rapid movement of hardware from one place to another, the need for international technical collaboration between and among governments and the private sector, and the waiving of legal barriers in times of national emergency to facilitate recover». Cfr. *Ibidem*.

[127] Cfr. CHARNEY e altri, *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms*, Microsoft, 2016.

[128] Per una ricostruzione critica della proposta si veda JEUTNER, *The Digital Geneve Convention: A Criticatl Apprasial of Microsoft's Proposal*, in *Journal of International Humanitarian Legal Studies*, 2019, p. 158 ss.

ed è stato svolto da un gruppo di studiosi internazionali capeggiati dal Professor Micheal N. Schmitt. Nonostante l'intera operazione sia stata svolta sotto l'egida della NATO *Cooperative Cyber Defence Centre of Excellence* (CCD COE), va sin da subito evidenziato che il Manuale esprime esclusivamente l'idea degli studiosi che hanno preso parte al progetto e non rispecchia in alcun modo il punto di vista né degli Stati che fanno parte della Nato, né tanto meno della NATO stessa.

Essa si sostanzia in un'opera di natura dottrinale che ha avuto il merito di affrontare in modo sistematico l'intero problema relativo all'applicazione del diritto internazionale al cyberspazio. Come dicevamo il frutto di tale studio ha portato all'adozione di due differenti versioni. La prima, intitolata *Tallinn Manual on the International Law applicable to Cyber Warfare,* consta di 95 regole e affronta per lo più le tematiche relative alle regole dello *ius in bello* e dello *ius ad bellum* applicabili al contesto virtuale. Queste peculiarità in realtà hanno portato ad un'aspra critica da parte degli Stati, soggetti non coinvolti nel processo, i quali hanno espresso perplessità in ragione di una visione esclusivamente militare del cyberspazio[129].

Per questi motivi, la versione aggiornata del Manuale estende il numero di regole previste a 154 e affronta in maniera più ampia il problema relativo al diritto internazionale prevedendo, oltre alle regole già scritte nella versione precedente, anche l'insieme di regole previste nel campo del diritto internazionale in tempo di pace (responsabilità degli Stati, il diritto del mare, i diritti umani).

[129] FLECK, *Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual,* in *Journal of Conflict & Security Law,* 2013, p. 332–335; XINMIN, *Key Issues and Future Development of International Cyberspace Law,* in *China Quarterly of International Strategic Studies,* 2016, p. 128

5. Il valore delle iniziative degli attori non statale nella formazione di regole internazionali applicabili al cyberspazio

Nella parte conclusiva di questo capitolo, dobbiamo chiederci quale sia il valore delle iniziative intraprese dagli attori non statali e se queste possano in qualche modo contribuire alla formazione delle regole applicabili al cyberspazio.

Com'è noto, invero, e come è stato ribadito dalla Commissione del Diritto internazionale in materia di identificazione delle norme internazionali consuetudinarie, la prassi per l'individuazione della consuetudine è riconducibile esclusivamente agli Stati e in alcuni casi alle organizzazioni internazionali[130]. In linea di principio quindi i comportamenti degli altri attori non contribuiscono alla formazione delle norme consuetudinarie, «but may be relevant when assessing the practice»[131] degli Stati e delle organizzazioni internazionali.

In altre parole, non vuol dire che le iniziative intraprese dagli attori non statali siano del tutto irrilevanti nella formazione delle regole di diritto internazionale. Anzi, potremmo addirittura dire che tali atti di *sofw law*, soprattutto laddove esse provengano da soggetti particolarmente rilevanti in quel settore, possano costituire «a vital intermediate stage towards a more rigorously binding system, permitting experiment and rapid

[130] Commissione del diritto internazionale, *Identification of customary international law: Text of the Draft Conclusion Provisionally Adopted by the Drafting Committee*, UN Doc. A/CN.4/L. 872, 30 maggio 2016, p. 2, ove nelle *draft conclusion* n. 4, rubricata *Requirement of practice*, si può leggere «1. The requirement, as a constituent element of customary international law, of a general practice means that it is primarily the practice of States that contributes to the formation, or expression, of rules of customary international law. 2. In certain cases, the practice of international organizations also contributes to the formation, or expression, of rules of customary international law. 3. Conduct of other actors is not practice that contributes to the formation, or expression, of rules of customary international law, but may be relevant when assessing the practice referred to in paragraphs 1 and 2».

[131] *Ibidem*, p. 2.

modification»[132]. Per di più a ciò potrebbe anche aggiungersi, com'è stato sostenuto in dottrina, che la formazione di norme internazionali attraverso l'ausilio di soggetti diversi dagli Stati potrebbe rendere tale processo più inclusivo e multilaterale rispetto ad un sviluppo esclusivamente Stato-centrico[133].

A noi sembra che il fenomeno della creazione di norme internazionali per il cyberspazio sia indicativo di questa tendenza: in mancanza di norme pattizie capaci di regolare in maniera generale tutti i comportamenti rilevanti per il diritto internazionale sul cyberspazio e l'assenza di prassi *chiara* e di *opinio iuris*, il ruolo svolto dagli attori non statali risulta essere particolarmente rilevante al fine di individuare il diritto internazionale applicabile e il modo in cui questo debba declinarsi in relazione al cyberspazio.

A ben vedere, in realtà, il dominio virtuale non è il primo ed unico caso in cui attraverso le iniziative intraprese da attori non statali − per mezzo atti di *soft law* − si sia giunti alla creazione di accordi, successivamente diventati vincolanti, o alla creazione di norme di diritto internazionale consuetudinario. In tal senso è noto infatti il ruolo svolto dal giurista Lemkin dapprima nella promozione e poi nella stesura delle bozze della Convenzione sul Genocidio del 1948[134] oppure dall'influenza che hanno avuto le pressioni svolte dalla ONG *Amnesty International* per l'adozione della convenzione contro la tortura del 1984[135]. Un esempio più recente può essere considerata

[132] Cfr. MACAK, *op.cit.*, p. 892 e la bibliografia riportata nella nota 136:

[133] Cfr. BESSON, *Theorising the Sources of International Law*, in BESSON, TASIOULAS (a cura di), *The Philosofy of International Law*, Oxford, 2010, p. 170-171.

[134] COOPER, *Raphael Lemkin and the Struggle for the Genocide Convention*, 2008, New York, 2008, *passim*.

[135] AMNESTY INTERNATIONAL, *No safe haven for tortures - This rocky road to the Convention against Torture*, 19 novembre 2014

la Convenzione internazionale sulle bombe a grappolo i cui negoziati si sono svolti in presenza di soggetti privati sopravvissuti ai bombardamenti[136].

Si può concludere, dunque, evidenziando come se da un lato il comportamento degli Stati, soprattutto nelle sedi negoziali, continua ad essere caratterizzato da una certa reticenza nell'individuare le norme di diritto internazionali, nonché la loro interpretazione, da applicare al cyberspazio, dall'altro non può parlarsi di una vera e propria crisi del diritto internazionale in tale settore.

A noi sembra più appropriato inquadrare l'attuale situazione come una fase transitoria che con il passare del tempo può portare ad una duplice conseguenza: la creazione di *specifiche* cyber-norme internazionali consuetudinarie ovvero, e in maniera più verosimile, ad una più adeguata interpretazione del diritto internazionale consuetudinario già esistente allo *specifico* settore del cyberspazio[137].

---

[136] Cfr. MACAK, *op.cit.*, p. 894.

[137] In dottrina è stato altresì sostenuto che a causa dei fallimenti dei negoziati nei diversi *fora*, un modo alternativo per poter fare chiarezza sul tema sarebbe quello di demandare la questione alla Commissione del Diritto internazionale. Secondo questa teoria la Commissione avrebbe anzitutto lo scopo di individuare le norme di diritto internazionale rilevanti e, in secondo luogo, chiarire come queste andrebbero applicate alle operazioni informatiche. In questo modo, la Commissione potrebbe effettuare uno studio approfondito per capire anche quali settori del diritto internazionali sono particolarmente lacunosi e quindi favorire un loro sviluppo. Questa riflessione, in ultima analisi, mirerebbe « to consider a new possible forum to continue the international discussions and negotiations on cyber international law, namely referring the question of the interpretation of the international law applicable to cyber operations to the ILC. It has highlighted that the ILC would offer an appropriate platform to involve both States and non-state actors, and to take into account the diversity of approaches to the issue. That being said, we should not be naïve: the ILC does not constitute a panacea to the increasing threats to the international peace and stability of cyberspace. Indeed, norms of international law, and consequently the work of the ILC, are not able to solve all the issues related to state-sponsored cyber operations. Moreover, despite offering some interesting features, especially if compared to other existing solutions, referring the matter to the ILC is not exempt from downsides and is open to the general criticisms of the ILC. In this sense and when compared to the UNGGE or the *Tallinn Manual Process*, the ILC may constitute a solution although an imperfect one». Cfr. DELERUE, *The Codification of the International Law applicable to Cyber Operations: A Matter for the ILC?*, in *Esil Reflections*, 2018, consultabile

Quest'ultima ipotesi, invero, è quella che sembra più adeguatamente percorribile e, a tal fine, un ruolo particolarmente importante è svolto da soggetti diversi dallo Stato (in particolare dalla dottrina e dalle aziende di settore), i quali attraverso l'adozione di atti di *softw law* stanno contribuendo a fare maggiore chiarezza in questo specifico settore. In virtù di queste ultime considerazioni nel prossimo capitolo verranno prese in considerazione le norme di diritto internazionale già esistenti e si cercherà di capire in che modo queste possano o debbano essere declinate per maggiormente aderire alle specifiche caratteristiche del cyberspazio, per compiere questa analisi, come anticipato, non si può prescindere da tutti quegli atti di *soft law* che sono stati, seppur brevemente, analizzati in questo capitolo.

CAPITOLO II
LE NORME DI DIRITTO INTERNAZIONALE APPLICABILI AL CYBERSPAZIO: IL PROBLEMA DEGLI ATTACCHI INFORMATICI

SOMMARIO: 1. Il principio di sovranità e la sua possibile applicazione al cyberspazio. - 2. La nozione di patrimonio comune dell'umanità. – 2.1. La nozione di patrimonio comune dell'umanità in relazione al cyberspazio. – 3. La definizione di attacco informatico rilevante per il diritto internazionale. - 3.1 Divieto dell'uso della forza e attacchi informatici. – 3.1.1. Il caso *stuxnet*. – 3.1.2. L'attacco informatico statunitense nei confronti dell'Iran del 20 giugno 2019. – 4. Il principio del non intervento negli affari interni di uno Stato. – 4.1. Attacchi informatici e

online al seguente indirizzo https://esil-sedi.eu/esil-reflection-the-codification-of-the-international-law-applicable-to-cyber-operations-a-matter-for-the-ilc/

violazione del principio del non intervento. – 5. Il problema dell'attribuzione allo Stato del fatto illecito compiuto da soggetti privati. – 5.1. La possibile attribuzione ad uno Stato di un attacco informatico. - 5.2. *Segue:*. – 5.2.1. L' (inversione dell') onere della prova. - 5.2.2. Lo standard di prova: il caso delle elezioni statunitensi del 2016 e l'affare Stuxnet. – 5.3. Il possibile ricorso a criteri alternativi: il regime della responsabilità oggettiva. - 6. Il principio di *due diligence* e la sua rilevanza nel contesto degli attacchi informatici.

1. Il principio di sovranità e la sua possibile applicazione al cyberspazio

Il presente capitolo deve necessariamente prendere le mosse dall'assunto, precedentemente esaminato, per cui od oggi non è possibile affermare l'esistenza di nome consuetudinarie specifiche per il cyberspazio né tantomeno obblighi discendenti da accordi internazionali(v. cap. I).

Ciò detto, quindi, scopo di questo capitolo è quello di comprendere se le norme di diritto internazionale già esistenti possano essere applicate allo specifico settore del cyberspazio e, in caso di riposta affermativa, in che modo eventualmente queste vadano declinate.

La nostra analisi deve muovere dunque da uno dei principi fondamentali del diritto internazionale, ovvero il principio di sovranità. Com'è noto, quest'ultimo, unitamente al corollario dal quale discende il rispetto dell'eguaglianza reciproca tra gli Stati, ebbe origine in occasione della pace di Westphalia nel 1648. Il modello westfaliano era basato sul principio della delimitazione territoriale e sulla non ingerenza negli affari interni di un altro Stato[138].

[138] Per una ricostruzione dettagliata si veda BESSON, *Sovereignty*, in *Max Planck Encyclopedia of Public International Law*, 2011.

Il principio di eguaglianza tra gli Stati è stato inoltre ripreso dalla Carta delle Nazioni Unite, la quale all'art. 2(1) stabilisce che l'Organizzazione è fondata sul principio della sovrana eguaglianza di tutti i suoi Membri[139].

Tuttavia, il principio di sovranità è stato dal trattato di Westphalia ad oggi oggetto di una constante evoluzione. Le tappe più importanti di questo percorso, e limitatamente a partire dal ventesimo secolo, possono essere così brevemente riassunte.

L'inizio del ventesimo secolo è di norma considerato il periodo durante il quale è nato il concetto moderno del principio di sovranità. È sempre da quel momento, inoltre, che si suole indicare l'inizio del diritto internazionale della cooperazione, in luogo di un diritto internazionale della coesistenza[140], nonché la nascita del concetto di sovranità esterna. Ciò emerge abbastanza chiaramente se si prendono in considerazione le prime decisioni delle Corte Permanente di Giustizia Internazionale, in particolare con le sentenze *Wimbledon*[141] e *Lotus*. Con quest'ultima decisione, infatti, la Corte ha precisato che «[i]nternational law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of

[139] Carta delle Nazioni Unite, San Francisco 1945, articolo 2 paragrafo 1.

[140] BESSON, *op.cit.*, p. 7.

[141] Corte permanente di giustizia internazionale, *caso Wimbledon* (Francia, Giappone, Gran Bretagna e Italia c. Germania), 17 agosto 1923, p. 25. Nel caso di specie, la Corte ha precisato che «The Court declines to see in the conclusion of any Treaty by which a State undertakes to perform or refrain from performing a particular act an abandonment of its sovereignty. No doubt any convention creating an obligation of this kind places a restriction upon the exercise of the sovereign rights of the State, in the sense that it requires them to be exercised in a certain way. But the right of entering into international engagements is an attribute of State sovereignty».

common aims. Restrictions upon the independence of States cannot therefore be presumed»[142].

Questa iniziale concezione di sovranità esterna deve tuttavia essere corroborata da un'altrettanta definizione di sovranità interna. Con questo termine si suole indicare l'autorità suprema che uno Stato esercita sul proprio territorio oppure il massimo potere che lo Stato esercita all'interno di quel dato territorio[143].

Nonostante le due diverse concezioni siano tra loro collegate, bisogna certamente tenere a mente che quando si parla dell'una e dell'altra non si vuole far riferimento alla differenza tra sovranità interna e internazionale. A ben vedere infatti la sovranità interna (o anche detta *domestic sovereignty*) fa riferimento sia alla sovranità interna che esterna dato che attraverso l'impianto normativo interno vengono disciplinati sia i rapporti dello Stato con altri Stati sia gli affari interni dello stesso[144]. Con sovranità internazionale interna invece si indicano l'insieme di diritti ed obblighi che lo Stato ha nei confronti delle persone e delle cose situate all'interno del proprio territorio. Basti pensare in tal senso al correlato principio di territorialità, alla giurisdizione, e al principio del non intervento (*infra*).

Per quanto concerne invece la sovranità internazionale esterna, essa si riferisce ai diritti ed obblighi che riguardano lo Stato in relazione ai rapporti con gli altri Stati della comunità internazionale. E in questo caso i principi che ne discendono sono diversi da quelli poc'anzi individuati, essendo rilevanti regole come l'immunità degli Stati dalla giurisdizione civile di un altro Stato oppure l'immunità degli agenti stranieri[145].

---

[142] Corte permanente di giustizia internazionale, *caso Lotus* (Francia c. Turchia), 7 settembre 1927, p. 18.

[143] *Customs Regime between Germany and Austria [Advisory Opinion] [Individual Opinion of Judge Anzilotti]*, p.57.

[144] BESSON, *op.cit.*, p. 13.

[145] *Ibidem.*

Ciò detto, quello che a noi in questa sede interessa riguarda quello specifico corollario del principio di sovranità che si sostanzia nel principio della sovranità territoriale. Nella famosa decisione nel caso Island of Palmas il giudice Huber definì la sovranità come «[i]ndependence in regard to a portion of the glob as the right to exercise therein, to the exclusion of any other State, the functions of a State»[146] . Anche la Draft Declaration on Rights and Duties of States, emanata dalla Commissione del diritto internazionale, fornisce una indicazione simile. L'art. 1, infatti, prevede che «every State has the right to independence and hence to exercise freely, without dictation by any other State, all its legal power, including the choice of its own form of government»[147]. La sovranità territoriale indica pertanto un diritto esclusivo di ogni Stato di esercitare il potere all'interno del proprio territorio nonché un obbligo di protezione da eventuali interventi esterni. In tal senso inoltre si esprime la Dichiarazione relativa ai principi di diritto internazionale, concernenti le relazioni amichevoli e la cooperazione fra gli Stati, la quale afferma più precipuamente che nessuno Stato (o gruppi di Stati) ha il diritto di intervenire, direttamente o indirettamente nelle questioni interne o esterne di un altro Stato. Di conseguenza, non solo l'intervento armato, ma anche ogni altra forma di ingerenza o di minaccia, diretta contro la personalità di uno Stato o contro le sue strutture pubbliche, economiche e culturali, sono contrarie al diritto internazionale[148].

Bisogna chiedersi dunque se il principio in esame possa estendersi i) alle infrastrutture fisiche che compongono il cyberspazio; e ii) al

[146] Reports of International Arbitral Awards, *Island of Palmas Case* (Netherlands v. USA), (1928), Volume II, p. 38.

[147] Si veda Commissione del diritto internazionale, Draft Declaration on Rights and Duties of States, UN. Doc. 375 (IV) del 6 dicembre 1949.

[148] Assemblea Generale, Res 2625 A/8082 (24 ottobre 1970), p. 121.

cyberspazio nel suo complesso. E se quindi possa parlarsi di una sovranità esclusiva degli Stati su di esso[149].

È innegabile che negli ultimi anni si sia manifestata da parte degli Stati *uti singoli* una crescente necessità di esercitare, attraverso la propria sovranità territoriale sulle infrastrutture informatiche[150], un maggiore controllo delle attività compiute con l'uso di internet. A tal proposito si è rievocata una concezione di sovranità (cyber)westfaliana. In particolare, secondo questa tendenza, è in corso una affermazione dei confini virtuali[151], sovrapponibili a quelli statali, all'interno dei quali gli Stati, in nome di una sicurezza nazionale, (de)limitano le attività che possono essere svolte per mezzo e attraverso gli strumenti informatici, aumentando il controllo su di essi.

---

[149] PIRKER, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in ZIOLKOWSKI (a cura di) *Peacetime Regime for State Activities in Cyberspace*, Tallinn, 2013, p. 191.

[150] Questa esigenza è cresciuta soprattutto successivamente alle rivelazioni avvenute nel 2013 da parte dell'agente della CIA Edward Snowden, il quale svelò l'esistenza di diversi programmi, utilizzati dai governi statunitense e britannico, in grado di sorvegliare i cittadini di tutto il mondo, andando a minare fortemente il diritto alla privacy. Di questi aspetti si parlerà più diffusamente nel terzo capitolo di questo lavoro. Per adesso sia consentito rimandare, seppur solo brevemente, all'analisi svolta da MILANOVIC, *Human Rights and Foreing Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal*, 2015, p. 81 ss.

[151] DEMACHAK, DOMBROWSKI, *Rise of a Cybered Westphalian Age*, in *Strategic Studies Quarterly*, 2011, p. 45. Più precisamente, secondo gli autori « A new "cybered Westphalian age" is slowly emerging as state leaders organize to protect their citizens and economies individually and unwittingly initiate the path to borders in cyberspace. Not only are the major powers of China and the United States already demonstrating key elements of emerging cybered territorial sovereignty, other nations are quickly beginning to show similar trends. From India to Sweden, nations are demanding control over what happens electronically in their territory, even if it is to or from the computers of their citizens. This process may be meandering, but we argue it was inevitable, given the international system of states and consistent with the history of state formation and consolidation. As cyberspace is profoundly man-made, no impossible barriers hinder the growth of national borders in cyberspace. They are possible technologically, comfortable psychologically, and manageable systemically and politically. Small steps in securing against threats will lead to further steps over time and, especially, in response to discoveries such as Stuxnet or its derivatives in the future».

I modelli statali che depongono in tal senso sono diversi. Anzitutto quello relativo alla Repubblica popolare cinese la quale, al fine di garantire la sicurezza dei propri cittadini da frodi informatiche, false informazioni e attacchi informatici, utilizza un sistema di controllo e di limitazione delle connessioni sia in entrata che in uscita. L'intenzione del Governo cinese sarebbe quella di costruire una propria rete internet al fine di tracciare sia l'origine delle informazioni che la loro destinazione[152], creando così un cd. *Great Firewall*[153]. Oltre la Cina, anche la prassi di altri Stati – per lo più mediorientali[154]– sembra convergere verso un penetrante controllo sulle infrastrutture informatiche situate sui propri territori e tendente ad una rievocazione del modello westfaliano[155]. L'Iran, ad esempio, al pari della Cina, cerca di creare una propria versione di internet, attraverso un serrato controllo delle informazioni, ammettendo e rendendo accessibili solo quelle ritenute conformi alla legge islamica[156].

In questo modo quindi, mediante la creazione di un cyberspazio con dei confini territoriali (e virtuali) ben definiti, si determinerebbe per analogia una applicazione della sovranità statale così come viene esercitata all'interno del proprio territorio. Tale modello, secondo i sostenitori di questa tesi, sarebbe da preferire rispetto ad un modello fondato sulla cooperazione tra Stati, a causa dell'eccessiva dispendiosità temporale e

[152] DEMACHAK, DOMBROWSKI, *op.cit.*, p. 46.

[153] SHACKERLFORD, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge, 2014, p. 71. Più precipuamente, secondo l'Autore, la Cina sarebbe considerabile come il Paese con il tasso di censura più elevato al mondo, avendo elaborato un insieme di politiche e di strutture burocratiche al fine di regolamentare la libertà di espressione online. Per fare una stima numerica, vi sarebbero circa 30.000 persone dislocate tra 12 agenzie governative per compiere il lavoro di regolazione e censura così come implementato dal governo cinese.

[154] In tal senso si veda il Report *Enemies of the internet* del 2014.

[155] DEMACHAK, DOMBROWSKI, *op.cit.*, p. 46.

[156] Cfr. GOURLEY, *Cyber Sovereignty*, in YANNAKOGEORGOS, LOWTHER (a cura di) *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, Londra-New York, 2013, p. 277.

della difficile applicazione di alcune norme di diritto internazionale (come quelle relative alla responsabilità degli Stati) che il modello cooperativo richiederebbe[157].

Siffatta tendenza tuttavia non può in alcun modo essere condivisa. Sebbene infatti molti Stati abbiano adottato una normativa interna per affrontare e prevenire alcune fattispecie criminose localizzabili nel proprio territorio – ad esempio in materia di pirateria – o misure più incisive come il controllo delle infrastrutture fisiche situate sul proprio territorio, al fine di facilitare l'individuazione del flusso di informazioni ed eventualmente limitarle, riconoscere validità a tale approccio significherebbe violare la natura globale del cyberspazio[158], nonché procedere verso una cd. balcanizzazione delle Rete[159].

In altre parole, così procedendo, si verrebbero a creare tante reti internet per quanti sono gli Stati nazionali, come una sorta di intranet nazionale. Il che determinerebbe in ultima analisi una frammentazione e un irrimediabile «detrimento al valore di internet come tutto maggiore della somma delle singole parti»[160]. Ciò detto, sebbene il rischio di una frammentazione sia un'ipotesi molto realistica, ancorché in una fase iniziale, la sua concreta attuazione implicherebbe una serie di problemi di natura sia tecnica che politica[161].

---

[157] GOURLEY, *op.cit.*, p. 57.

[158] ZIOLKOWSKI, *General Princples of International Law applicable in Cyberspace*, in ID, *Peacetime Regime for State Activities in Cyberspace*, 2013, Tallin, p. 162.

[159] CORNISH, *Governing Cyberspace through Constructive Ambiguity*, in *Survival*, 2015, p. 157.

[160] ODDENINO, *Diritto individuali, sicurezza informatica e accesso alla conoscenza in rete: la revisione delle International Telecommunication Regulations dell'ITU*, in *Diritti umani e diritto internazionale*, 2013, p. 538.

[161] LIAROPULOS, *Exploring the Complexity of Cyberspace Governance: State sovereignty, Multi-stekeholderism, and Power Politics*, in *Journal of Information Warfare*, 2016, p. 16. Più precisamente, secondo l'Autore le diverse tipologie di problematiche potrebbero così essere definite. «(…) In strictly technical terms, it is doubtful that cyberspace will fragment as a globalnetwork. Current institutions that are responsible for the interoperability of cyberspace

Nonostante quindi non possa escludersi che le infrastrutture fisiche situate su di un determinato territorio – anche se parte del più ampio insieme composto appunto dal cyberspazio – siano sottoposte alla sovranità e alla giurisdizione di quel determinato Stato, allo stesso tempo però non può ritenersi l'intero cyberspazio sottoposto alle comuni regole che disciplinano la sovranità statale. In ragione della natura globale[162], invisibile, non identificabile e intangibile[163] ad esso riconosciuta, uno Stato, piuttosto che un altro, non può appropriarsene unilateralmente[164]. Inoltre, a ben vedere, la sovranità esercitata dal singolo Stato involgerebbe esclusivamente il primo livello del cyberspazio (le infrastrutture) e non

willcontinue to ensure the resilience of the global infrastructure. Technology evolves faster than law,but states have already resorted to their Westphalian toolkit, and the ideas of data sovereignty,national clouds, and local data storages are gaining ground. Last but not least, the politicalconsequences of managing diverse national cyberspaces must be considered, as opposed togoverning shared cross-border online spaces in a synergistic manner».

[162] Secondo il Dipartimento della Difesa statunitense «the global commons consist of international waters and airspace, space, and cyberspace». Cfr. Department of Defense United States of America, *Strategy for Homeland Defense and Civil Support*, 2005, p. 12

[163] Tali caratteristiche sono state utilizzate in dottrina per descrivere il cyberspazio. Si veda, in particolare, Rosenne il quale sostiene «[u]nlike other spaces, cyberspace is invisible, unidentifiable, irrefrangible, intangible, and cannot be felt or identified in any way: it has no known natural characteristics. It is simply there, and used by electromagnetic impulses made by human beings. The law can control the use that human beings put to it». Cfr. ROSENNE, *The perplexities of Modern International Law*, in *Recueil des Cours de l'Académie de Droit International*, 2004, p. 330.

[164] Nello stesso senso si veda, ZIOLKOWSKI, *op.cit.*, p. 162; VON HEINEGG,, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013, p. 126. Secondo quest'ultimo «[t]he integration of physical components of cyber infrastructure located within a State's territory into the "global domain" of cyberspace cannot be interpreted as a waiver of the exercise of territorial sovereignty. While, in view of the genuine architecture of cyberspace, it may be difficult to exercise sovereignty, the technological and technical problems involved do not prevent a State from exercising its jurisdiction over the cyber infrastructure located in areas in its sovereign territory. States have, in fact, continuously emphasized their right to exercise control over such infrastructure, to assert their jurisdiction over cyber activities on their territory and to protect their cyber infrastructure against transborder interference by other States or by individual».

anche gli altri due, in particolare quell'insieme di dati e informazioni che viaggiano attraverso il livello precedente[165].

Così delimitata la portata del principio di sovranità, bisogna chiedersi ed indagare se non vi sia un regime internazionale capace di inquadrare il cyberspazio in una cornice normativa internazionale che garantisca maggiormente la tutela di questo spazio e non comprometta le caratteristiche interinseche spazio comune ed accessibile a tutti. Un esempio in tal senso potrebbe essere dato dal regime del patrimonio comune dell'umanità.

2. La nozione di patrimonio comune dell'umanità

La nozione di patrimonio comune dell'umanità, rintracciabile già dal XVII secolo nel diritto internazionale classico, configura un particolare regime giuridico internazionale degli spazi comuni, e si caratterizza per la presenza di diversi elementi: *a)* il divieto di una appropriazione esclusiva da parte degli Stati; *b)* l'obbligo di utilizzare i beni esclusivamente per scopi pacifici; *c*) l'obbligo di una cooperazione degli Stati al fine di preservarne la natura per le future generazioni; *d)* l'individuazione o la creazione di un organismo internazionale che gestisca il patrimonio comune per conto dell'intera comunità internazionale[166].

Tale regime giuridico si configura come un *tertium genus* rispetto alle ipotesi di una esclusiva sovranità degli Stati e quello relativo alla mancanza di qualsiasi regola giuridica. I suoi principi ispiratori – secondo alcuni –

[165] SHACKELFORD, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law* in *Berkley Journal of International Law*, 2009, p. 213.

[166] WOLFRUM, *The Principle of the Common Heritage of Mankind,* in Max Planck Encyclopedia of Public International Law, 1983, p. 312; NOYES, *The Common Heritage of Mankind: Past, present, and Future, in Denver*, in *Journal of International Law and Policy*, 2012, 456; RUOTOLO, *Internet-ional Law,* cit., p. 85; S. MARCHISIO, *Corso di Diritto Internazionale*, Torino, 2017, p. 220;

hanno segnato il passaggio dal diritto internazionale della coesistenza a quello della cooperazione[167].

La sua moderna accezione, tuttavia, è stata rievocata nel 1967 in occasione della Terza Conferenza per la codificazione del diritto del Mare dall'ambasciatore maltese Arvid Pardo[168], rappresentante maltese presso le Nazioni Unite[169]. La proposta per la prima volta inquadrava la nozione di patrimonio comune dell'umanità in relazione al regime giuridico dei suoli e sottosuoli marini, situati oltre i limiti delle giurisdizioni nazionali, ritenendoli spazi non sottoponibili all'appropriazione da parte degli Stati, utilizzabili per scopi pacifici e promuovendo una gestione che permetta l'utilizzo da parte dell'intera umanità[170].

Il primo riscontro concreto della proposta maltese si ebbe dapprima con la dichiarazione adottata dall'Assemblea Generale delle Nazioni Unite sui principi relativi ai fondali marini con la quale, oltre a definire tali spazi come patrimonio comune dell'umanità, si prevedeva la realizzazione di un meccanismo internazionale che assicurasse una gestione razionale del

[167] S. MARCHISIO, *op.cit.,* 220.

[168] La citata modernizzazione del concetto di Patrimonio Comune dell'Umanità secondo alcuni non è da riconoscere all'ambasciatore Pardo. Come si legge infatti nel documento, presentato dall'Ambasciatore Aldo Cocca, titolato *Legal Sub-Committee of the Committee on the Peaceful Uses of Outer* Spaces: «First, the international community from now on possessed a written law of outer space which, for reasons of time and procedure, was not yet positive law valid for all legal systems, but was nontheless valid for every inhabitant of the globe considered independently of Such systems. Secondly, the international community had recognized the existence of a new subject of international law, namely, mankind itself, and creates a jus humanitatis. Thirdly, the international community had, in the persons of the astronauts appointed envoys of mankind in outer space. Fourthly, the international community had endowed that new subject of international law - mankind - with the vastest common property (res communis humanitatis) which the human mind could at present conceive of, namely outer space itself, including the Moon and the other celestial bodies». Cfr. R. WOLFRUM, *op.cit.*, p. 1 nota 1; COCCA, *The Advances in International Law through the Law of Outer Space*, in *Journal of Space Law,* 1981, p. 15; UN Doc. A/AC.105/C.2/SR.75 (19 giugno 1967) 7-8.

[169] WOLFRUM, *op.cit.*, p. 312

[170] NOYES, *op.cit.*, p. 456; G. M. RUOTOLO, *Internet-ional Law,* cit., p. 85; S. MARCHISIO, *op.cit.*, p. 189

patrimonio[171]; e successivamente nella Parte XI della Convenzione delle Nazioni Unite sul diritto del mare[172].

Il concetto in esame è stato poi utilizzato in relazione ad ulteriori contesti molto eterogenei tra loro: nell'Accordo sulle attività degli Stati sulla luna e gli altri corpi celesti (1979)[173]; la dichiarazione universale sul genoma umano e di diritti dell'uomo adottata dalla Conferenza generale dell'Unesco nel 1997. Secondo detta dichiarazione, il genoma umano, che rappresenta la specie umana, può essere inteso in senso simbolico patrimonio dell'umanità[174] e non può essere oggetto di appropriazione da parte degli Stati o individui.

Ebbene, se da un lato dette dichiarazioni, che richiamano direttamente o indirettamente la nozione di patrimonio comune dell'umanità, ci permettono di tracciare alcune sue caratteristiche aggiuntive, dall'altro lato è necessario sottolineare le differenze che intercorrono tra la nozione applicata ai casi poc'anzi menzionati e quella (eventualmente) applicabile al cyberspazio.

Quanto al primo punto, la più importante ci sembra essere la sua versatilità e flessibilità, nonché un suo progressivo utilizzo – in concomitanza con lo sviluppo tecnologico – tanto da ricomprendere in ultima analisi il genoma umano, oggetto sicuramente distante dal campo d'azione originariamente individuato. Ne discende pertanto la possibile applicabilità anche al di fuori delle ipotesi previste dalle convezioni suindicate. Va inoltre osservato che, sebbene non manchino opinioni in senso contrario in dottrina[175], al principio

---

[171] RUOTOLO, *Internet-ional Law*, cit., p. 85; S. MARCHISIO, *op.cit.*, p. 189.

[172] RUOTOLO, *Internet-ional Law*, cit., p. 85; S. MARCHISIO, *op.cit.*, p. 189.

[173] L'articolo 11 dell'Accordo stabilisce espressamente che «[t]he moon and its natural resources are the common heritage of mankind, which finds its expression in the provisions of this Agreement, in particular in paragraph 5 of this article. (…) The moon is not subject to national appropriation by any claim of sovereignty, by means of use or occupation, or by any other means».

[174] L'articolo 1 della Dichiarazione indica che «[t]he human genome underlies the fundamental unity of all members of the human family, as well as the recognition of their inherent dignity and diversity. In a symbolic sense, it is the heritage of humanity».

[175] Si veda, ad esempio, JOYNER, *Legal Implications of the Concept of the Common Heritage of Mankind*, in *International and Comparative Law Quarterly*, 1986, p. 190.

in esame sia oramai possibile riconoscere natura consuetudinaria[176]. Si tratta di una conclusione che può trarsi anzitutto da una prassi convenzionale che, nonostante sia quantitativamente ridotta, risulta essere particolarmente significativa sia in ragione della natura di accordo di codificazione del trattato in questione sia, in ogni caso, dall'ampia condivisione che i principi in esso contenuti ha suscitato nell'ambito della comunità internazionale nel suo complesso. Il riferimento va soprattutto alla Convenzione delle Nazioni Unite sul diritto del mare (unitamente all'accordo relativo all'attuazione della parte XI della Convenzione)[177] e al Trattato sulle attività degli Stati sulla luna e sugli altri corpi celesti. A ciò si aggiungono una serie di atti di *soft law* che pur non avendo carattere vincolante si segnalano per lo sforzo da essi profuso nel senso della ricostruzione del diritto internazionale generale, e che proprio in materia di patrimonio comune dell'umanità hanno riconosciuto l'esistenza di una norma consuetudinaria. Sotto questo profilo, le dichiarazioni dell'*International Law Association* adottate a Seoul e a Nuova Deli ne offrono un esempio significativo[178].

Per quanto concerne invece le differenti applicazioni della nozione di 'patrimonio comune dell'umanità', va evidenziato che mentre con riguardo al mare, ai corpi celesti – come la luna – e allo stesso genoma umano possa parlarsi di una perdita della sovranità statale, le caratteristiche del cyberspazio (commistione di territorialità e a-territorialità) determinano piuttosto una limitazione del potere di sovranità dello Stato in ragione

[176] Cfr. WOLFRUM, *op. cit.*, p. 333-337; ID, *The Common Heritage of Mankind*, in *Max Plack Encyclopedia of Public International Law*, 2009.

[177] Gli Stati Uniti, che non hanno ratificato la Convenzione, possono essere qualificati come obiettori persistenti alla norma consuetudinaria esistente. In tal senso si v. NOYES, *op.cit.*, p. 455 e 468; CASSESE, *op.cit.*, pp. 111-117.

[178] International Law Associations (ILA), *Declaration on the Progressive Development of Principles of Public International Law Relating to a New International Economic Order*, in *International Law Associations report of sixth-second conference*, 1987, paragrafo 7.1; International Law Associations, *New Delhi Declaration of Principles of International Law Relating to Sustainable Development*, in *International Law Report of seventieth conference*, 2002, p. 24.

dell'interesse collettivo alla protezione del bene perseguito dall'intera comunità internazionale.

2.1 La nozione di Patrimonio comune dell'umanità in relazione al cyberspazio

Alcuni degli elementi della nozione di patrimonio comune dell'umanità precedentemente individuati ci sembrano applicabili al contesto virtuale del cyberspazio. Ci riferiamo in particolare al divieto di appropriazione unilaterale, all'obbligo di utilizzo pacifico e all'obbligo di cooperazione tra gli Stati, elementi applicabili al fine di garantire un accesso alla rete libero e aperto a tutti.

Una parte della Comunità internazionale infatti sembra ritenere necessario – al fine di preservare la natura globale di Internet – un sistema coordinato per una *International Internet governance*[179]. Questa volontà si evince chiaramente dalla Dichiarazione di Principi, emanata all'esito del *World Summit on the Information Society* (WSIS)[180], secondo cui «the international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations»[181]. L'idea manifestata in quell'occasione sembra essere orientata verso un approccio aperto e democratico che sia capace di promuovere una cooperazione tra gli Stati e favorire il coinvolgimento di diversi soggetti, come appunto i privati e le organizzazioni non governative.

---

[179] SEGURA SERRANO, *Internet Regulation and the Role of International Law*, in *Max Planck Yearbook of United Nations Law*, 2006, p. 255.

[180] In modo più approfondito il tema è stato trattato nei paragrafi precedenti, pertanto per un'analisi sul tema si vedano i parr. 2.1 e 2.2.

[181] World Summit on the Information Society, *Declaration of principles, Building the Information Society: a Global Challenge in the New Millenium*, (Ginevra 2003) paragrafo 48.

Al di là di quanto stabilito nel corso del WSIS, anche la prassi di alcuni Stati depone in tal senso. Gli Stati Uniti, ad esempio, nonostante il preminente ruolo nella gestione dei *Root Server*[182], hanno confermato il loro impegno nel non intraprendere alcuna azione che possa compromettere il funzionamento, la sicurezza e l'efficienza di Internet, promuovendone uno sviluppo multilaterale e diffuso che abbia luogo in differenti *fora*[183].

Più di recente poi una espressa richiesta di considerare il cyberspazio come patrimonio comune dell'umanità è stata avanzata dall'Ambasciatore maltese in occasione della *World Summit on Information Society Review* Process[184].

In quella circostanza, lo Stato maltese ha ribadito come attraverso l'utilizzo di norme di diritto internazionale è possibile proseguire lo sviluppo e la crescita di Internet come strumento comune per l'intera umanità[185],

---

[182] Il modo attraverso cui Internet funziona dipende in buona sostanza dai *root* server (server radice). In totale ce ne sono tredici e la loro funzione è essenzialmente quella di fungere da *database* per tutti i nomi a dominio. In altre parole, ogni qualvolta ci sia una domanda di accesso ad un determinato punto della Rete, i root server reindirizzano la richiesta verso i server specifici e quest'ultimi a loro volta forniscono le informazioni. È chiaro quindi che la gestione dei root server determina in ultima analisi la gestione di Internet inteso come 'rete di reti'. Ebbene, gli Stati Uniti, in particolare la *National Telecommunications and Information Administration* (NTIA), per il tramite di ICANN e IANA detiene il potere esclusivo di autorizzare qualsiasi modifica al contenuto del *database*. Tale esercizio di potere esclusivo viene esercitato dal governo statunitense anche per qui *root server* che sono situati sui territori di altri Stati. La giustificazione per l'applicazione extraterritoriale del potere di governo statunitense, in assenza di norme di diritto internazionale che gli riconoscano tale facoltà, sembrerebbe risiedere in una sorta di *acquiescenza* degli Stati su cui i *root server* sono dislocati. Cfr. RUOTOLO, *Internet-ional Law, cit.*, pp. 51-60.

[183] Il governo statunitense infatti con l'adozione di un documento rubricato *US Principles on the Internet's Domain Name and Addressing System* ha espresso infatti la volontà «to preserve the security and stability of the Internet's Domain Name and Addressing System (DNS). Given the Internet's importance to the world's economy, it is essential that the underlying DNS of the Internet remain stable and secure. As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file». Il documento è reperibile *online.*

[184] Dopo poco più di dieci anni dal primo Summit mondiale sulla società dell'informazione si è svolto nel dicembre 2015 a New York il processo di revisione delle dichiarazioni adottate a Ginevra e a Tunisi. L'incontro è culminato con l'adozione di una risoluzione (A/70/L.33) dell'Assemblea Generale avente ad oggetto tematiche di particolare spessore per il futuro sviluppo della società dell'informazione, tra queste vanno ricordate la cybersicurezza, la *governance* di Internet e il rapporto con i diritti umani.

[185] World Summit on Information Society Review Process, Statement by Dr. Alex Sceberras Trigona Special Envoy of the Prime Minister of the Republic of Malta Permanent Mission of the Republic of Malta to the United Nations, 15 dicembre 2015.

chiedendo al Segretario Generale delle Nazioni Unite di introdurre lo specifico argomento nell'Agenda dell'Assemblea Generale intitolato "*protection of the Internet as part of the Common Heritage of Mankind*"[186].

L'applicazione della nozione del patrimonio comune quindi inciderebbe sul principio di sovranità determinando in capo agli Stati, sul cui territorio sono situate le infrastrutture, un ruolo di mero gestore di esse al fine di perseguire un più ampio interesse, comune alla maggior parte degli Stati, che è appunto quello di una Rete libera ed aperta a tutti.

Ciò detto, bisogna rilevare che uno dei punti più critici per l'applicabilità della nozione di patrimonio comune dell'umanità è quello relativo alla creazione di un organismo internazionale capace di assicurare e garantire l'accesso all'intera comunità. In dottrina si è paventata l'idea di istituire in seno alle Nazioni Unite un ente nuovo ed indipendente, in cui gli individui che ve ne fanno parte non siano espressione degli interessi dello Stato di appartenenza, al pari della Corte Internazionale di Giustizia o dell'Autorità Internazionale dei Fondali Marini[187]. Tuttavia, le caratteristiche dell'ente in questione e alcuni modelli di funzionamento, sebbene già individuate dal *Working Group on Internet* Governance (WGIG), non hanno mai trovato una concreta applicazione a causa delle divergenti opinioni espresse da Stati come Stati Uniti, Cina e Russia[188]. A tal proposito basti pensare alla contrapposizione creatasi in seno alla già richiamata *World Conference on International Telecommunications* (WCIT-12). In occasione della Conferenza, infatti, si sono creati due gruppi distinti di Stati. Da un lato, gli Stati occidentali (capeggiati dagli Stati Uniti), favorevoli al mantenimento di una Rete libera e aperta a tutti, gestita dall'ICANN e capace di auto-

[186] World Summit on Information Society Review Process, cit., 6.

[187] SPANG HANSSEN. *Who should Govern public international Computer networks,* in *Nordic Journal of International Law, 2008,* p. 21, 22.

[188] Si pensi ad esempio al dibattito in occasione della *World Conference on International Telecommunications* tenutasi nel 2012 a Dubai sotto l'egida dell'*International Telecommunications Union* (ITU). In merito si veda, tra gli altri, ODDENINO, *op.cit.*, p. 532.

svilupparsi come risorsa globale; dall'altro, invece, gli Stati orientali (Cina e Russia in particolar modo) i quali propendevano per un maggior controllo sulla rete, sia per motivi legati alla sicurezza nazionale ed internazionale (si pensi a fenomeni come il *cybercrime*, *cyberterrorsim*, *cyberwar*, etc.), sia perché contrari al rapporto tra ICANN e Stai Uniti[189].

A causa dell'esito piuttosto compromissorio avutosi in occasione della WCIT-12, il ruolo di coordinamento e funzionamento è ancora svolto dall'ICANN, ente che ha come funzione principale quella di garantire l'efficienza e il funzionamento dei DNS. Tuttavia, la funzione di supervisore svolta dal Dipartimento del Commercio statunitense – come abbiamo visto – è stata da sempre uno dei punti più controversi al riconoscimento di un ruolo neutrale ed indipendente dell'ente.

Ad oggi, però, la situazione potrebbe essere cambiata. Con il completamento del processo di transizione della gestione del sistema di *Internet Assigned Numbers Authority* dal dipartimento del commercio americano all'ICANN – senza la supervisione degli Stati Uniti – il suo ruolo potrebbe finalmente essere concepito in maniera diversa. A partire dal 2014, infatti, è stato annunciato l'inizio del procedimento di transizione,[190] il cui obiettivo era quello di riconoscere la natura globale ed indipendente dell'ICANN con una struttura partecipativa e aperta a tutti gli *stakeholder*. Il processo si è concluso a fine 2016 quando il contratto tra l'ICANN e il Dipartimento del commercio americano è ufficialmente scaduto[191]. Tuttavia, sebbene la complessa struttura organizzativa dell'ICANN non permetta in questa sede di svolgerne un'analisi approfondita, è necessario chiarire alcuni

[189] Le tensioni tra i due gruppi di Stati furono così forti che si parlò addirittura di una 'guerra fredda digitale'. Per una ricostruzione più approfondita della vicenda, si veda, tra gli altri, ODDENINO, *op.cit.*, p. 534.

[190] National Telecommunications and Information Administration (NTIA), United States Department of Commerce, *Ntia announces Intent to Tranition Key Internet Domain Name Functions*, 14 marzo 2014, reperibile *online.*

[191] La notizia è reperibile *online.*

aspetti riguardanti la sua natura giuridica e la sua composizione, aspetti che sono in un certo senso collegati. Ebbene, in relazione al primo punto, secondo un rapporto di studio emanato dal Congressional Research Service statunitense, l'ICANN si configurerebbe come una vera e propria organizzazione internazionale[192]: questa attribuzione scaturirebbe essenzialmente dalle caratteristiche intrinseche dell'oggetto da esso gestito, la Rete, che per sua natura si configura come internazionale (o transnazionale) prevaricando i confini nazionali. Siffatta conclusione – prima della rescissione del contratto – appariva sicuramente forzata. Il fondamento giuridico dell'ente riposa su un atto di diritto interno statunitense, piuttosto che su di un trattato internazionale, il che esclude l'ICANN dal novero delle organizzazioni internazionali, per lo meno se intese in senso stretto[193]. D'altra parte, è agevole rilevare come anche dopo la scadenza del contratto con il Dipartimento del Commercio, l'ICANN non sembra aver assunto tali caratteristiche. La sua composizione cd. *multisteakholders*, che vede rappresentati Stati, soggetti privati, organizzazioni non governative, fa propendere piuttosto per un ente rappresentativo della cd. "global community". Tale espressione, utilizzata nel comunicato che diede inizio al procedimento di transizione delle funzioni IANA[194], indica genericamente l'insieme degli enti che esercitano attività internazionalmente rilevanti, anche se non rientranti nel novero dei soggetti di diritto internazionale, come organizzazioni non governative, imprese multinazionali e da ultimo gli individui[195].

---

[192] RUOTOLO, *Il sistema dei nomi a dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, in *Il diritto dell'informazione e dell'informatica*, 2016, p. 51.

[193] Cfr. ID, *Il sistema dei nomi a dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, cit. p. 51; SCHWEIGHOFER, *Role and Perspectives of ICANN*, in W. BENEDEK, V. BAUER e M. C. KETTEMAN (eds), *Internet Governance and the Information Society: Global Perspective and European Dimensions*, Utrecht, 2008, p. 83ss.

[194] National Telecommunications and Information Administration (NTIA), *Office of Public Affairs*, 2014, 482ss, reperibile *online*.

[195] RUOTOLO, *Il sistema dei nomi a dominio alla luce di alcune recenti tendenze dell'ordinamento internazionale*, cit., p. 2.

Senonché anche la qualificazione dell'ICANN come ente internazionale indipendente, capace di assicurare l'accesso e la gestione di Internet, e suscettibile come tale di realizzare uno degli elementi sottesi alla nozione di patrimonio comune dell'umanità, resta dubbia. Se da un lato infatti la conclusione del processo di 'privatizzazione' può essere sintomatico della volontà di riconoscere il cyberspazio come spazio e risorsa comuni all'intera umanità, dall'altro i risvolti politici che risiedono nelle scelte relative alla sua gestione sono innegabili e spesso, come successo in passato, all'origine di posizioni contrastanti[196]. In altre parole – al di là del processo di transizione – una qualificazione del genere sarebbe accettabile solo in presenza di un modello organizzativo nuovo, orizzontale e democratico, in cui la componente statale e quella non statale interagiscono su un piano paritario[197].

L'altra questione che parimenti merita un'approfondita trattazione è quella relativa all'utilizzo pacifico del cyberspazio. Quest'elemento, che rappresenta una delle caratteristiche che qualificano il regime del patrimonio comune dell'umanità, è certamente applicabile al cyberspazio, ma allo stesso tempo mette in rilievo la possibilità che attraverso attacchi informatici possano essere compiuti degli illeciti internazionali.

Partendo da questo assunto dobbiamo anzitutto indagare quale sia la definizione di attacco informatico che maggiormente rispecchi la prassi e meglio si attagli al diritto internazionale.

---

[196] Per una recente ricostruzione dottrinale del processo di riforma dell'ICANN si veda M.R. CARRILLO, *La reforma de la corporacion para la asignacion de nombres y numeros de internet (ICANN): un analisis en terminos de legitimidad*, in *Revista Espanola de Derecho International*, 2018.

[197] Per un approccio simile si veda T. NATOLI, *op.cit.*, p. 29. L' Autore suggerisce una diversa prospettiva attraverso un parallelismo con alcuni modelli organizzativi già esistenti, come quelli relativi alle telecomunicazioni internazionali via satellite (si veda ad esempio l'INMARSAT, INTELESAT e l'EUTELSAT). Queste organizzazioni intergovernative hanno subito, a partire dal 1999, un processo di semi-privatizzazione (che nel caso della Rete andrebbe inteso in senso inverso, e cioè dal privato al pubblico) che ha dato vita ad una forma di gestione ibrida dei servizi forniti, nato dalla contemporanea presenza di un'organizzazione internazionale pubblica e più società private. Qualora tale sistema venisse applicato alla gestione della Rete potrebbe parlarsi di un modello capace di esprimere la volontà generale e le necessità dell'intera Comunità internazionale.

3. La definizione di attacco informatico rilevante per il diritto internazionale

Il problema relativo agli attacchi informatici nel contesto internazionale può essere affrontato da diversi punti di vista. Innanzitutto, si può analizzare la tematica nell'ottica dei crimini individuali, e in particolare sulla possibilità di qualificare il *cyberterrorismo* come crimine internazionale[198]. Ci si può porre poi sul piano dello *jus in bello* e

[198] Secondo la più recente dottrina, è ben possibile che condotte informatiche, volte a istigare o facilitare crimini internazionali, possano ricadere nell'ambito giurisdizionale della Corte Penale Internazionale (CPI), soddisfacendo almeno il requisito della gravità. Più in particolare, le condotte cibernetiche potrebbero, almeno potenzialmente, soddisfare lo standard di gravità così come elaborato dalla CPI e dal Procuratore. Tuttavia, la possibilità concreta che quest'ultimo decida di iniziare un'azione che coinvolga attività cibernetiche dipende pur sempre dalla sua discrezionalità e dalle situazioni soggettive che si palesano caso per caso. Di conseguenza, il Procuratore potrebbe decidere di perseguire un comportamento che involge situazioni informatiche oppure giungere a conclusioni differenti in base a considerazioni comparative che involgono, ad esempio, le prove prodotte oppure la possibilità di individuare e arrestare l'indagato. Si veda più diffusamente ROSCINI, *Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes*, in *Criminal Law Forum*, 2019, p. 247 ss. Da una prospettiva parzialmente diversa, secondo altra parte della dottrina, un attacco informatico potrebbe più verosimilmente integrare la nozione di crimine di guerra, generando così una responsabilità individuale del soggetto/individuo. Secondo questa impostazione, invece, un attacco informatico difficilmente potrà soddisfare i requisiti richiesti dall'art. 8 bis, par. 1 (secondo cui « [a]i fini del presente Statuto, «per crimine di aggressione» s'intende la pianificazione, la preparazione, l'inizio o l'esecuzione, da parte di una persona in grado di esercitare effettivamente il controllo o di dirigere l'azione politica o militare di uno Stato, di un atto di aggressione che per carattere, gravità e portata costituisce una manifesta violazione della Carta delle Nazioni Unite»). Infine, gli attacchi informatici, perpetrati durante dei conflitti armati già in atto, potrebbero altresì integrare dei 'crimini contro l'umanità', solo però a condizione che sia soddisfatto l'art. 7, par. 2(a) dello Statuto, secondo cui «[s]i intende per 'attacco diretto contro popolazioni civili' condotte che implicano la reiterata commissione di taluno degli atti preveduti al paragrafo 1 contro popolazioni civili, in attuazione o in esecuzione del disegno politico di uno Stato o di una organizzazione, diretto a realizzare l'attacco questi vengano posti in essere per dare attuazione ad un disegno politico dello Stato oppure da un soggetto appartenente alla struttura organizzativa dello Stato o di una organizzazione». Cfr. AMBOS, *International Criminal Responsibility in Cyberspace*, in TSAGOURIAS, BUNCHAN (a cura di) *Research Handbook on International Law and Cyberspace*, Cheltenham e Northampton, 2015, p. 118 ss.

affrontare dunque i problemi sollevati dall'uso delle tecnologie informatiche durante i conflitti già in corso[199]. E infine si può stabilire se e quando un attacco informatico ricade nell'ambito di applicazione delle regole in tema di *jus ad bellum*. Il presente capitolo si propone di analizzare solo quest'ultimo ambito di indagine e, a tal fine, la prima questione da affrontare è quella relativa all'individuazione degli attacchi informatici rilevanti per il diritto internazionale. In altre parole, bisogna capire se e quando un attacco informatico possa essere considerato contrario ad un obbligo internazionale e di conseguenza configurare un illecito internazionale.

Al fine di inquadrare in modo compiuto la tematica che si qui si sta analizzando, appare necessario individuare anzitutto la definizione di

[199] Al fine di descrivere solo brevemente il problema è utile prendere come caso di studio il conflitto armato in Ucraina e analizzare attraverso il prisma del diritto internazionale umanitario l'uso di software informatici durante un conflitto già in corso. Secondo quanto riportato nel 2016 da una società di sicurezza informatica statunitense, CrowdStrike Intelligence, un gruppo di hacker russi sarebbe riuscito ad installare un *malware* all'interno di una applicazione destinata a dispositivi mobile usati dalle forze di artiglieria ucraine impegnate nel conflitto dell'Ucraina orientale, iniziato nell'aprile del 2014. L'applicazione originaria permette di accelerare l'elaborazione dei dati utili per l'individuazione di un obiettivo da colpire con uno specifico pezzo di artiglieria, vale a dire l'obice D-30. Riducendo notevolmente il processo di elaborazione, da qualche minuto a circa 15 secondi, le forze ucraine sono state capaci di aumentare l'intensità di fuoco contro le forze separatiste filo-russe. Senonché, le forze militari russe, intervenute a supporto delle forze separatiste filo-russe, sono riuscite ad intercettare le comunicazioni telefoniche e ad accedere ai dati di localizzazione dei pezzi di artiglieria governative ucraine e quindi a colpirle anticipatamente. Grazie a tale software, le forze russe sono riuscite ad individuare e distruggere la maggior parte degli obici impiegati dalle forze governative ucraine. A ciò si aggiunge che il conflitto armato in Ucraina è stato anticipato da azioni informatiche, quali il blocco dei siti governativi ucraini e della telefonia mobile del Paese, da parte di gruppi hackers che hanno svolto un ruolo di apripista alle forze russe in prospettiva di una loro avanzata in territorio ucraino. Ebbene, secondo una parte della dottrina l'utilizzo di un programma malevolo potrebbe costituire quindi un attacco informatico configurabile come parte integrante di un attacco armato tradizionale qualora sussista un nesso diretto di causalità tra il risultato ottenuto dal suo impiego e il ricorso alla forza cinetica. E cioè, in altre parole, l'attacco sarebbe costituito da due fase temporalmente distinte, ma strettamente e imprescindibilmente connesse tra loro. Sul punto per una ricostruzione più puntuale e dettagliata si veda FORNARI, *Conflitto in Ucraina, orsi fantasiosi e programmi malevoli*, in *Rivista di diritto internazionale*, 2017, p. 1156 ss.

attacco informatico che si intende utilizzare. A tale scopo, occorre vagliare le diverse ipotesi avanzata sia in dottrina che nei differenti *fora* di discussione, nonché quelle prospettate dagli Stati.

In linea generale, il termine 'attacco informatico' (*cyber attack*) si inserisce nel più ampio contesto delle cd. *Computer Network Operations* (d'ora in poi CNO).

Diverse sono le fonti che cercano di fornire, in maniera più o meno completa, una nozione di attacco informatico. Una prima definizione è quella ascrivibile ad un'agenzia specializzata in seno alla NATO, la *Nato Cooperative Cyber Defence Centre of Excellence* (d'ora in poi CCDCOE) che nel 2013 ha pubblicato il cd. Manuale di Tallinn. Quest'ultimo definisce un *cyber attack* come un'operazione informatica, sia offensiva sia difensiva, che può ragionevolmente causare lesione o morte di persone ovvero danni o distruzione di oggetti[200].

Più nello specifico, secondo tale definizione due sono gli elementi che consentono ad una azione di essere qualificata come attacco informatico: da un lato, la presenza di un «*act of violence*'[201]»; dall'altro lato, la produzione diretta o indiretta di conseguenze distruttive. Dal primo elemento si evince che non tutte le operazioni informatiche devono essere qualificate come attacchi informatici, restando escluse – ad esempio – quelle ipotesi di mera *intelligence* che si concretizzano nel cd. *cyber espionage*[202]. Dal secondo elemento, invece, deriva la circostanza che ad essere rilevanti non sono solo quegli attacchi che hanno come diretta

[200] Manuale di Tallin, rule 30, secondo cui: «*a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to person or damage or destruction to objects*».

[201] *Ibidem*, rule 30, par. 3.

[202] Quando ci riferiamo al cd. *cyber espionage* intendiamo: «*the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence*». Cfr. HATHAWAY, CROOTOF, *The Law of Cyber-Attack*, in *California Law Review*, 2012, p. 829, nota 48.

conseguenza la distruzione di un oggetto, ma anche quelle ipotesi in cui ciò si verifica in via indiretta[203].

Questa definizione, tuttavia, se appare condivisibile laddove fonda la qualificazione di una operazione come 'attacco informatico' dando rilevanza alle conseguenze sia dirette che indirette che da una tale condotta possono derivare, d'altro canto ci sembra criticabile nella misura in cui considera come attacchi informatici anche quelle operazioni che si esplicano in condotte meramente difensive[204].

Definizioni di *cyber attack* sono rintracciabili anche in fonti ulteriori, alcune governative altre inter-governative. Da un lato, infatti, abbiamo quella fornita dagli Stati Uniti, in particolare dalla *United States Cyber Command* (d'ora in poi USCYBERCOM)[205], dall'altro lato quella della *Shanghai Cooperation Organization* (d'ora in poi SCO), un organismo intergovernativo fondato nel 2001 dai Capi di Stato di Cina, Russia, Kazakistan, Kirghizistan, Tagikistan e Uzbekistan.

La prima fa riferimento ad una definizione militare di *cyber attack* fornendone una nozione più limitata: gli attacchi informatici sarebbero quelle azioni, compiute attraverso l'uso di computer ovvero di altri dispositivi elettronici, che intendono manomettere o distruggere le infrastrutture informatiche 'critiche' di uno Stato ovvero il loro

---

[203] Manuale di Tallin, rule 30, par. 3.

[204] Un esempio di tale operazione può essere l'utilizzo di antivirus che proteggono computer o una rete di computer da attacchi esterni; come tale non ci sembra possa essere ricondotta, una operazione del genere, nel novero delle definizioni di attacco informatico. Differente, invece, è il discorso con riguardo alla cd. active defense intesa come una 'contromisura elettronica' «designed to strike attacking computer systems and shut down cyber attacks midstream. (…) For the most part, active defenses are classified, though programs that send destructive viruses back to the perpetrator's machine or packet-flood the intruder's machine have entered the public domain», cfr. CARR, *Inside Cyber Warfare*, Sebastopol, 2010, p. 46.

[205] Trattasi di un Commando, facente parte dell'esercito americano, specializzato in tutte quelle attività di coordinamento, di pianificazione e di conduzione di operazioni nel contesto del cd. cyberspazio. Cfr. http://www.arcyber.army.mil/Organization/USCyberCommand.

funzionamento[206]. Tali attacchi possono essere compiuti anche indirettamente attraverso l'uso di trasmettitori elettronici, *malware*[207] o anche con differenti periferiche. Anche qui, come nella definizione adottata nel Manuale di Tallin, l'attenzione è posta sugli obiettivi di tali attacchi e le loro conseguenze (cd. *Objective-based approach*)[208]. Tuttavia, siffatta definizione non ci sembra del tutto convincente. Invero, la stessa limiterebbe notevolmente l'ambito di operatività degli attacchi informatici, escludendo quegli attacchi che non sono rivolti verso infrastrutture informatiche che siano classificate come 'critiche' da uno Stato[209].

D'altro canto, invece, la definizione fornita dalla SCO comprende quelle azioni, perpetrate con l'uso delle nuove tecnologie di informazione

[206] Si riporta la definizione completa: «a hostile act using computer or related networks or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves-for instance, attacks on computer system witch are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery». Cfr. CARTWRIGHT, *Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operations* 5, 2011, p. 5, par. 10.

[207] Con tale termini si fa riferimento a un qualsiasi software utilizzato per rubare informazioni sensibili, accedere a sistemi informatici privati o mostrare pubblicità indesiderata. I tipi di *malware* più noti sono i *virus* e i *worm.*

[208] HATHAWAY, CROOTOF, *op. cit.*, p. 824.

[209] Il problema della definizione di infrastrutture critiche di uno Stato si è posto anche in relazione al cd. approccio *target based* o *strict liability*. Questo approccio si baserebbe sul bersaglio, oggetto dell'attacco. In particolare, sarebbero ritenuti attacchi vietati alla luce del diritto internazionale quelli rivolti a 'infrastrutture nazionali definite come critiche'. D'accordo con altri autori, riteniamo che questo tipo di approccio sia inappropriato ai nostri fini. Almeno per due motivi: in primo luogo, non vi è una definizione internazionalmente accetta di 'infrastruttura critica', e ciò potrebbe comportare una interpretazione estensiva o restrittiva del termine in relazione alle concerete circostanze che si palesano. In secondo luogo, questo approccio non è sorretto da una pressi statale. Cfr. CONDRON, *Getting It Right: Protecting American Critical Infrastructure, in Cyberspace,* in *Harvard Journal of Law and Technology,* 2007, p. 415-416; COUZIGOU, *The Challenges Posed by Cyber Attacks to the Law on Self-Defence,* in *European Society of International Law Conference Paper* n. 16/2014, 2014, p. 8.

e comunicazione, volte a destabilizzare le decisioni prese dalla società e dallo Stato: siano questi di tipo politico, economico ovvero culturale; definendo così la *information war* come «*mass psyhological brainwashing to destabilize society and State (…)*» (cd. *Means-based approach*)[210]. Una definizione così ampia appare immotivatamente estesa. Il rischio concreto che si corre è appunto quello di limitare qualsiasi attività che ha luogo in internet. A ben vedere, in considerazione dei paesi che compongono la SCO, tale pericolo non appare così peregrina; basti pensare alle censure che in molti dei paesi suindicati vengono mosse alla libera espressione in internet con particolare riguardo alle tematiche di carattere politico[211].

La definizione di attacco informatico maggiormente utilizzata in dottrina, che ci sentiamo di condividere, è quella fornita dal Dipartimento della difesa americano. Quest'ultimo definisce i *Computer Network Attack* (d'ora in poi CNA) come quelle azioni intraprese con l'utilizzo di reti di computer al fine di 'oscurare' (in inglese, *deny)*, 'interrompere', 'degradare' o 'distruggere' le informazioni contenute nel computer, reti di computer o, anche, i computer e le reti stesse[212]. Tale definizione ci dà, in

[210] HATHAWAY, CROOTOF, *op. cit.*, p. 825.

[211] *Ibidem*, p. 825.

[212] Vale la pena specificare il significato che viene dato ai singoli termini utilizzati. Laddove si parla di 'oscurare' (*deny*) si intende il diniego all'accesso di informazioni, ad utenti autorizzati, per un determinato periodo di tempo; 'l'interruzione', invece, è quella operazione volta alla riprogrammazione in maniera surrettizia di altri computer per interromperne i processi. Un esempio classico di tale tipologia di attacco è quello volto alla forzata sospensione della energia elettrica, in una data area, attraverso la manomissione di quei sistemi che erogano l'energia stessa. Per 'degradazione' si intende un particolare tipo di attacco volto a ridurre la capacità di elaborazione dei sistemi informatici, attraverso l'induzione all'uso di mezzi meno efficienti, con lo scopo di rallentare i cicli logistici e decisionali; infine, la tipologia più invasiva di attacco è quella che si esplica attraverso la 'distruzione' di una rete di computer e le sue risorse sia *software* che *hardware.* Al fine di raggiungere tale scopo si fa uso di specifici programmi informatici come *virus, malware, worm* etc. Cfr. United States Department of Defence, *An Assessment of International Legal Issues in Information Operations,* 1999; BAYLES, *The Ethics of Computer Network Attack,* in *Journal of the US Army War College*, 2001, pp. 44-58; United States Department of Defence, *Dictonary of Military and Associated Terms,* 2010; BUFALINI, *Uso della forza, legittima difesa e problemi di attribuzione in*

primo luogo, la possibilità di distinguere il diverso grado di ingerenza che, attraverso un attacco informatico, può essere attuato nei confronti di uno Stato.

Inoltre, la proposizione di una gradualità, circa l'invasività degli attacchi, ci permette di meglio individuare le possibili contromisure che lo Stato vittima dell'attacco può eventualmente utilizzare in autotutela. Riteniamo, infatti, che tanto nel caso di operazioni meno invasive, quanto nelle ipotesi di attacco informatico con conseguenze distruttive, si possa ritenere integrato l'elemento oggettivo dell'illecito internazionale, essendo violato il principio del non intervento[213] e della sovranità territoriale dello Stato vittima[214].

In secondo luogo, la definizione implicitamente dà rilevanza all'aspetto delle conseguenze dell'attacco. Riteniamo necessario aver riguardo a quest'ultima caratteristica per una serie di motivi: anzitutto, perché ci permette di escludere, dal novero degli attacchi informatici, quelle operazioni che rientrano semplicemente in un avanzato uso della tecnologia per radiocomandare armi a distanza (basti pensare, ad esempio, all'uso di droni) o all'ipotesi differente di *cyber espionage*[215]. Inoltre, così procedendo, si esclude la possibilità che attraverso un uso ampio della nozione di attacco informatico ne discenda un modo per controllare e censurare la libertà di espressione (soprattutto in ambito politico) in internet.[216] Si pensi ad esempio ai recenti sforzi da parte di alcuni governi

situazione di attacco informatico, in TANZI, LANCIOTTI (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2011, p. 432;

[213] Su questo aspetto si rimanda al par. 3.1 del Capitolo II

[214] BUFALINI, *op.cit.*, p. 416.

[215] ANTOLIN-JEKINS, *Defining the Parameters of Cyberwar Operations: Looking for Law in all Wrong Places?*, in *Naval Law Review*, 2006, p. 138.

[216] HATHAWAY, CROOTOF, *op.cit.*, pp. 824-825.

(Iran, Egitto) di limitare l'uso dei nuovi *media* alle organizzazioni politiche[217].

Una volta così individuata la definizione di attacco informatico è altresì necessario capire se e in che modo una operazione informatica possa violare un obbligo internazionale.

3.1 Divieto dell'uso della forza e attacchi informatici

Una volta definiti gli aspetti più rilevanti degli attacchi informatici, bisogna procedere considerando dapprima il rapporto tra quest'ultimi e il divieto di uso della forza e, successivamente, analizzare il principio del non intervento negli affari interni di uno Stato.

Il principio che sancisce il divieto di usare la forza è stato definito come «the heart of the United Nation Charter»[218] e, com'è noto, esso è espressamente previsto dall'art. 2 par. 4 della Carta delle Nazioni Unite, secondo il quale gli Stati membri «devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza»[219]. È altresì noto che la disposizione in esame rifletta un principio di diritto internazionale consuetudinario, nonché appartenga a quella categoria di norme imperative che prendono il nome di *jus* cogens[220].

---

[217] *Ibidem*; DEHGHAN, *Iran Clamps Down on internet Use*, The Guardian, 5 gennaio 2012, disponibile su https://www.theguardian.com/world/2012/jan/05/iran-clamps-down-internet-use.

[218] HENKIN, *The Reports of the Death of Article 2(4) are Greatly Exaggerated*, in *American Journal of International Law*, 1971, p. 544-54

[219] Traduzione dell'Autore. Cfr. Carta della Nazioni Unite, San Francisco, 1945, art. 2 par. 4. Più nel dettaglio il menzionato articolo stabilisce che «[a]ll 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».

[220] La natura consuetudinaria dell'art. 2 par. 4 della Carta delle Nazioni Unite è stata riconosciuta dalla Corte Internazionale di Giustizia nella nota sentenza sulle *Attività militari e paramilitari in e contro il Nicaragua*. Al paragrafo 188 della Sentenza, la Corte stabilisce infatti

A fronte di tale imperativo principio occorre tuttavia capire il significato da attribuire al termine 'forza'. A tal fine è necessario ricorrere agli artt. 31 e 32 della Convenzione di Vienna sul diritto dei trattati del 1969. Come è noto, l'art 31 stabilisce che «un trattato deve essere interpretato in buona fede seguendo il senso ordinario da attribuire ai

che « both Parties take the view that the principles as to the use of force incorporated in the United Nations Charter correspond, in essentials, to those found in customary international law. The Parties thus both take the view that the fundamental principle in this area is expressed in the terms employed in Article 2, paragraph 4, of the United Nations Charter. They therefore accept a treaty-law obligation to 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. The Court has however to be satisfied that there exists in customary international law an opinio juris as to the binding character of such abstention. This opinio juris may, though with al1 due caution, be deduced from, inter alia, the attitude of the Parties and the attitude of States towards certain General Assembly resolutions, and particularly resolution 2625 (XXV) entitled "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations". The effect of consent to the text of such resolutions cannot be understood as merely that of a "reiteration or elucidation" of the treaty commitment undertaken in the Charter. On the contrary, it may be understood as an acceptance of the validity of the rule or set of rules declared by the resolution by themselves. The principle of non-use of force, for example, may thus be regarded as a principle of customary international law, not as such conditioned by provisions relating to collective security, or to the facilities or armed contingents to be provided under Article 43 of the Charter. It would therefore seem apparent that the attitude referred to expresses an opinio juris respecting such rule (or set of rules), to be thenceforth treated separately from the provisions, especially those of an institutional kind, to which it is subject on the treaty-law plane of the Charte». A paragrafo 190 continua poi « A further confirmation of the validity as customary international law of the principle of the prohibition of the use of force expressed in Article 2, paragraph 4, of the Charter of the United Nations may be found in the fact that it is frequently referred to in statements by State representatives as being not only a principle of customary international law but also a fundamental or cardinal principle of such law. The International Law Commission, in the course of its work on the codification of the law of treaties, expressed the view that "the law of the Charter concerning the prohibition of the use of force in itself constitutes a conspicuous example of a rule in international law having the character of jus cogens9'(paragraph (1) of the commentary of the Commission to Article 50 of its draft Articles on the Law of Treaties, ILC Yearbook, 1966-11, p. 247). Nicaragua in its Memorial on the Merits submitted in the present case States that the principle prohibiting the use of force embodied in Article 2, paragraph 4, of the Charter of the United Nations "has come to be recognized as jus cogens". The United States, in its Counter-Memorial on the questions of jurisdiction and admissibility, found it material to quote the views of scholars that this principle is a "universal norm", a "universal international law", a "universally recognized principle of international law", and a "principle of jus cogens». Cfr. Corte Internazione di Giustizia, *Attività militari e paramilitari in e contro il Nicaragua* (Nicaragua c. Stati Uniti), 27 giugno 1986, parr. 187-190.

termini del trattato nel loro contesto e alla luce del suo oggetto e del suo scopo»[221], ciò vuol dire che laddove si volesse attribuire al termine 'forza' il suo significato ordinario si dovrebbe giungere alla conclusione secondo cui esso include qualsiasi tipologia di forza e non solo quindi quella armata[222]. A ciò va aggiunto che l'art. 2 par. 4 non fa alcun riferimento alla tipologia di forza vietata, mentre non mancano ipotesi in cui all'interno della Carta il termine forza è espressamente qualificato come *armata*. Se si guarda, ad esempio, il Preambolo della Carta si può notare come ad essere richiamata è esclusivamente la forza di tipo *armata*[223]. Allo stesso modo, se si volge lo sguardo agli ulteriori articoli della Carta, e precisamente agli artt. 41-46, si può notare come il Consiglio di sicurezza può adottare misure «not involving the use of armed force or if such measures prove inadequate, armed force»[224]. Ebbene, se si volesse procede attraverso questo metodo comparatistico si dovrebbe giungere nuovamente alla conclusione che l'assenza di una espressa previsione nell'art. 2 par. 4 della Carta sta ad indicare che il divieto ricomprende non solo la forza *armata*, ma presumibilmente anche la forza politica ed economica.

Senonché la norma in questione deve altresì essere esaminata alla luce delle altre disposizioni dell'art. 31 (1) della Convenzione di Vienna. In particolare, una volta attribuito un dato significato al termine è necessario

[221] Questo articolo si può considerare corrispondente al diritto internazionale consuetudinario. In tal senso si è espressa la Corte Internazionale di Giustizia nella decisione *Arbitral Award* del 31 giugno 1989, secondo cui «[a]rticles 31 and 32 of the Vienna Convention on the Law of Treaties…may in many respects be considered as a codification of existing customary international law». Cfr. *I.C.J. Reports 1991*, pp. 69-70, par. 48.

[222] Cfr. BUNCHAN, *Cyber Attakcs: Unlawful Uses of Force or Prohibited Invterventions*, in *Journal of Conlfict and Security Law*, 2012, p. 215.

[223] Secondo il Preambolo della Carta delle Nazioni Unite, infatti, « (…) to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest (…)».

[224] Cfr. Carta delle Nazioni Unite, cap. VII.

verificare che lo stesso sia compatibile con i principi del trattato stesso. In altre parole, non è possibile attribuire un dato significato ad un termine nel trattato se questo poi risulta essere in contrasto con lo scopo e l'oggetto del trattato stesso[225]. Questa precisazione è particolarmente rilevante rispetto a quanto si sta analizzando. E ciò essenzialmente perché la Carta delle Nazioni Unite riconosce in modo abbastanza chiaro che suo scopo è quello di assicurare la pace e la sicurezza internazionale, nonché quello di limitare il diritto degli Stati di usare la forza armata[226]. Emblematico, a tal file, è proprio il preambolo[227] della Carta il quale specifica che le Nazioni Unite sono un'organizzazione creata al fine di prevenire «the scourage of war»[228] e che «armed force shall not be used, save in the common interest»[229]. Dunque, se lo scopo principale delle NU è quello di limitare l'uso della forza armata, ciò vuol dire che il termine forza usato nell'art. 2 par. 4 va interpretato nel senso di forza *armata*[230].

Ebbene, sulla base delle brevi considerazioni qui effettuate è facile notare come l'interpretazione dell'art. 2 par. 4 denoti non poche difficoltà. A ben vedere, infatti, le indicazioni testuali forniscono elementi a supporto di entrambe le interpretazioni, sia quella che fa rientrare nel divieto di uso

[225] AUST, *Modern Treaty Law and Practice*, Cambridge, 2007, p. 235.

[226] BUNCHAN, *op.cit.*, p. 215.

[227] Come è noto l'art. 31 (2) della Convenzione di Vienna sul diritto dei trattati del 1969 stabilisce che « Ai fini dell'interpretazione di un trattato, il contesto comprende, oltre al testo, il preambolo e gli allegati ivi compresi: ogni accordo in rapporto col trattato e che è stato concluso fra tutte le parti in occasione della conclusione del trattato; ogni strumento posto in essere da una o più parti in occasione della conclusione del trattato e accettato dalle parti come strumento in connessione col trattato».

[228] Carta della Nazioni Unite, preambolo.

[229] *Ibidem.*

[230] BUNCHAN, *International Law and the Construction of the Liberal Peace*, Oxford, 2013, p. 57.

della forza la sola forza armata sia quella per cui il divieto potrebbe essere esteso anche a coercizioni economiche oppure politiche[231].

Per superare tale disomogeneità interpretativa è possibile richiamare nuovamente la Convenzione di Vienna del 1969, il cui articolo 32[232], rubricato mezzi complementari di interpretazione, stabilisce che «[s]i può fare ricorso ai mezzi complementari di interpretazione, e in particolare ai lavori preparatori e alle circostanze nelle quali il trattato è stato concluso, allo scopo, sia di confermare il senso che risulta dall'applicazione dell'art. 31, sia di determinare il senso quando l'interpretazione data in conformità all'articolo 31: lascia il senso ambiguo o oscuro; oppure conduce ad un risultato che è manifestamente assurdo o irragionevole». La disposizione richiamata assume particolare rilevanza proprio in relazione all'art. 2 (4); ciò principalmente perché dai lavori preparatori si evince come le diverse proposte di qualificare il divieto di uso della forza in modo più ampio si siano tutte concluse con un nulla di fatto: durante i lavori preparatori la prima proposta era quella di includere nel divieto di uso della forza ipotesi ulteriori rispetto alla forza armata.

Più dettagliatamente, ad esempio, la delegazione brasiliana aveva proposto che l'art. 2 par. 4 espressamente proibisse la minaccia o l'uso della forza, nonché la minaccia e l'uso di misure economiche che fossero incompatibili con lo scopo delle Nazioni Unite. Com'è noto, la proposta è rimasta tale e non si è mai convertita in altro, non essendo stata accettata da parte dei paesi occidentali[233]. Epilogo analogo si è avuto con le richieste avanzate dall'Ecuador, il quale voleva includere il divieto dell'uso della

[231] In questo senso si veda, tra gli altri, BENATAR, *The Use of Cyber Force: Need for Legal Justification?* in *Goettingen Journal of International Law*, 2009, p. 383. Secondo l'Autore infatti «the wording of article 2(4) is ambiguous to say the least. The very same text is conducive to radically opposed understandings of the concept of force».

[232] Anche l'art. 32 può essere considerato alla stregua del diritto internazionale consuetudinario. Si veda nota n. 186.

[233] *Ibidem.*

forza morale e fisica[234], e con quelle dell'Iran che invece sollecitava gli altri Membri ad includere quantomeno il divieto della forza politica, secondo le parole di quest'ultimo, infatti, «[a]ll the Member States of the Organization should refrain from intervening in their international relations, either directly or indirectly, in the internal affairs of the other States and from the threat or use of force in any manner inconsistent with the purposes of the Organization»[235].

Ebbene, attraverso l'uso supplementare dei lavori preparatori è quindi possibile affermare che il divieto previsto dall'art. 2(4) della Carta fa riferimento esclusivamente ad una specifica tipologia di forza e cioè quella armata[236].

Invero, in tal senso depongono anche le successive dichiarazioni emanate dalle Nazioni Unite. A tal proposito basti pensare, ad esempio, alla 'Dichiarazione relativa ai principi di diritto internazionale, concernenti le relazioni amichevoli e la cooperazione fra gli stati, in conformità con la carta delle nazioni unite' del 1970[237], la 'Dichiarazione sulla definizione di aggressione', del 1974 e la 'Dichiarazione sul non uso della forza', del 1987. Per quanto concerne la prima, essa distingue l'uso della coercizione economica e politica dall'uso delle armi, specificando che nel primo caso ci troviamo dinanzi ad un caso annoverabile alle ipotesi

[234] UNCIO, vol 3, 422 (Ecuador)

[235] UNCIO, vol 6, 563 (Iran)

[236] Secondo alcuni autori «The term does not cover any possible kind of force, but is, according to the correct and prevailing view, limited to armed force». Si veda RANDELZHOFER, *Article 2(4)*, in SIMMA (a cura di), *The Charter of the United Nations: A Commentary*, Oxford, 2002, p. 117. Secondo altri «Unfortunately, "force" itself is a flexible term. Under modern conditions the threat or use of economic retaliation may be as effective against a weaker state as the threat or use of armed force. But it appears that the prohibition of Article 2(4) is directed exclusively at force in the sense of 'armed force'»: BENTWICH, MARTIN, *A Commentary of the Charter of the United Nations,* Routledge, 1950, p. 12.

[237] Assemblea Generale, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations,* A/RES/2625 (XXV), 24 ottobre 1970.

di obbligazioni dello Stato a non intervenire negli affari interni di un altro Stato e non è invece da considerare una *species* del principio che obbliga gli Stati ad astenersi dall'usare la forza nelle relazioni con altri Stati[238].

In modo non dissimile si pronuncia anche la Dichiarazione sul non uso della forza, la quale prende in considerazione le ipotesi di coercizione economica[239] e l'uso della forza[240] come due situazioni ben distinte.

Infine, oltre ai lavori preparatori e alle indicazioni fornite dalle dichiarazioni successive all'adozione della Carta, anche la prassi degli Stati converge verso una definizione di uso della forza di tipo restrittivo, che includa esclusivamente la forza *armata*. E infatti molto raramente le misure coercitive di carattere economico e politico sono state annoverate all'interno del all'art. 2 (4) della Carta[241].

---

[238] Secondo la citata dichiarazione, da un lato, «No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law»; dall'altro lato, invece, « No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State». Cfr. *Ibidem*.

[239] Secondo l'art. 8 della Dichiarazione, infatti, «No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the excercise of its sovereign rights and to secure from it advantages of any kind». Cfr. Assemblea Generale, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraing from the Threat or Use of Force in International Relations*, UNGA Res 42/22 (1987).

[240] Secondo l'art. 7 della Dichiarazione, infatti, «State have the duty to abstein from armed interventation and all others form of interference or attempted threats against the personality of the State or against its political, economic and cultural elements». Cfr. Assemblea Generale, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraing from the Threat or Use of Force in International Relations*, UNGA Res 42/22 (1987).

[241] HENDERSON, *The Use of Force and International Law*, Cambridge, 2018, p. 55. In senso contrario, e cioè per considerare misure coercitive di carattere economico come ipotesi rientranti nell'art. 2 (4) della Carta si veda, in generale, LARAE-PEREZ, *Economic Sanctions as a Use of Force: Re-Evaluationg the Legality of Sanctions from an Effects-Based Perspective*, in *Boston University International Law Journal*, 2002, p. 161 ss.

Una volta individuata quale tipologia di forza è necessaria affinché sia integrato l'art. 2(4) della Carta, occorre chiedersi se un attacco informatico, nella definizione precedentemente utilizzata, sia in grado di raggiungere il livello di forza *armata* e di conseguenza integrare una violazione dell'art. 2 (4).

Data l'attuale potenzialità degli attacchi informatici, basti pensare ad un attacco informatico che comprometta le infrastrutture essenziali di uno Stato oppure un attacco capace di provocare la distruzione di un aereo o di altre apparecchiature militari, non può aprioristicamente escludersi che un attacco informatico possa essere inteso come espressione dell'uso della forza. Appare innegabile quindi che allorquando una operazione informatica produca effetti del tutto simili a quelli che si sarebbero potuti verificare con tradizionali mezzi bellici, questo non possa che essere considerato come una violazione del divieto di uso della forza[242]. D'altro canto, l'art. 2 (4) non prevede alcuna distinzione in merito al mezzo attraverso cui l'uso della forza debba poi concretarsi. Inoltre, anche la Corte Internazionale di Giustizia, nel caso relativo alla *liceità dell'uso delle armi nucleari*, riferendosi alla Carta, ha affermato che «[t]hese provisions do not refer to specific weapons. They apply to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, nor permits, the use of any specific weapon, including nuclear weapons. A weapon that is already unlawful per se, whether by treaty or custom, does not become lawful by reason of its being used for a legitimate purpose under the Charter»[243].

[242] BUFALINI, *Uso della forza, legittima difesa e problemi di attribuzione in situazione di attacco informatico*, in LANCIOTTI, TANZI (a cura di), Uso della forza e legittima difesa nel diritto internazionale contemporaneo, Napoli, p. 417.

[243] *Legality of the Threat or Use of Nuclear Weapons*, *I.C.J. Reports*, 1996, par. 39

Ciò detto, è altrettanto vero che la forza armata intesa in senso tradizionale ha sempre fatto riferimento ad armi che producessero una forza cinetica, e cioè armi che producessero una vera e propria esplosione[244]. Questo approccio tuttavia può ritenersi ampiamente superato se non altro per il fatto che così procedendo si escluderebbero dal divieto di uso della forza anche armi chimiche, biologiche e nucleari che di per sé non causano sempre una esplosione in senso stretto.

Al fine di superare l'approccio fondato sul tipo di arma utilizzata, e proprio per ricomprendere all'interno dell'art. 2 (4) anche ipotesi nuove che non erano state direttamente prese in considerazione dalla Carta, Brownlie sostenne che l'interpretazione dell'art. 2 dovesse basarsi sugli *effetti* che l'arma produce. Secondo l'Autore, poi, il limite per determinare se vi è stata un'azione contraria al divieto di uso della forza è quello di considerare se l'arma usata abbia causato «destruction to life and property»[245].

Per quanto riguarda lo specifico settore degli attacchi informatici, è possibile individuare tre differenti approcci per inquadrare una operazione informatica nell'art. 2 (4).

Il primo, che riposa essenzialmente su una concezione classica dell'uso della forza, si basa sulla tipologia di arma utilizzata. Questo approccio ha senz'altro il pregio, in astratto, di distinguere in modo chiaro la coercizione armata (che integra una violazione dell'art. 2 (4)) da quella economica e politica, che invece come abbiamo visto non rientra nelle ipotesi previste dall'art. 2(4). Secondo una parte della dottrina, sulla base di questa qualificazione, un attacco informatico sarebbe espressione dell'uso della forza solo allorquando esso sia capace di limitare l'utilizzo di una rete elettrica in quanto, prima dell'evoluzione tecnologica, l'unico

[244] BROWNLIE, *International Law and the Use of Force by States*, Clarendon, 1963, p. 362
[245] *Ibidem*.

modo per raggiungere un tale scopo era attraverso l'ausilio di bombe o di altre forme di forza cinetica[246]. Senonchè, questa categorizzazione dopo una più attenta analisi non appare altro che un'altra ipotesi che possa rientrare nell'approccio basato sugli effetti dell'azione[247].

Appare altresì evidente che questo modo di procedere determinerebbe, in ultima analisi, l'esclusione dell'applicazione dell'art. 2(4) al contesto informatico in quanto un attacco informatico, che per sua natura non rientra nella nozione classica di 'arma', non potrebbe mai raggiungere la soglia dell'uso della forza. Circostanza quest'ultima che sebbene rara non può essere categoricamente esclusa.

Il secondo approccio, invece, qualifica un attacco informatico alla stregua di un attacco armato, contrario all'art. 2 (4), sulla base delle infrastrutture colpite dell'operazione (cd. *target-based approach*). In altre parole, affinché si possa dire che un attacco informatico sia contrario all'art. 2 (4) è necessario che l'operazione informatica sia rivolta verso le infrastrutture critiche della nazione[248]. Seguendo questo schema, un attacco informatico dovrebbe essere automaticamente considerato un attacco armato per il semplice fatto che esso sia rivolto ad una specifica infrastruttura[249].

Anche questa teoria mostra diversi punti deboli e almeno due sono facilmente individuabili.

In primo luogo, è agevole constatare come all'interno della definizione di infrastruttura critica sia possibile annoverare un elevato numero di

---

[246] GRAHAM, *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 2010, p. 91.

[247] HANDLER, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, in *Stanford Journal of International Law*, 2012, p. 227.

[248] SHARP, *Cyberspace and the Use of Force*, 1999, p. 129-132.

[249] A causa di questa qualificazione automatica, questo approccio è stato definito anche di 'strict liability'. Cfr. GRAHAM, *op.cit.*, p. 91.

sistemi, di risorse, di processi appartenenti ad una determinata nazione. Secondo gli Stati Uniti, e precisamente la legge sulla protezione delle infrastrutture critiche, si evince che sono tali «systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters».[250] Il Dipartimento per la sicurezza nazionale, inoltre, ha fatto rientrare nel novero delle infrastrutture critiche circa trenta differenti settori[251]. Ebbene, se si volesse considerare questo approccio si finirebbe con l'affermare che un attacco informatico, indipendentemente dal grado di offensività, sarebbe contrario al divieto di uso della forza semplicemente quando rivolto contro uno di questi settori, che in buona sostanza riguardano tutti gli aspetti di uno Stato. A questa osservazione, va poi aggiunto che una non essendovi una definizione internazionalmente condivisa ed accettata di 'infrastruttura critica', potrebbe discenderne una interpretazione estensiva o restrittiva del termine in relazione alle concerete circostanze che si palesano[252].

Il secondo motivo per cui il *target based apporach* non può essere condiviso riguarda essenzialmente il mancato riferimento alla gradualità che può assumere un attacco informatico.

Com'è stato notato in dottrina, infatti, una operazione informatica può produrre effetti con intensità completamente diversi. Si può infatti

[250] Cfr. 42 U.S.C., par. 5195(e).

[251] I settori riguardano l'agricoltura, il cibo, l'acqua, la salute, i servizi di emergenza, il governo, le industrie, le telecomunicazioni, l'energia, i trasporti, il sistema bancario e finanziario, le industrie chimiche. Cfr. Dipartimento per la sicurezza nazionale, *National Infrastructure Protection Plan,* 2005, p. 103.

[252] CONDRON, *Getting It Right: Protecting American Critical Infrastructure, in Cyberspace,* in HJLT, 2007, p. 415- 416; COUZIGOU, *The Challenges Posed by Cyber Attacks to the Law on Self-Defence*, in *European Society of International Law Conference Paper n. 16/2014*, 2014, p. 8.

assistere ad operazioni volte esclusivamente a creare effetti indesiderati, si pensi ad esempio alla manomissione temporanea di un sistema, oppure ad azioni potenzialmente pericolose, che posso concretarsi nell'implementazione di una cd. bomba logica[253] nel *software* informatico, il quale non produrrà danni immediati ma solo futuri. Infine, può realizzarsi l'ipotesi più grave, che consiste in azioni immediatamente distruttive, come la manomissione permanente di un sistema tramite un virus[254]. Orbene, seguendo l'approccio *de quo* si arriverebbe quindi alla errata conclusione per cui tutte le operazioni poc'anzi descritte integrerebbero una violazione dell'art. 2(4) senza distinzione alcuna.

L'ultimo approccio è quello si fonda sugli effetti/conseguenze dell'azione[255]. Secondo questo metodo, e nonostante le sue diverse varianti, il focus per determinare se una azione informatica integra una violazione del divieto di uso della forza si basa sugli effetti che essa produce. In altre parole, allorquando un attacco informatico produca degli effetti uguali a quelli prodotti da un attacco tradizionale, vale a dire effetti distruttivi sulle cose o sulle persone, allora si potrà ritenere che una tale operazione sia espressione dell'uso della forza così come previsto dalla Carta[256]. Se questo può essere considerato il punto nodale della teoria

[253] Con il termine 'bomba logica' si fa riferimento ad una specifica parte di codice informatico, inserito in un dato software, che produce i suoi effetti allorquando determinate condizioni si verificano.

[254] Cfr. HOLLIS, *Why States need International Law for Information* Operations, in *Lewis and Clark Law* Review, 2007, p. 1042

[255] Nonostante la similitudine terminologica tra i due termini, la locuzione 'effetti' è quella maggiormente utilizzata ed accettata pertanto anche in questo lavoro si farà riferimento ad essa.

[256] Cfr. BUCHAN, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, in *Journal of Conflict and Security Law*, 2012, p 212; DINNISS, *Cyber Warfare and the Laws of War*, Cambridge: Cambridge University Press, 2012, p 74. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2012, p. 47. Inoltre, la tesi che si basa sul riconoscimento degli effetti degli attacchi informatici è stata riconosciuta anche dagli Stati Uniti, i quali in più occasioni hanno ribadito: «[t]here is no way to be certain how these principles of international law will be applied by the international community to computer network attacks. As with other developments in international law, much will depend on how

basata sugli effetti dell'azione, è tuttavia necessario rilevare che all'interno di questa cornice sono stati individuate differenti ipotesi particolari maggiormente attagliate allo specifico settore degli attacchi informatici.

---

the nations and international institutions react to the particular circumstances in which these issues are raised for the first time. If we were to limit ourselves to the language of Article 51, the obvious question would be, "Is a computer network attack an 'armed attack' that justifies the use of force in self-defense?" If we focused on the means used, we might conclude that electronic signals imperceptible to human senses don't closely resemble bombs, bullets, or troops. On the other hand, it seems likely that the international community will be more interested in the consequences of a computer network attack than in its mechanism. It might be hard to sell the notion that an unauthorized intrusion into an unclassified information system, without more, constitutes an armed attack. On the other hand, if a coordinated computer network attack shuts down a nation's air traffic control system along with its banking and financial systems and public utilities, and opens the floodgates of several dams resulting in general flooding that causes widespread civilian deaths and property damage, it may well be that no one would challenge the victim nation if it concluded that it was a victim of an armed attack, or of an act equivalent to an armed attack. Even if the systems attacked were unclassified military logistics systems, an attack on such systems might seriously threaten a nation's security. For example, corrupting the data in a nation's computerized systems for managing its military fuel, spare parts, transportation, troop mobilization, or medical supplies may seriously interfere with its ability to conduct military operations. In short, the consequences are likely to be more important than the means use» (cfr. US Department of Defense, *An Assessment of International Legal Issues in Information Operations*, May 1999, p 18). In modo non dissimile si è espresso anche il Legal Advisor del Dipartimento di Stato americano, Harold Koh, il quale ha sostenuto che « [i]n analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.* In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors: including the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes. Only a moment's reflection makes you realize that this is common sense: if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force». (Cfr. KOH, *International Law in Cyberspace*, Speech at the USCYBERCOM Inter-Agency Legal Conference, 18 September 2012, in GUYMON (a cura di), *Digest of United States Practice in International Law*, 2012, p 595.

Secondo una prima teoria è stato sostenuto che ogni operazione informatica che intenzionalmente produca effetti distruttivi all'interno del territorio di un altro Stato è di per sé un'azione contraria a quanto stabilito dall'art. 2(4)[257].

Tale conclusione, tuttavia, non appare condivisibile.

Anzitutto, non pochi dubbi sorgono in relazione al significato del termine 'distruttivo', non essendo chiaro se l'Autore si riferisca alle sole ipotesi di distruzione fisica oppure se includa anche ipotesi di coercizione economica.

Anche volendo ammettere, come d'altronde sostiene il fautore di questa tesi, che il termine in questione vada inteso in senso ampio e che quindi possa ricomprendere non solo ipotesi di distruzione fisica, ma anche quelle di danni economici, la conclusione in ogni caso non appare accettabile[258]. Secondo l'Autore, infatti, ancorché l'art. 2 (4) non ricomprenda tutte le ipotesi di coercizione economica e politica che abbiano lo scopo di influenzare le azioni di un altro Stato, la sua portata si estenderebbe per ricomprendere quelle ipotesi in cui la coercizione

[257] SHARP, *Cyberspace and the Use of Force,* 1999, p. 133. Secondo l'Autore, più precipuamente, «it was concluded that the scope, duration, and intensity of the force must be analysed to determine if an armed attack has occurred and what may constitute a necessary and proportional response. Should a computer network attack cause a single train to crash, it would be an unlawful use of force but likely not an armed attack. In contrast, should a computer network attack cause dozens of such trains and aircraft to crash, it would very likely be considered an armed attack which invokes the victim state's right to use force in self-defence. Accordingly, *any* computer network attack that intentionally causes *any* destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of article 2(4) that may produce the effects of an armed attack prompting the right of self-defense.

[258] Nello stesso senso si veda SILVER, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in SCHMITT, O'DONNELL (a cura di) *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, International Law Studies, 2002, p. 86.

politica ed economica sia tale da inficiare l'integrità territoriale o l'indipendenza di un altro Stato[259].

Il problema principale di questa tesi, anche volendo prescindere dalla sua contrarietà intrinseca all'interpretazione maggioritaria dell'art. 2(4), è essenzialmente quello di introdurre un criterio distintivo tra azioni informatiche che si concretano in coercizioni economiche e che assurgono ad una violazione dell'indipendenza, e quelle invece che si limitano ad influenzare le azioni di un altro Stato. Differenziazione che nella pratica difficilmente potrà risultare utile.

Sempre sulla base della teoria degli effetti, è stata altresì avanzata una differente ipotesi volta a distinguere gli attacchi informatici che integrano una coercizione economica e politica da quelli che invece sono contrari all'art. 2(4). In particolare, ci riferiamo alla teoria proposta da Schmitt, il quale parte da una differenziazione di base: da un lato vi sono quei casi considerati di facile risoluzione per cui se una operazione informatica produce danni materiali a cosa oppure a persone in maniera analoga a quanto farebbe un attacco tradizionale allora le due ipotesi sarebbero totalmente sovrapponibili e dunque l'attacco informatico sarà contrario all'art. 2 (4) della Carta. I casi in cui può verificarsi siffatta circostanza sono riconducibili, ad esempio, al caso in cui un gruppo di hacker, attraverso un attacco informatico, riesca a manomettere il sistema di

[259] SHARP, *op.cit.*, p. 86. Lo stesso Autore ha poi affermato che «it was concluded that if a state uses the internet to cause a single train crash in another state, it would be an unlawful use of force but not one of a scope, duration, and intensity to constitute an armed attack. In contrast, it would very likely be considered an armed attack should a state cause dozens of such incidents, or if a state caused one major incident such as the complete and long-term crash of the New York Stock Exchange. *Ibidem*, p. 117.

controllo del traffico aereo provocando la caduta di un aeroplano[260] oppure riesca a dare istruzioni ad una centrale nucleare per autodistruggersi[261].

Dall'altro lato invece vi sono tutte quelle ipotesi in cui l'utilizzo del paradigma classico del divieto di uso della forza risulta particolarmente difficile. Proprio in relazione a quest'ultima categoria, sono stati enucleati almeno cinque differenti criteri in presenza dei quali una operazione informatica può essere considerata espressione dell'uso della forza[262]. I criteri individuati sono i seguenti: s*everity* (grado di gravità che un attacco armato è capace di produrre, esso ricomprende solo le ipotesi in cui l'azione comporta danni fisici o la distruzione di uno o più beni)[263]; *immediacy* (ovvero la velocità con cui si producono le conseguenze dell'attacco)[264]; *directness* (il grado di collegamento che sorge tra l'attacco in *sé* e le sue dirette conseguenze)[265]; *invasiveness* (indica l'alto

[260] A tal proposito è stata sottolineata la vulnerabilità del sistema di aviazione statunitense, argomentando che « [t]he Federal Aviation Administration ("FAA") diligently maintains a mantle of safety in increasingly crowded skies, but it depends on computers. An unfriendly power or terrorist group could develop the capability for a devastating, concerted attack on FAA computers nationwide. Recently, the radars at the busy Pittsburgh airport were blinded for six full minutes,5 giving us a snapshot of what a test of a capability to attack that system could be like». Cfr. BOWMAN, *Is International Law Ready for the Informational Age?*, in *Fordham International Law Journal*, 1995, p. 1939.

[261] L'esempio è stato avanzato in dottrina in questi termini « [a]salient point is that an excessive computer dependency creates a special vulnerability.48 The more technologically advanced-and, therefore, computer reliant-a State is, the more susceptible it is to a paralyzing CNA. Overall, State A may be less developed scientifically and technologically than State B. 49 Yet, the very advantage of State B becomes a debilitating burden once State A manages to penetrate State B's electronic defenses. This, writ large, is the scenario of a nuclear core meltdown. Through a CNA, State A-having no nuclear capability of its own-can in a sense "go nuclear" by exploiting the scientific and technological infrastructure of State B, thus turning the tables on the target State. State B, as it were, provides the nuclear weapon against itself (the weapon being triggered by agents of State A)». Cfr. DINSTEIN, *Computer Network Attacks and Self-Defense*, in SCHMITT, O'DONNELL, *op.cit.*, p. 105.

[262] SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, p. 914.

[263] *Ibidem*.

[264] *Ibidem*.

[265] *Ibidem*.

livello di intrusione perpetrato all'interno dello Stato vittima dell'attacco)[266]; *measurability* (si riferisce alla facilità con cui è possibile accertare la misura dell'attacco)[267]. Tali criteri sono stati poi utilizzati anche dal Tallinn Manual 2.0, che ha aggiornato la versione precedente del 2013, il quale alla regola 69 fornisce la definizione di uso della forza rilevante per gli attacchi informatici affermando che «[a]cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force»[268].

Ebbene, nonostante la teoria in esame resti quella maggiormente richiamata in dottrina, per il grado di dettaglio che la stessa propone, va rilevato che essa non è scevra da critiche.

---

[266] *Ibidem*.

[267] *Ibidem*.

[268] Il Manuale, invero, fornisce una più puntuale descrizione di quello che deve intendersi con ognuno dei termini indicati. E infatti al suo interno è possibile leggere « (a)Severity. Subject to a de minimis rule, consequences involving physical harm to individuals or property will in and of themselves qualify a cyber operation as a use of force. Those generating mere inconvenience or irritation will never do so. Between the extremes, the more consequences impinge on critical national interests, the more they will contribute to the depiction of a cyber operation as a use of force. In this regard, the scope, duration, and intensity of the consequences will have great bearing on the appraisal of their severity. Severity is the most significant factor in the analysis. (b) Immediacy. The sooner consequences manifest, the less opportunity States have to seek peaceful accommodation of a dispute or to otherwise forestall their harmful effects. Therefore, States harbour a greater concern about immediate consequences than those that are delayed or build slowly over time, and are more likely to characterise a cyber operation that produces immediate results as a use of force than one that takes weeks or months to achieve its intended effects. (c) Directness. The greater the attenuation between the initial act and its consequences, the less likely States will be to deem the actor in violation of the prohibition of the use of force. Whereas the immediacy factor focuses on the temporal aspect of the consequences in question, directness examines the chain of causation. For instance, market forces, access to markets, and the like determine the eventual consequences of economic coercion (e.g., economic downturn). The causal connection between the initial acts and their effects tends to be indirect – economic sanctions may take weeks or even months to have a significant effect. In armed actions, by contrast, cause and effect are closely related. An explosion, for example, directly harms people or objects. Cyber operations in which cause and effect are clearly linked are more likely to be characterised as uses of force than those in which they are highly attenuated». Cfr. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Tallinn, 2017, p. 334-335.

In primo luogo, una più attenta analisi mette in luce come la teoria *de qua* finisce per dare importanza esclusivamente agli effetti distruttivi che l'attacco informatico è in grado di produrre, non aggiungendo nulla in più rispetto alla teoria basate strettamente sugli effetti prodotti da una operazione informatica. Si potrebbe sostenere, come fatto in dottrina, che l'unico elemento realmente caratterizzante è quello relativo alla *severity*, l'unico in grado di fungere quale scriminante, dato che gli altri elementi non sarebbero di alcun aiuto nella distinzione tra uso della forza e altre forme di coercizione, come quella economica[269]. A tal proposito basti pensare al criterio della *directness*, la quale non è certamente una delle caratteristiche principale di un'azione che integra l'uso della forza armata. A tale conclusione si giunge agevolmente se si considera quanto affermato dalla Dichiarazione sulla definizione di aggressione, ove per «atto di aggressione», e cioè la più pericolosa forma di uso illegale della forza, viene inteso non solo l'uso di bombe e le invasioni territoriali nei termini tradizionali, ma anche azioni che non necessariamente producono effetti distruttivi diretti, come ad esempio il blocco dei porti o delle coste di uno Stato da parte delle forze armate di un altro Stato, oppure l'utilizzo del territorio di uno Stato al fine di compiere un'aggressione nei confronti di un terzo Stato[270].

[269] BUFALINI, *op.cit.*, p. 420.

[270] Cfr. Assemblea Generale delle Nazioni Unite, *Definizione di Aggressione*, Risoluzione 3314, dicembre 1974, ove all'articolo 3 si può più precisamente leggere che « Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provisions of article 2, qualify as an act of aggression: (a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof; (b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State; (c) The blockade of the ports or coasts of a State by the armed forces of another State; (d) An attack by the armed forces of a State on the land, sea or air forces, or marine and air fleets of another State; (e) The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the conditions

Inoltre, anche il riferimento alla *immediacy* appare inadeguato al contesto cibernetico. A tal proposito basti far riferimento all'ipotesi della cd. bomba logica, la quale per sua stessa natura produce effetti solo dopo un certo periodo di tempo oppure al verificarsi di determinate condizioni e quindi sarà capace di produrre un danno ben dopo che l'attacco è stato sferrato[271].

In linea più generale dunque si può sostenere che affinché tali elementi possano effettivamente essere considerati utili è necessaria la conoscenza di una elevata quantità di informazioni, ipotesi che almeno fino ad oggi non appare suffragata dal comportamento degli Stati, i quali invece, come visto nel precedente capitolo, appaiono ancora reticenti nel fornire le informazioni che riguardano il loro cyberspazio[272]. A ciò va poi aggiunta

provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement; (f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State; (g) The sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or its substantial involvement therein».

[271] ROSCINI, *Cyber Operations and the Use of Force in International Law*, p. 49.

[272] Questa affermazione conosce ancora poche eccezioni, ma tra queste vanno senz'altro annoverate le recenti dichiarazioni proveniente dal Regno Unito e dalla Francia. Quest'ultima, in particolare, appare particolarmente interessante in quanto fornisce un esempio di prassi che gli Stati potrebbero seguire. Più nel dettaglio, la dichiarazione analizzi i due differenti settori quello relativo allo *ius in bello* e allo *ius ad bellum* dalla prospettiva francese. Per quello che a noi interessa è senz'altro utile riportare alcune parti che forniscono utili indicazioni in materia di applicabilità delle norme di diritto internazionale agli attacchi informatici. Secondo la dichiarazione, infatti, « Les violations les plus graves de souveraineté, notamment celles qui portent atteinte à l'intégrité territoriale ou à l'indépendance politique de la France, peuvent constituer une violation du principe d'interdiction de recours à la menace ou à l'emploi de la force, lequel s'applique à tout emploi de la force indépendamment de l'arme employée. Dans l'espace numérique, le franchissement du seuil de l'emploi de la force ne dépend pas du moyen numérique employé, mais des effets de la cyberopération. Une cyberopération conduite par un État à l'encontre d'un autre Etat constitue une violation du principe d'interdiction de recourir à la force si ses effets sont similaires à ceux qui résultent de l'utilisation d'armes classiques. Toutefois, la France n'exclut pas la possibilité qu'une cyberopération dénuée d'effets physiques puisse être également qualifiée de recours à la force. En l'absence de dommages physiques, une cyberopération peut être considérée comme un recours à la force à l'aune de plusieurs critères, notamment les circonstances qui prévalent au moment de l'opération, tels que l'origine de l'opération et la nature de l'instigateur (son caractère militaire ou non), le degré d'intrusion, les

una ulteriore considerazione. La teoria esposta appare non solo estremamente soggettiva, ma anche e soprattutto parziale, non fornendo alcuna indicazione circa le ipotesi in cui un attacco informatico non raggiunga la soglia prevista dall'art. 2(4) e quindi non viola il divieto di uso della forza[273].

Le incertezze esposte dal punto di vista teorico si sono poi riversate anche nei tentativi di qualificazione degli attacchi informatici attraverso il prisma dell'art. 2(4).

Il problema, invero, si pone perché ad oggi sebbene potenzialmente un attacco informatico possa produrre degli effetti distruttivi paragonabili a quelli di un attacco tradizionale non sembra vi siano casi in cui ciò si sia effettivamente verificato.

---

effets provoqués ou recherchés par l'opération, ou encore la nature de la cible visée. Ces critères ne sont, bien entendu, pas exhaustifs. À titre d'exemple, le fait de pénétrer des systèmes militaires en vue d'atteindre les capacités de défense françaises, ou de financer, voire d'entraîner des individus afin que ces derniers perpètrent des cyberattaques contre la France pourrait, ainsi, être qualifié de recours à la force. Tout recours à la force n'est toutefois pas constitutif d'une agression armée au sens de l'article 51 de la Charte des Nations unies, notamment si ses effets sont limités, réversibles ou n'atteignent pas une certaine gravité». Cfr. Ministere des Armes, *Droit International Appliqué aux Opérations dans le Cyberspace*, 2019, p. 7.

[273] Secondo Schmitt infatti si possono verificare quattro differenti scenari, che possono essere così individuati: *i)* un attacco informatico corrisponde ad un attacco armato diretto a causare danni a degli oggetti tangibili o a degli individui, in questo caso il Consiglio di Sicurezza (Cds) ha la possibilità di qualificare l'attacco come violazione della pace o atto di aggressione e può di conseguenza utilizzare le misure previste dall'art. 42 della Carta, ovvero quelle implicati l'uso della forza; *ii)* l'operazione informatica non costituisce un attacco armato, ma il CdS ha comunque il potere di qualificare la situazione nei termini di minaccia alla pace e autorizzare l'uso della forza per evitare che la situazione sfoci in una vera e propria violazione della pace; *iii)* l'attacco informatico rappresenta un attacco armato e quindi gli Stati possono agire in legittima difesa individuale o collettiva, secondo quanto previsto dall'art. 51 della Cara; e infine *iv)* l'operazione informatica non rappresenta un attacco armato ma è parte integrante di un'operazione volta a culminare in un attacco armato. Anche in quest'ultima ipotesi gli Stati avranno la possibilità di agire in legittima difesa ai sensi dell'art. 51, ma solo se: a) «the acts in self-defense occur during the last possibile window of opportunity available to effectively counter the attack» e b) «the CNA is an irrevocable step in an imminent (near-term) and probably unavoidable attack». Cfr. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, p. 935-936.

Infatti, i tentativi di ricomprendere alcuni attacchi informatici sotto l'egida dell'art. 2(4) della Carta sono apparsi tutti particolarmente forzati e si sono conclusi con un nulla di fatto. Alla luce di questa affermazione si possono esaminare alcuni casi della prassi per comprendere più adeguatamente quanto si sta dicendo.

3.1.1. Il caso *stuxnet*

Il primo caso da esaminare, sebbene più datato, è senz'altro quello che si riferisce all'operazione informatica che prende il nome di *Stuxnet*[274]. La scelta di partire proprio da questa ipotesi si giustifica in ragione della rilevanza che il caso ha assunto in dottrina, nonché per la sua incerta qualificazione giuridica da un punto di vista internazionale.

I fatti possono essere così brevemente riassunti. Nel luglio 2010 il governo iraniano ha scoperto l'esistenza di un virus *malware* all'interno dei propri sistemi informatici. Nonostante il virus avesse infettato una ingente quantità di computer, il suo epicentro è stato individuato presso la centrale nucleare di Natanz. Quest'ultima si occupa del processo di arricchimento dell'uranio al fine di produrre materiale nucleare[275]; per

[274] I riferimenti sia in dottrina che in fonti più strettamente divulgative al caso *Stuxnet* sono particolarmente cospicui. In questa sede ci si può limitare ad indicare i seguenti: SINGER, *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*, in *Case Western Reserve Journal of International Law*, 2015, p. 79 ss.; PEAGLER, *The Stuxnet Attack: a New Form of Warfare and the (In)Applicability of Current International Law*, in *Arizona Journal of International and Comparative Law*, 2014, p. 399 ss. RICHMOND, *Evolving Battlefields: does Stuxnet demonstrate a Need for Modifications to the Law of Armed Conflict?*, in *Fordham International Law Journal*, 2012, p. 842 ss.

[275] Nonostante le dichiarazioni del governo iraniano circa l'uso esclusivamente pacifico del processo di arricchimento dell'uranio, sono note le preoccupazioni della Comunità internazionale sul tema e le risoluzioni del Consiglio di sicurezza. In particolare, la Risoluzione 1696 del 31 luglio 2006 è senz'altro emblematica. In essa infatti si può leggere « *Concerned* by the proliferation risks presented by the Iranian nuclear programme, mindful of its primary responsibility under the Charter of the United Nations for the maintenance of international peace and security, and being determined to prevent an aggravation of the situation (…) 3.

giungere a questo risultato sono necessarie condizioni precise e particolari che si concretano nell'inserimento dell'uranio all'interno di apposite centrifughe e nella loro rotazione a una determinata velocità, temperatura e pressione[276].

Il codice *Stuxnet* era stato scritto al fine di forzare la rotazione della centrifuga, causando un incremento e un successivo e repentino decremento della sua velocità. In questo modo le vibrazioni a cui essa è stata soggetta avrebbero determinato il mancato raggiungimento delle condizioni necessaria affinché il processo di arricchimento si concludesse nel modo stabilito.

Sulla base di queste vicende, va sin da subito rilevato come il governo iraniano non ha fornito informazioni dettagliate in merito alle effettive conseguenze assunte dall'operazione. Anzi, le dichiarazioni fornite dai soggetti interessati appaiano contraddittorie. Da un lato, infatti, il responsabile della organizzazione dell'energia atomica iraniana ha affermato che il virus è stato scoperto nel momento in cui ha iniziato ad *infettare* i sistemi informatici e questo ha permesso agli esperti di evitare che lo stesso producesse effetti distruttivi sulle apparecchiature[277]. Di

Expresses the conviction that such suspension as well as full, verified Iranian compliance with the requirements set out by the IAEA Board of Governors, would contribute to a diplomatic, negotiated solution that guarantees Iran's nuclear programme is for exclusively peaceful purposes, underlines the willingness of the international community to work positively for such a solution, encourages Iran, in conforming to the above provisions, to re-engage with the international community and with the IAEA, and stresses that such engagement will be beneficial to Iran; 4. Endorses, in this regard, the proposals of China, France, Germany, the Russian Federation, the United Kingdom and the United States, with the support of the European Union's High Representative, for a long-term comprehensive arrangement which would allow for the development of relations and cooperation with Iran based on mutual respect and the establishment of international confidence in the exclusively peaceful nature of Iran's nuclear programme (S/2006/521)». Cfr. Consiglio di Sicurezza, *Resolution 1696 (2006)*, S/RES/1696 (2006), 31 luglio 2006.

[276] BUCHAN, *op.cit.*, p. 219.

[277] Cfr. FAYAZMANESH, *Containing Iran: Obama's Policy of "Tough Diplomacy*, Cambridge, 2013, p. 256, ove si può leggere che «One year and several months ago, Westerners sent a virus to (our) country's nuclear sites … They had hoped to stop our speedy peaceful

contro, invece, secondo il Presidente iraniano il *software* sarebbe stato capace di produrre alcuni danni, ma l'entità degli stessi non sarebbe stata individuata[278]. Ancora diverse sono le conclusioni a cui è giunto l'Istituto per le scienze e la sicurezza internazionale, secondo il quale le vibrazioni causate alla centrifuga da parte dell'attacco informatico sarebbero sufficienti a causare la sua distruzione[279].

---

nuclear activities through software. But, we discovered the virus exactly at the same spot it wanted to penetrate because of our vigilance and prevented the virus from harming [equipment]».

[278] BUCHAN, *op.cit.*, p. 220.

[279] L'Istituto ha prodotto sia un report preliminare il 22 dicembre 2010 ove si può leggere «[a]lthough Stuxnet is a reasonable explanation for the apparent damage to module A26, questions remain about this conclusion. The attacks seem designed to force a change in the centrifuge's rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge. But still unknown are parts of the attack sequences and possible responses by the FEP control system. These responses could act during the attack to reduce the magnitude of the change in frequency or otherwise act to protect the centrifuges. A priority is better characterizing Stuxnet's attack sequences and determining Stuxnet's goals in a centrifuge plant. If its goal was to quickly destroy all the centrifuges in the FEP, Stuxnet failed. But if the goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP, while making detection difficult, it may have succeeded, at least temporarily». Cfr. ALBRIGHT, BRANNAN, WALROND, *Did Stuxnet Take out 1.000 Centrifuges at the Natanz Enrichment Plant?*, Institute for science and International Security, 22 dicembre 2010.

Dopo circa un anno lo stesso Istituto ha presentato una versione aggiornata del *report*, affermando che «[a]ssuming Iran exercises caution, Stuxnet is unlikely to destroy more centrifuges at the Natanz plant. Iran likely cleaned the malware from its control systems. To prevent re-infection, Iran will have to exercise special caution since so many computers in Iran contain Stuxnet. Although Stuxnet appears to be designed to destroy centrifuges at the Natanz facility, destruction was by no means total. Moreover, Stuxnet did not lower the production of LEU during 2010. LEU quantities could have certainly been greater, and Stuxnet could be an important part of the reason why they did not increase significantly. Nonetheless, there remain important questions about why Stuxnet destroyed only 1,000 centrifuges. One observation is that it may be harder to destroy centrifuges by use of cyber attacks than often believed. The authors of Stuxnet remain unknown. This is one of the attractions of cyber attacks. The perpetuator can easily hide. Rumors and common sense point to a country or team of countries, but proving that they engineered Stuxnet remains almost impossible. Stuxnet's elaborate nature and its updating show a firm determination to sabotage Iran's nuclear program. It is certain that foreign intelligence agencies will continue in their efforts to sabotage Iran's centrifuge program». Cfr. ALBRIGHT, BRANNAN, WALROND, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, Insitute of Science and International Security, 15 febbraio 2011.

Come anticipato, le problematiche relative a questo caso riguardano non solo gli aspetti fattuali ma soprattutto quelli relativi alla qualificazione giuridica di tale operazione. In altre parole, ci si chiede se *Stuxnet* sia un attacco informatico capace di integrare una violazione del divieto di uso della forza.

Bisogna sin da subito rilevare come una risposta definitiva e soddisfacente al problema non sia stata ancora raggiunta. Le ipotesi dottrinarie che si sono susseguite sul tema sono molteplici ed eterogenee tra loro, tuttavia è possibile sussumerle intorno a due distinti filoni: uno secondo cui l'attacco informatico sarebbe sicuramente espressione dell'uso della forza; e l'altro per cui *Stuxnet* solo potenzialmente può essere inquadrato come azione contraria all'art. 2 (4).

Per quanto concerne il primo gruppo di autori, i quali ritengono l'azione informatica una chiara violazione dell'art. 2(4), essi giustificano tale conclusione in quanto il *malware* è stato intenzionalmente progettato per essere usato nei confronti di un altro Stato ed ha causato la distruzione fisica di alcune delle strutture presenti sul territorio dello Stato stesso, e cioè, in particolare, il sistema di centrifughe della centrale[280].

Secondo altri, invece, più direttamente il caso *Stuxnet* è qualificabile come uso della forza in quanto capace di produrre danni fisici e tangibili alle infrastrutture nucleari dello Stato iraniano[281].

---

[280] In questi termini si veda BROWN, *Why Iran Didn't Admit Stuxnet was an Attack*, in *Joint Force Quarterly*, 2011, p. 70.

[281] Su questa posizione si vedano BOOTHBY e altri, *When is a Cyberattack a Use of Force or an Armed Attack?*, in *Computer Journal*, 2012, p. 82-83; FIDLER, *Was Stuxnet an Act of War? Decoding a Cyberattack*, in *IEEE Security and Privacy*, 2011, p. 56-57; MOORE, *Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models*, in *Naval Law Review*, 2015, p. 24. Secondo quest'ultimo Autore, infatti, «Applying the effects-based model, Stuxnet would be a violation of Article 2(4)'s prohibition of the use of force because of the overall physical and economic effects of the malware on the Iranian nuclear complex. The effects-based model looks at the scope and magnitude of the cyberattack on the target state. With Stuxnet, the scope and magnitude of the effects include the infiltration and exploitation of computer systems and the destruction of more than ten percent of the centrifuges

Alla medesima categoria va ricondotta altresì quella parte di dottrina che ha analizzato il caso *Stuxnet* attraverso il prisma del Tallinn Manual. Secondo costoro infatti il caso *de quo* integrerebbe il criterio della *severity*, precedentemente individuato come criterio determinante per la differenza tra uso della forza armata e coercizioni economiche e politiche, in quanto «the Stuxnet attack was severe because it caused physical harm to property. Stuxnet caused the centrifuges to speed up and slow down their rotation causing them to break»[282].

Allo stesso modo va rigettata la tesi di segno opposto secondo cui non avendo causato nessun danno fisico, l'attacco non si è concretizzato nemmeno in un illecito internazionale e pertanto dovrebbe essere considerato «legal masterpiece»[283]. È agevole obiettare in questo caso che sebbene l'attacco non abbia raggiunto la soglia di uso della forza armata, esso è senz'altro qualificabile come atto contrario al divieto di non ingerenza negli affari interni di uno Stato (*infra*).

Al secondo gruppo, invece, vanno ricondotte quelle ipotesi che prospettano una soluzione meno netta, alla quale anche noi ci sentiamo di aderire. Le conclusioni da cui muove questa parte della dottrina è l'incertezza circa le concrete e reali conseguenze che l'attacco informatico ha assunto. Su questa necessaria considerazione, ci sembra che la soluzione più adeguata al caso, e cioè quella capace di rispecchiarne al

---

at Iran's largest nuclear fuel enrichment plant. Based on the scope and magnitude of the effects of Stuxnet on Natanz, the attack would be a use of force prohibited by Article 2(4) equivalent to an armed attack».

[282] WEISSBRODT, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, in *Minnesota Journal of International Law*, 2013, p. 376. A conclusion simili giungono anche FOLTZ, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, in *Joint Force Quarterly*, 2012, p. 44; POCHÉ, *This Means War! (Maybe?) – Clarifying Casus Belli in Cyberspace*, in *Oregon Review of International Law*, 2013, p. 413 e 433-434; DEV, *Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response*, in *Texas International Law Journal*, 2014, p. 395.

[283] ZIOLKOWSKI, *Stuxnet – Legal Considerations*, in *Journal of International Law of Peace and Armed Conflict*, 2012, p. 142.

meglio gli aspetti fattuali, si basi sulla non qualificazione di *Stuxnet* come espressione dell'uso della forza. Invero, questa conclusione si può agevolmente spiegare se si considera che l'unico effetto certo di *Stuxnet* è quello di aver modificato la velocità di operazione della centrifuga. Così stando le cose non si ritenere che questa attività sia espressione dell'uso della forza. Discorso diverso, invece, *andrebbe* fatto laddove l'effetto indiretto causato dalla modifica si fosse concretizzato in una effettiva distruzione o danneggiamento dell'infrastruttura[284].

3.1.2. L'attacco informatico statunitense nei confronti dell'Iran del 20 giugno 2019

L'altro caso che intendiamo esaminare riguarda una più recente vicenda che ha visto protagonisti sempre l'Iran e gli Stati Uniti. A differenza del caso precedente, quest'ultimo non è stato ancora oggetto di un diffuso interesse da parte della dottrina. La sua trattazione, tuttavia, appare interessante in quanto l'attacco è stato ritenuto da parte della dottrina un esempio di oparazione informatica contraria al divieto di uso della forza[285]. Brevemente, stando alle fonti esistenti (la maggior parte di natura giornalistica), gli Stati Uniti hanno lanciato un attacco informatico nei confronti di un gruppo di spie iraniane collegate al Corpo di guardia rivoluzionario iraniano come reazione agli attacchi subiti alle petroliere nello stretto di Hormuz, nonché all'abbattimento di un drone di

[284] Alle medesime conclusioni giungono anche BUCHAN, *op.cit.*, p. 220-221; WOLTAG, *Computer Network Operations Below the Level of Armed Force*, in *ESIL Conference Paper Series*, Conference Paper No. 1/2011, 2011, p. 7.

[285] Cfr. SCHACK, *Did the US Stay "Well Below the Threshold of War" With its June Cyberattack on Iran?*, in *Ejil:Talk! Blog of the European Journal of International Law*, settembre 2019. Consultabile online al seguente indirizzo http://www.ejiltalk.org/did-the-us-stay-well-below-the-threshold-of-war-with-its-june-cyberattack-on-iran/.

sorveglianza americano[286]. L'obiettivo preciso dell'attacco non è stato specificato, né individuato, ma si ritiene sia stavo rivolto contro i *database* usati dal gruppo paramilitare iraniano per tracciare ed effettuare gli attacchi contro le petroliere, riducendo così, almeno temporalmente, le capacità di Teheran di gestire segretamente il traffico delle navi nel golfo persico[287]. Secondo fonti iraniane, i sistemi non sono stati utilizzabili per diversi mesi e l'attacco, sebbene originariamente dovesse avere una durata solo limitata, ha avuto effetti più lunghi del previsto[288], tant'è che gli esperti sarebbero tuttora impegnati nel recupero delle informazioni distrutte.

Parte della dottrina ha provato a qualificare l'attacco informatico come espressione dell'uso della forza vietata dall'art. 2 (4) della Carta. Per giungere a questa conclusione è stata richiamata la regola 69 del Tallinn Manual che, come precedentemente visto, fonda la qualificazione degli attacchi informatici sulla base dei criteri della «*severity, invasiveness, State involvment, military character*». Secondo la ricostruzione effettuata dalla dottrina, l'attacco è stato condotto da una unità militare statunitense (la USCYBERCOM) contro infrastrutture militari iraniane. Inoltre, gli effetti dell'attacco sono stati immediati percepibili e le conseguenze direttamente connesse all'attacco. Su queste premesse si è giunti alla conclusione che l'operazione informatica sia espressione dell'uso della forza[289]. In altre parole, secondo la tesi prospettata, allorquando una unità

[286] *Ibidem*.

[287] BARNES, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, *The New York Times*, 28 agosto 2019, consultabile online al seguente indirizzo https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber attack.html?action=click&module=Top%20Stories&pgtype=Homepage

[288] SCHACK, *op.cit.*

[289] Secondo l'Autore di questa tesi, più precisamente, «[g]oing through these criteria, it seems reasonable to conclude that their application points towards classifying the US cyberattack as use of force. Specifically, in terms of the *severity*, *invasiveness*, *State involvement*, and *military character* of the attack, it is noteworthy that it was conducted by a

militare di uno Stato conduca una operazione informatica contro l'unità militare di un altro Stato e questa ne determina per un significativo lasso di tempo una limitazione nell'utilizzo, allora si potrò concludere che l'attacco informatico sia espressione della forza anche in assenza di un danno fisico effettivo[290].

A noi pare che nonostante lo sforzo di questa ricostruzione, la conclusione a cui esso giunge non può essere condivisa.

Anzitutto, si nutrono alcuni dubbi circa la ricostruzione giuridica da cui parte l'autore. Se come sostengono le diverse fonti, l'attacco informatico è stato lanciato in risposta ad un attacco precedentemente subito (l'abbattimento dei droni) allora il punto di vista dell'analisi dovrebbe partire non dalla qualificazione attraverso l'art. 2(4), ma piuttosto da quello delle contromisure e più in particolare dalla legittima difesa (art. 51 della Carta delle Nazioni Unite). In quest'ottica ci si potrebbe chiedere se l'azione sia conforme all'art. 51, giungendo presumibilmente a conclusioni negative non essendo soddisfatti tutti i requisiti necessari per poter reagire in legittima difesa[291]. Ma, anche volendo prescindere dalla impostazione metodologica, giungere alla conclusione *de qua* attraverso l'utilizzo dei criteri del Tallinn Manual appare senz'altro forzata. Come abbiamo avuto modo di vedere in precedenza, l'aspetto determinante per

US military unit (US Cyber Command) against Iranian military assets, which were apparently critical to Iran's capabilities in the Hormuz Strait, and that the attack deleted or made unavailable information and took computer systems – including military communications networks – offline for several months. Additionally, in terms of the *immediacy* and *directness* criteria, the effects of the attack seem to have occurred immediately and with direct causality between the attack and the harm done. Furthermore, the harm seems clearly *measurable* in the sense that there has been significant publicity about the target and effects of the attack. Finally, the militaristic nature of the attack seems to dispense with the *presumptive legality* issue. As such, this method points towards finding a use of force». Cfr. SCHACK, *op.cit.*.

[290] *Ibidem.*

[291] In particolare, è difficile affermare che l'attacco statunitense abbia rispettato i requisiti di necessità e proporzionalità.

poter qualificare un attacco informatico secondo questa teoria è la necessaria presenza quantomeno della *severity*. Nel caso di specie, invece, almeno sulla base delle informazioni finora disponibili, non pare vi sia stata la distruzione né tantomeno un danno concreto alle infrastrutture iraniane, essendosi limitato il 'danno' ad un malfunzionamento del sistema. A nulla rileva il fattore temporale, essendo un elemento eccessivamente variabile ed arbitrario.

Ebbene, sulla base dei casi qui esposti si può forse intravedere uno degli aspetti più controversi degli attacchi informatici rispetto al diritto internazionale, vale a dire: se un attacco informatico non raggiunge la soglia del divieto di uso della forza, ma si sostanzia in un comportamento capace di interrompere il funzionamento di una infrastruttura di uno Stato, oppure rendere inaccessibili alcuni servizi, oppure limitare la fruibilità di alcuni di essi sarà sempre lecito da un punto di vista internazionale?

La risposta a questa domanda è senz'altro di carattere negativo, in quanto è ben possibile che venga violato un altro principio fondamentale del diritto internazionale, e cioè il principio del non intervento negli affari interni di uno Stato di cui si darà conto nei prossimi paragrafi.

4. Il principio del non intervento negli affari interni di uno Stato

Il principio del non intervento negli affari interni di uno Stato nella sua originaria accezione si limitava a prevedere il divieto per uno Stato di intervenire negli affari interni di un altro attraverso il solo uso della forza. Questa teoria, attribuita a Vattel, non faceva nessun riferimento espresso alle parole 'interferenze' o 'intervento', ma si limitava a sostenere che l'intervento dei paesi europei nel Nuovo Mondo con l'uso della forza

violava le regole della guerra[292]. Senonché ad oggi è certamente possibile riconoscere al principio in esame non solo un contenuto diverso, che non si riferisca alla sola 'interferenza' attraverso l'uso della forza, ma è possibile altresì qualificarlo nei termini di un principio di carattere consuetudinario[293].

Esso, inoltre, è oggi inteso come uno dei corollari del diritto di sovranità territoriale dello Stato, della sua integrità territoriale e della sua indipendenza economica[294], e si concreta nel divieto da parte di uno Stato di intervenire *coercitivamente* nei confronti di un altro in quelle materie in cui lo Stato (offeso), in base al principio di sovranità, può decidere

[292] ZURBUCHEN, *Vattel's 'Law of Nations' and the Principle of NonIntervention*, in Grotiana, 2010, p. 69. Da un punto di vista storico, come detto, la prima formulazione del principio del non internvento viene sovente attribuita a Vattel, anche se è discutibile che vi fosse una prassi degli Stati antecedente al diciannovesimo secolo. A tal proposito, spesso si fa riferimento alla cd. dottrina Monroe, proclamata dal presidente statunitense nel 1823, secondo cui «any interposition for the purpose of oppressing them [the newly formed states of the Americas] or controlling in any other manner their destiny» sarebbe stata intesa come una minaccia agli Stati Uniti d'America.

[293] In questi termini si è espressa la Corte Internazionale di Giustizia nel noto caso tra Stati Uniti e Nicaragua, ove la Corte ha precisato che «the Court considers that it [the principle of non-intervention] is part and parce of customary international law. As the Court has observed: "Between independent States, respect for territorial sovereignty is an essential foundation of international relations" (I.C.J. Reports 1949, p. 35), and international law requires political integrity also to be respected. Expressions of an *opinio juris* regarding the existence of the principle of non-intervention in customary international law are numerous and not difficult to find. Of course, statements whereby States avow their recognition of the principles of international law set forth in the United Nations Charter cannot strictly be interpreted as applying to the principle of non-intervention by States in the interna1 and external affairs of other States, since this principle is not, as such, spelt out in the charter. But it was never intended that the Charter should embody written confirmation of every essential principle of international law in force. The existence in the *opinio juris* of States of the principle of non-intervention is backed by established and substantial practice. It has moreover been presented as a corollary of the principle of the sovereign equality of States». Cfr. International Court of Justice, *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), 27 giugno 1986, par. 202.

[294] OPPENHEIM, *International Law*, IX edizione (a cura di Robert Jennings, Arthur Watts), 1992, p. 428-51.

liberamente come comportarsi. Fanno parte di questa categoria le scelte politiche, economiche, sociali e culturali, nonché la politica estera[295].

L'interferenza in sé, intesa come influenza negli affari interni di uno Stato, non costituisce una violazione del principio del non intervento[296].

Ciò che caratterizza il principio in esame è infatti la presenza dell'elemento *coercitivo*[297]. D'altronde ciò appare chiaro sin dalla formulazione adottata nella "Dichiarazione relativa ai principi di diritto internazionale, concernenti le relazioni amichevoli e la cooperazione fra gli Stati", ove viene indicato che «[n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind»[298]. Il testo, invero, riprende in modo quasi speculare quanto stabilito diversi anni prima all'interno della 'Dichiarazione sulla inammissibilità di intervenire negli affari interni di uno Stato e la protezione della sua indipendenza e sovranità'[299] per poi essere utilizzato nella successiva Carta dei diritti

[295] Nella sentenza *Nicaragua* viene precisato infatti « in view of the generally accepted formulations, the principle forbids al1 States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty. to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy». Cfr. *Nicaragua*, par. 205.

[296] *Ibidem.*

[297] JAMNEJAD, WOOD, *The Principle of Non-intervention*, in *Leiden Journal of International Law*, 2009, p. 348.

[298] UN Doc. A/Res/2625(XXV).

[299] La dichiarazione infatti stabilisce che «[n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind. Also, no State shall organize, assist, foment, Finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State». Cfr. Assemblea Generale, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protecion of Their Independence and Sovereignty*, A/RES/20/2131, 21 dicembre 1965.

economici[300], nonché in successive risoluzioni dell'Assemblea Generale[301].

Allo stesso modo anche la CIG nella sentenza *Nicaragua* ha precisato che «[a] prohibited intervention must (…) be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social

[300] All'art. 32 della Carta è stabilito che «No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights». Cfr. *Charter of Economic Rights and Duties of States*, GA Res. 3281, 1974.

[301] Cfr. Peaceful and Neighbourly Relations among States, UN Doc. A/1236 (XII) (1957); Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, UN Doc. A/2131 (XX) (1965 Declaration); Status of the Implementation of the Declaration on the Inadmissibility of Intervention in the DomesticAffairs of States and the Protection of their Independence and Security, UN Doc. A/Res/2225 (XXI) (1966); Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, UN Doc. A/Res/2625(XXV) (1970); Charter of Economic Rights and Duties of States, UN Doc. A/Res/3281(XXIX) (1970); Declaration on the Establishment of the New International Economic Order, UN Doc. A/Res/3201 (S-VI) (1974); Non-interference in the Internal Affairs of States, UNDoc.A/Res/31/91 (1976 Declaration); Non interference in the Internal Affairs of States, UNDocs. A/Res/32/153 (1977), A/Res/33/74 (1978), A/Res/34/101 (1979), A/Res/35/159 (1980); Declaration on the Inadmissibility of Intervention and Interference in the Interna lAffairs of States,UNDoc.A/Res/36/103 (1981 Declaration); SolemnAppeal to States in Conflict to Cease ArmedAction Forthwith and to SettleDisputes between Them throughNegotiations, and to StatesMembers of the United Nations to Undertake to Solve Situations of Tension and Conflict and Existing Disputes by Political Means and to Refrain from the Threat or Use of Force and from any Intervention in the Internal Affairs of Other States, UNDoc. A/Res/40/9 (1985); EconomicMeasures as aMeans of Political and Economic Coercion against Developing Countries, UN Docs. A/Res/39/210 (1984), A/Res/40/185 (1985), A/Res/41/165 (1986), A/Res/42/173 (1987), A/Res/44/215 (1989), A/Res/46/210 (1991), A/Res/48/168, (1993); Unilateral Economic Measures as a Means of Political and Economic Coercion against Developing Countries, UN Docs. A/Res/52/181 (1997), A/Res/54/200 (1999), A/Res/56/179 (2001), A/Res/58/198 (2003), A/Res/60/185 (2005), A/Res/62/183 (2007); Respect for the Principles of National Sovereignty and Non-interference in the Internal Affairs of States in Electoral Processes, UN Docs. A/RES/44/147 (1989), A/RES/45/151 (1990), A/RES/46/130 (1991), A/RES/47/130 (1992), A/RES/48/124 (1993), A/RES/50/172 (1995), A/Res/52/119 (1997), A/RES/54/168 (1999); Respect for the Principles of National Sovereignty and Non-interference in the Internal Affairs of States in Electoral Processes as an Important Element for the Promotion and Protection of Human Rights, UN Doc. A/Res/56/154 (2001). L'importanza del principio del non intervento è stata poi ribadita anche dal Consiglio di Sicurezza nella Risoluzione 1790 del 2007.

and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention is particularly obvious in the case of an intervention which uses force, either in the form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State»[302].

Dalla breve rassegna casistica qui esposta appare chiaro che affinché un comportamento possa dirsi contrario al principio del non intervento, e quindi non si limiti ad essere una mera 'interferenza', è necessaria la presenza di almeno due elementi: l'operazione deve interessare aspetti che rientrino all'interno del cd. dominio riservato degli Stati e allo stesso tempo deve avere un carattere coercitivo[303].

Ciò detto, e nonostante i chiarimenti forniti dalla CIG, resta da capire cosa debba intendersi per comportamento coercitivo e se il principio del non intervento possa essere utile per qualificare quegli attacchi informatici che non raggiungono la soglia dell'uso della forza come illeciti.

La presenza dell'elemento coercitivo, invero, è stata studiata in relazione a determinate circostanze, giungendo a conclusioni diverse in base alla singola ipotesi presa in considerazione[304]. Tuttavia, ciò che appare certo è che tale principio è volto a tutelare un novero di ipotesi del tutto diverse rispetto alla sua originaria concezione. Esso può essere

[302] *Nicaragua*, par. 205.

[303] Cfr. SCHMITT, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, in *Chicago Journal of International Law*, 2018, p. 48.

[304] Si pensi ad esempio ai casi relativi al prematuro riconoscimento e non riconoscimento della soggettività giuridica di uno Stato, e in particolare al caso che ha interessato il riconoscimento della Abkhazia e dell'Ossezia del sud da parte della Russia e della Georgia e alla condanna da parte della comunità internazionale (cfr. JAMNEJAD, WOOD, *op.cit*, p. 373.). Oppure alle ipotesi maggiormente controverse come la propaganda o la diplomazia (cfr. *Ibidem*, p. 374).

qualificato come un principio essenziale relativo, che muta in relazione ai cambiamenti del diritto internazionale[305]. Secondo le parole di Oppenheim, l'essenza dell'elemento *coercitivo* riposa sul fatto che il comportamento dello Stato deve essere capace di privare un altro Stato del controllo di cui egli normalmente gode su quella specifica materia[306]. In definitiva, quindi, l'elemento determinate resta quello della *coercizione* intesa come quelle attività capaci di minare e di 'interferire' con tutti quegli aspetti che uno Stato è libero di scegliere autonomamente. Ebbene, così delineato il principio bisogna domandarsi se esso può essere utile a configurare un illecito internazionale allorquando venga posta in essere una operazione informatica.

4.1. Attacchi informatici e violazione del principio del non intervento

Per quanto concerne la declinazione del principio del non intervento in riferimento agli attacchi informatici, bisogna muovere, almeno da un punto di vista generale, dalle stesse considerazioni effettuate nel paragrafo precedente. E cioè affinché un attacco informatico possa essere considerato in violazione del principio del non intervento è necessario che vi siano due requisiti: l'operazione deve interessare uno degli aspetti appartenenti al dominio riservato degli Stati e deve essere *coercitiva*[307]. In assenza di uno dei due, l'operazione può costituire una interferenza, ma non raggiungerà la soglia di un intervento illecito.

[305] *Ibidem*, p. 381.

[306] JENNINGS, WATTS (a cura di), *Oppenheim's International Law*, IX edizione, 2008, p. 428.

[307] Sono diversi gli autori che ammettono l'applicazione del principio del non intervento al contesto degli attacchi informatici. Si veda, tra gli altri, RUOTOLO, *internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012, p. 101.

Per quanto riguarda il primo aspetto, le attività rientranti nel dominio riservato dello Stato sono spesso sovrapposte a quelle facenti capo alla sovranità dello Stato stesso. E, nonostante una prima limitazione della sovranità degli Stati si è avuta con riguardo al trattamento degli stranieri, i limiti più importanti alla libertà dello Stato di comportarsi come meglio crede sono oggi rappresentati da quelle norme, per lo più di carattere convenzionale, che perseguono valori di giustizia, di cooperazione e di solidarietà tra i popoli[308]. Nonostante ad oggi il *dominio riservato* dello Stato sia sempre più oggetto di limitazioni, basti pensare all'incessante sviluppo della materia dei diritti umani, che ha in un certo senso eroso la esclusiva competenza degli Stati per tutti gli aspetti della sua politica interna, un esempio di attività che senz'altro rientra nella sfera sia del *dominio riservato* che della sovranità dello Stato è rappresentato dalla scelta del sistema politico e di conseguenza nelle elezioni politiche[309]. E infatti è proprio su questo aspetto che intendiamo concentrarci. Un'attività informatica posta in essere da uno Stato straniero capace di influenzare il processo elettorale decisionale di uno Stato può essere senz'altro intesa come ingerenza negli affari interni dello Stato, ma affinché possa dirsi violato il principio del non intervento è necessario che vi sia, come più volte ribadito, anche l'elemento *coercitivo.*

L'individuazione di quest'ultimo nel contesto virtuale non è di certo agevole. Abbiamo già avuto modo di vedere che, anche prescindendo dalle

[308] Così CONFORTI, *Diritto Internazionale*, XI edizione (a cura di Massimo Iovane), 2018, p. 213.

[309] La CIG nella sentenza Nicaragua ha puntualmente affermato che tra gli aspetti che riguardano il dominio riservato di uno Stato si può far certamente rientrare «the choice of politica system»; SCHMITT, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, *op.cit.*, p. 49; TSAGOURIAS, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, in *Ejil:Talk! Blog of The European Journal of International Law*, 2019, consultabile online al seguente indirizzo https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/

caratteristiche del cyberspazio, non sempre è facile capire quando ci si trova in una ipotesi in cui il requisito della *coercizione* è soddisfatto. Tuttavia, ai nostri fini, può essere utile quanto stabilisce il Tallinn Manual in tema di intervento negli affari interni di uno Stato attraverso operazioni informatiche. Secondo il Manuale infatti la *coercizione* si riferisce ad un atto volto a privare un altro Stato della sua libertà di scelta, e cioè a forzare tale Stato ad agire in modo involontario oppure ad astenersi senza la sua volontà dall'agire in un determinato modo[310].

Non vi è dubbio che alcune operazioni informatiche possano soddisfare l'elemento coercitivo. Come affermato dagli Stati Uniti, infatti, «a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention»[311]. In altre parole, bloccare il sistema di votazione di un Paese attraverso un attacco informatico, ad esempio disabilitando i suoi sistemi informatici oppure attraverso l'invio di un *virus* capace di limitare le funzioni del sistema, è senz'altro un comportamento qualificabile in violazione del principio del non intervento. In queste situazioni, il risultato delle elezioni, che è espressione della libertà di coloro che vanno a votare, viene manipolato contro la volontà degli elettori stessi[312].

---

[310] Secondo il Tallinn Manual, che a sua volta riprende quanto detto nella Dichiarazione sulle relazioni amichevoli tra gli Stati, il termine *coercizione* «is not defined in international law. As used in this Manual, coercion is not limited to physical force, but rather refers to an affirmative act designed to deprive another State of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way». Cfr. Tallinn Manual, op.cit., p. 317.

[311] EGAN, *Remarks on International Law and Stability in Cyberspace*, 10 novembre 2006, consultabile online al seguente indirizzo https://www.state.gov/s/l/releases/remarks/264303.htm

[312] SCHMITT, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, p. 50.

Se questo è vero, è altrettanto vero però che non tutte le operazioni informatiche volte ad influenzare le decisioni in un altro Stato possono intendersi come contrarie al principio *de quo*. E, infatti, la coercizione deve essere distinta dalla persuasione, dalla mera critica, dalla propaganda, e cioè da tutte quelle azioni che perseguono l'obiettivo di influenzare le azioni dello Stato bersaglio, ma non quello di convincerlo oppure forzarlo ad assumere quei determinati comportamenti[313].

Per meglio comprendere come potrebbe agire il principio *de quo* rispetto agli attacchi informatici, possiamo prendere ad esame quanto accaduto durante le elezioni presidenziali del 2016 negli Stati Uniti[314]. Brevemente, per quanto riguarda gli aspetti fattuali della vicenda, durante la campagna elettorale per le elezioni presidenziali, alcuni *hacker* sono riusciti ad infiltrarsi nei computer del Comitato democratico statunitense, che sosteneva i candidati democratici, e hanno sottratto informazioni rilevanti per poi renderle pubbliche sul sito WikiLeaks[315].

[313] In questi termini, è ancora una volta utile riportare quanto dice il Tallinn Manual al commentario della regola 66 (*Intervention by States*), ove viene specificato che «(…) coercion must be distinguished from persuasion, criticism, public diplomacy, propaganda (see also discussion in Rule 4), retribution, mere maliciousness, and the like in the sense that, unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State, or seek no action on the part of the target State at all. As an illustration, a State-sponsored public information campaign via the internet designed to persuade another State of the logic of ratifying a particular treaty would not amount to a violation of the prohibition of intervention. Similarly, if a State's Ministry of Foreign Affairs publishes content on social media that is highly critical of another State's internal and external policies, the activity is not coercive in nature and therefore does not constitute prohibited intervention. The key is that the coercive act must have the potential for compelling the target State to engage in an action that it would otherwise not take (or refrain from taking an action it would otherwise take). A few Experts, however, argued that it is impossible to prejudge whether an act constitutes intervention without knowing its specific context and consequences. For them, the context and consequences of a particular act that would not normally qualify as coercive could raise it to that level».

[314] Per una ricostruzione dettagliata dei fatti si rimanda a BANKS, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, in *Texas Law Review*, 2017, p. 1487-1490.

[315] EFRONY, SHANY, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, in *American Journal of International Law*, 2018, p. 609.

Contestualmente venivano rubate dall'account di posta elettronica del Presidente dalla campagna elettorale di uno dei candidati migliaia di email[316]. Secondo le indagini effettuate dalla *Intelligence* americana a sostenere gli attacchi informatici contro gli Stati Uniti vi era la Russia, la quale, aveva interesse nel favorire la vittoria del candidato repubblicano[317].

Ebbene, affinché tale operazione possa essere considerata alla stregua di un intervento negli affari interni è necessario che essa involga una delle attività rientranti nel dominio riservato degli Usa e, allo stesso tempo, che sia coercitiva.

Se per quanto riguarda il primo aspetto non sorgono particolari problemi, essendo la scelta delle politiche interne e le modalità con cui si pongono in essere le elezioni certamente appartenenti a quella sfera di competenza esclusiva di ciascuno Stato, bisogna invece interrogarsi se siamo in presenza anche del secondo elemento.

In sostanza, un'azione coercitiva ha lo scopo di indurre lo Stato a fare qualcosa, come prendere una decisione che altrimenti non prenderebbe o di non impegnarsi in un'attività in cui altrimenti si impegnerebbe. Pertanto, si può dire che la coercizione è volta a subordinare la volontà sovrana dello Stato che è stato vittima dell'operazione[318].

Nel caso dell'intervento nelle elezioni, ciò potrebbe manifestarsi allorquando si verifichi la votazione di candidato che altrimenti non avrebbe vinto, l'indebolimento della base politica di un candidato prescelto oppure, al contrario, il rafforzamento del sostegno di un candidato senza successo in previsione delle elezioni future. Ebbene, nel caso che qui si sta esaminando non può escludersi che la natura segreta dell'operazione

[316] *Ibidem*.
[317] *Ibidem*.
[318] JAMNEJAD, WOOD, *op.cit.*, p. 381.

informatica abbia privato l'elettorato americano della sua libertà di scelta, creando una situazione in cui non poteva valutare equamente le informazioni fornite. Poiché gli elettori non erano consapevoli di essere stati manipolati da un potere straniero, il loro processo decisionale, e così la capacità di controllare il loro governo, è stata indebolita e distorta.

La qualificazione di tali operazioni come 'intervento' poggia sulla circostanza che esse sono state appositamente create per esercitare il controllo su una materia di esclusiva competenza dello Stato attraverso un espediente come ad esempio informazioni false, fuorvianti o generalmente manipolate[319].

Si può sostenere dunque che l'operazione di *hacking* e il rilascio delle informazioni hanno interferito con il processo elettorale introducendo informazioni che, ancorché si vogliano considerare autentiche, sono state acquisite con mezzi espressamente vietati dal diritto interno degli Stati Uniti, nonché dalla legge della maggior parte degli altri Stati, vale a dire la penetrazione illegale e diffusione di dati privati[320]. In questo senso, la libertà di scelta dell'elettorato è stata ampiamente compromessa.

---

[319] TSAGOURIAS, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, in *Ejil:Talk! Blog of The European Journal of International Law*, consultabile online al seguente indirizzo https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/

[320] Per quanto riguarda la legge degli Stati Uniti, infatti, secondo il paragrafo 1080 della legge sulle frodi e altre attività connesse all'uso di computer viene stabilito che « a) Whoever- (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation will fully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or will fully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

Senonché a questa ricostruzione potrebbe essere obiettato il fatto che non vi è certezza che l'intervento russo negli affari interni degli Stati Uniti abbia determinato effettivamente il risultato delle elezioni. In altre parole, bisogna capire se affinché si possa parlare di illecito internazionale per violazione del principio del non intervento sia necessario che vi sia un nesso di causalità diretto tra azione illecita ed effetti coercitivi, in questo caso appunto il cambiamento dell'esito delle elezioni. A tal riguardo, da un lato, si può sostenere che è opinione comune che l'intento russo era proprio quello di favorire l'elezione del presidente repubblicano[321] e, dall'altro lato, che anche in caso di effetti coercitivi indiretti è possibile in ogni caso applicare il principio del non intervento.

In merito a quest'ultimo punto, sebbene non vi sia concordia di opinioni, non ci sembra che si possa ammettere la tesi restrittiva per cui

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States (…)».

[321] Secondo il Report fornito dall'*intelligence* statunitense sull'interferenza de parte della Russia nel processo elettorale statunitense «[w]e assess with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election, the consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. When it appeared to Moscow that Secretary Clinton was likely to win the election, the Russian influence campaign then focused on undermining her expected presidency». Cfr. *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, 2017, p. 1; in dottrina su questo specifico tema si veda TRIFUNOSVSKA, *The Principle of Non-Interference and Cyber Operations*, in *Hungarian Yearbook of International Law and European Law*, 2017, p. 139.

solo nel caso di effetti coercitivi diretti si possa configurare una violazione del principio del non intervento. Prendiamo ad esempio il caso in cui uno Stato ottiene un accesso non autorizzato nel sistema governativo di un altro Paese per acquisire informazioni sensibili e, successivamente, decida di rendere pubbliche tali informazioni. L'obiettivo in questo caso è quello di generare una crisi interna che metta in dubbio le capacità dello Stato bersaglio circa le sue capacità di cyber defence. Lo Stato attore spera che il suo atteggiamento sia capace di indebolire, anche se temporaneamente, le difese informatiche dell'altro Stato affinché possa esercitare ulteriori attività di ingerenza al fine di sottrarre informazioni sensibili.

Ebbene, in questo caso, sposando la tesi restrittiva non vi sarebbe violazione del principio del non intervento in quanto l'operazione informatica non avrebbe obbligato direttamente il governo vittima a intraprendere particolari azioni (effetti diretti). Secondo un'altra prospettiva invece l'attacco costituirebbe un intervento illecito poiché il suo scopo era quello di indurre lo Stato bersaglio a prendere, anche se indirettamente, una decisione che altrimenti non avrebbe preso.

Su questi presupposti, anche laddove si volesse sostenere che l'operazione russa non abbia effettivamente condizionato l'esito finale delle elezioni statunitensi ciò sarebbe del tutto irrilevante.

L'illecito internazionale che viola il principio del non intervento, in definitiva, non richiede che l'operazione informatica abbia in concreto spiegato gli effetti diretti (in altre parole che abbia avuto un esisto positivo), ma è sufficiente che essa produca effetti coercitivi anche indiretti e riguardi uno di quegli aspetti rientranti nella sfera del dominio riservato dello Stato[322].

[322] SCHMITT, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, *op.cit.*, p. 52-53. A medesime conclusioni, anche se attraverso un ragionamento parzialmente diverso giungono anche altri Autori. Da una parte, infatti, vi è chi

5. Il problema dell'attribuzione allo Stato del fatto illecito compiuto da soggetti privati

Una volta delineati gli aspetti inerenti l'elemento oggettivo dell'illecito internazionale, che come detto un attacco informatico può certamente integrare, è necessario chiedersi se esso possa altresì essere attribuito ad uno Stato. In altre parole, dobbiamo chiederci se e in che modo un'azione condotta attraverso l'uso di strumenti informatici possa far sorgere una responsabilità internazionale in capo ad un determinato Stato. Prima di procedere all'analisi dei criteri di attribuzione più adatti al contesto delle operazioni informatiche, occorre però brevemente ripercorrere le tappe principali che hanno contribuito a delineare i principali criteri di imputazione.

---

ritiene che nello specifico caso della cyber interferenza nelle elezioni di un altro Stato a venire in rilievo è il principio del non intervento, ma attraverso l'ottica del principio di autodeterminazione dei popoli. A tal proposito, è stato sostenuto che « Where coercion as control can manifest itself more acutely is when a state's authority and will are manipulated at its source; in the process of their formation. To explain, when a state interferes in the electoral process, for example through disinformation or 'hack and leak' operations, it interferes with the structures but also with the environment that condition and facilitate the formation of authority and will by the people and substitutes the authentic process of self-determination with an artificially constructed process in order to generate particular attitudes and results aligned to the intervenor's will. In this case, the intervening state controls not only the peoples' cognitive environment within which authority and will are formed but also their choices. It also controls the authority and will of the government that emerges. Consequently, the right to self-determination as self-*governance* which is protected by the non-intervention principle is essentially curtailed» (cfr. TSAGOURIAS, *op.cit.*). D'altro canto, invece, vi è chi ha sostenuto una violazione del principio in esame rifacendosi ad una nozione di sovranità più ampia che ricomprenda anche la sfera di quello spazio virtuale definito come cyberspazio. A tal proposito, infatti, è stato sostenuto « (…) a cyber attack will constitute an unlawful intervention under customary international law where it can be regarded as the intentional application of coercion against a State in relation to a matter that it is freely entitled to determine. I submit that the cyber attacks against Estonia in 2007 provide a good example of cyber attacks amounting to an unlawful intervention. It is thus apparent that the principle of non-intervention represents a powerful (albeit often unrecognized) international legal tool that can be used by States in order to protect them from coercive cyber attacks. One final point is necessary». Cfr. BUNCHAN, *op.cit.*, p. 227.

Da un punto di vista generale, tra i differenti modi di far fronte alla problematica dell'attribuzione[323], possiamo distinguere, da un lato, il cd. 'approccio normativo' e, dall'altro, il cd. 'approccio fattuale'[324].

Il primo - condiviso dalla maggioranza della dottrina - affronta il problema ritenendo che, per poter attribuire una condotta ad uno Stato, è necessario aver riguardo all'esistenza di norme di diritto internazionale generale. In quest'ottica, così come per le altre norme generali, le vicende della prassi degli Stati non sarebbero solo un elemento da prendere in considerazione come parametro di confronto, piuttosto esse indicherebbero l'esistenza o meno di regole generali alle quali bisogna far capo per risolvere il problema dell'attribuzione[325].

L'approccio fattuale, invece, esclude che il problema dell'attribuzione possa essere ricondotto a una operazione normativa. Al contrario, si dovrà tener in considerazione l'esistenza effettiva di un collegamento tra l'individuo e lo Stato e, solo laddove vi sia un legame particolarmente stretto tra i due, la condotta dell'individuo potrà essere attribuita allo Stato stesso[326]. Per questo approccio quindi, ai fini dell'attribuzione, è di fondamentale importanza aver riguardo alle circostanze proprie di ciascun caso[327].

Senza dubbio, uno slancio verso l'inquadramento del problema in chiave normativa è stato effettuato dalla Commissione del diritto

---

[323] Si veda, tra gli altri: CONDORELLI, KRESS, *Part III The Sources of International Responsibility, Ch.18 The Rules of a Attribution: General Consideration* in CRAWFORD, PELLET, OLLESON (a cura di), *The Law Of International Responsibility*, Oxford, 2010; PALCHETTI, *L'Organo di fatto dello Stato nell'illecito internazionale*, Milano, 2007.

[324] PALCHETTI, *Op. cit.*, p. 12-18; ARANGIO-RUIZ, *State Fault and the Forms and Degrees of International Responsibility: Questions of Attribution and Relevance* in *Le droit international au service de la paix, de la justicia et du development, Mélanges Michel Virally, Paris,* 1991, p. *25; id., Second Report on State Responsibility, ILC Yearbook* 1989, Vol. II (1), pp. 48-53, par. 165-180.

[325] PALCHETTI, *op.cit.*, p. 17.

[326] PALCHETTI, op.*cit.*, p. 15-17.

[327] *Ibidem*, p. 19.

internazionale (d'ora in poi CDI), in particolare, con l'adozione nel 2001 del Progetto di Articoli sulla Responsabilità degli Stati (d'ora in poi Progetto).

Se da un lato, con riguardo ad alcune fattispecie si possa dire ormai pacifica l'attribuzione di condotte allo Stato[328] per altre, invece, vi sono ancora dei dubbi. In particolare, ci riferiamo all'ipotesi in cui ad agire sia un individuo o un gruppo di individui.

Nel Progetto, quest'ultima categoria viene disciplinata nell'art. 8: <<il comportamento di una persona o di un gruppo di persone sarà considerato un atto di uno Stato ai sensi del diritto internazionale se la persona o il gruppo di persone di fatto agiscono su istruzione, o sotto la direzione o il controllo di quello Stato nel porre in essere quel comportamento>>.

La versione definitiva della norma è stata frutto del lavoro svoltosi sia in seno alla stessa CDI che dalle Corti internazionali, durato più di un ventennio[329].

---

[328] La CDI in sede di commentario del suo Progetto, dopo aver precisato che un vincolo come quello della cittadinanza o il fatto di risiedere all'interno di quel determinato Stato non è sufficiente di per sé ai fini dell'attribuzione della condotta illecita, fa riferimento a quella che potremmo definire una 'regola generale'. All'art. 4 enuncia, infatti, la regola secondo cui: «il comportamento di un organo dello Stato sarà considerato come un atto dello Stato ai sensi del diritto internazionale, sia che tale organo eserciti funzioni legislative, esecutive, giudiziarie o altre, qualsiasi posizione abbia nell'organizzazione dello Stato e quale che sia la sua natura come organo del governo centrale o di un'unità territoriale dello Stato». Poi - al paragrafo 2 - prosegue: «un organo include qualsiasi persona o ente che rivesta tale posizione secondo il diritto interno dello Stato». Il termine 'organo' così come inteso dalla CDI, indica una categoria di individui che, in considerazione di un determinato collegamento con lo Stato, possono essere intesi come parte integrante dell'organizzazione dello stesso. Cfr. PALCHETTI, *Organi di fatto e illecito dello stato* in SPINEDI, GAINELLI, ALAIMO (a cura di), *La codificazione della responsabilità internazionale degli stati alla prova dei fatti, problemi e spunti di riflessione*, Milano, 2006, p. 8 ss.

[329] L'art. 8 del Progetto approvato in prima lettura nel 1980 specificava: «the conduct of a person or group of persons shall also be considered as an act of the State under international law if: a) it is established that such person or group of persons was in fact acting on behalf of that State; or b) such person or group of persons was in fact exercising elements of governmental authority in the absence of the official authorities and in circumstances which justified the exercise of those elements of authority». La norma includeva due differenti concetti: da un lato, quei soggetti o gruppi di soggetti che agiscono 'di fatto' per conto di uno

I principi su cui si fondava l'originario testo dell'art. 8 hanno trovato conferma nella storica sentenza *Nicaragua* della Corte internazionale di giustizia (d'ora in poi CIG). Nel caso di specie, com'è noto, la Corte ha affrontato il problema della possibile attribuzione agli Stati Uniti delle condotte poste in essere dai *Contras* e, proprio in relazione alle attività di questi ultimi, ha elaborato il cd. 'test del controllo effettivo': «*for this conduct* [quella posta in essere dai Contras] *to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed* [330]».

Stato e dall'altro, il *fonctionnaire de fait,* ossia quel soggetto che esercita funzioni governative in assenza di una «official authorities» e «i*n circumstances which justified the exercise of those elements of authority*» (cd. agente di necessità). Solo in seguito, con l'iniziativa del Relatore Speciale Crawford, vi è stata una differenziazione tra le due ipotesi che sono state ricomprese in due differenti articoli, rispettivamente l'art. 8 e l'art. 9 del Progetto. Cfr. *Report of the Commission on the work of its 32 session, in ILC Yearbook, 1980, vol II, Part two,* p. 30*;* DE FROUVILLE, *The Sources of International Responsibility, attribution of conduct to the State: Private Individuals* in CRAWFORD, PELLET, OLLESON (a cura di), *The Law Of International Responsibility*, Oxford, 2010.

[330] Corte Internazionale di Giustizia, sentenza del 17 giugno 1986, *Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua vs United States of America),* cit. par. 115. Secondo la Corte infatti: «(…)the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by contras in the course of their military or paramilitary operations in Nicaragua». Ancora «(…) even the general control by respondent State over a force with a high degree of dependency on it, would not in themselves mean, (…), that the United States directed or enforced the perpetration of act contrary to human rights and humanitarian law alleged by applicant State. (…)». In relazione alla scelta operata dalla Corte, rilevante risulta essere l'opinione separata del Giudice Ago. Da un lato, infatti, in merito al controllo effettivo la maggioranza dei Giudici della Corte ha adottato il "controllo effettivo", mentre l'opinione del Giudice Ago richiedeva «*nothing less than specific authorization of the wrongful conduct itself*». D'altro lato, invece, gli stessi erano d'accordo circa l'insufficienza di una situazione *generale* di dipendenza e supporto affinché fosse possibile attribuire le azioni dei Contrai agli Stati Uniti. A tal proposito si veda, J. CRAWFORD, *First report on State Responsibility, Addendum 5,* par. 200.

Sempre con riguardo alle condotte poste in essere da individui, ad una differente soluzione è giunto il Tribunale penale internazionale per la ex-Jugoslavia nel caso *Tadic*. In quella circostanza, la Camera d'appello del Tribunale ha elaborato il cd. 'test del controllo globale', giungendo a conclusioni parzialmente diverse rispetto alla Corte[331].

Il Tribunale ha analizzato il tipo di controllo che uno Stato deve attuare affinché la condotta di soggetti privati sia ad esso attribuibile, distinguendo tra l'ipotesi in cui ad agire siano individui 'non organizzati militarmente'[332] e l'ipotesi in cui i soggetti facciano parte di un gruppo 'organizzato e gerarchicamente strutturato'. In quest'ultima ipotesi, il Tribunale ha concluso ritenendo sufficiente dimostrare che lo Stato detenga 'il controllo generale sulle unità militari', non inserite nelle forze regolari, affinché si possa parlare di condotte a lui direttamente imputabili[333].

In definitiva, si è ritenuto che non sempre è necessario il medesimo grado di controllo per determinare se un gruppo di soggetti privati che,

[331] Il criterio fissato dalla Camera di Appello del Tribunale ha trovato conferma in sue successive pronunce. In particolare, i principi che determinerebbe l'attribuzione allo Stato di condotte che sono state soggette ad un suo controllo generale sono rintracciabili nei casi *Prosecutor v. Blaskic; Prosecutor v. Aleksovski, Prosecutor v. Delalic et al. (Celebici); Prosecutor v. Kordiac and Cerkez*. Per un approfondimento sul tema si veda, BARTOLINI, *Il concetto di controllo sulle attività di individui quale presupposto della responsabilità dello Stato* in SPINEDI, GAINELLI, ALAIMO (a cura di), *La codificazione della Responsabilità Internazionale degli Stati alla prova dei fatti. Problemi e spunti di riflessione*, Milano, 2006, p. 435 ss.

[332] Il Tribunale ha concluso che, per considerare gli individui come organi *de facto* dello Stato ed attribuirgli la responsabilità per le azioni commesse, è necessario che lo stesso fornisca delle specifiche istruzioni. Cfr. Tribunale penale internazionale per la ex-Jugoslavia, sentenza del 15 luglio 1999, the Prosecutor v. Tadic, Appeals Chambers, Judgment, cit. par. 118. Inoltre Tribunale Internazionale ha configurato un'altra possibilità ossia l'ipotesi che lo Stato faccia propri quei comportamenti, situazione questa disciplinata dall'art. 11 del Progetto della CDI.

[333] Tribunale Penale Internazionale per la ex-Jugoslavia, *cit.*, cit. par. 120;

alla stregua del diritto interno, non vengono configurati come organi dello Stato, possano essere ritenuti organi *de facto* dello Stato stesso[334].

Tale soluzione è stata fortemente criticata dalla CIG, nel 2007, nella controversia *Bosnia Erzegovina c. Serbia e Montenegro*[335]. In tale situazione la Corte, facendo leva sull'art. 8 del Progetto e sul cd. controllo effettivo, dapprima ha definito le argomentazioni a favore del controllo generale non persuasive[336]per poi, successivamente, distinguere le ipotesi degli organi di fatto da un lato, e la condotta di soggetti privati posta in essere sotto il 'controllo effettivo' o le specifiche istruzione dello Stato dall'altro[337].

---

[334] Invero, nel caso in cui si palesano tali circostanze, il Tribunale internazionale ha ritenuto che «under international law it is by no means necessary that the controlling authorities should plan all the operations of the units dependent on them, choose their targets, or give specific instructions concerning the conduct of military operations and any alleged violations of international humanitarian law. The control required by international law may be deemed to exist when a State (or, in the context of an armed conflict, the Party to the conflict) has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group. Acts performed by the group or members thereof may be regarded as acts of de facto State organs regardless of any specific instruction by the controlling State concerning the commission of each of those acts». Cfr. Tribunale Penale Internazionale per la ex-Jugoslavia, *cit*., par. 137.

[335] Per una analisi approfondita del problema si vedano, tra gli altri: CANNIZZARO, *Metodi di Soluzione di Conflitti fra Giurisdizioni Internazionali: il Contributo della Sentenza della CIG sul caso del Genocidio (Bosnia Erzegovina c. Serbia e Montenegro)"* in *European Journal of Legal Studies*, 2007*;* FRULLI, *Un passo avanti e due indietro: responsabilità individuale e responsabilità statale nella sentenza della Corte Internazionale di Giustizia nel caso Bosnia-Erzegovina c. Serbia* in *Diritti Umani e diritto internazionale*, 2007, pp. 579-593.

[336] La Corte ha affermato: «this is the case of the doctrine laid down in the Tadic Judgment. Insofar as the "overall control" test is employed to determine whether or not an armed conflict is international, which was the sole question which the Appeals Chamber was called upon to decide (…) the ICTY presented the "overall control" test as equally applicable under the law of State responsibility for the purpose of determining when a State is responsible for acts committed by paramilitary units, armed forces which are not among its official organ». Cfr. Corte internazionale di giustizia, sentenza del 26 febbraio 2007, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia Erzegovina v Serbia and Montenegro)*, Judgment, cit. par. 404.

[337] *Ibidem*, par. 397. Invero la Corte ha distinto le due ipotesi così delineate riconducendo l'ipotesi dell'organo di fatto, all'interno dell'art. 4 del *Progetto* mentre, l'ipotesi del "controllo effettivo" all'interno dell'art. 8. In dottrina, vi è stato chi ha criticato questo approccio ritenendo che la Corte abbia mescolato due distinte ipotesi di attribuzione, la prima basata sull'esistenza

La breve ricostruzione così effettuata mostra quindi come la chiave normativa, attraverso la creazione di 'regole giuridiche' generali, sia la strada maggiormente percorsa per far fronte al problema dell'attribuzione.

5.1. La possibile attribuzione ad uno Stato di un attacco informatico

Uno dei problemi più rilevanti e controversi circa il rapporto tra norme di diritto internazionale e attacchi informatici è senza dubbio quello relativo ai criteri di attribuzione da utilizzare allorquando una operazione informatica integra l'elemento oggettivo dell'illecito internazionale e si ritenga essere attribuibile ad uno Stato. A tal proposito basti pensare che alla fine del 2018, il Segretario della sicurezza interna statunitense ha affermato che ad oggi gli attacchi informatici pongono dei rischi maggiori rispetto agli attacchi tradizionali[338]. Senza voler sindacare la veridicità o meno di questa affermazione, quello che essa mette in luce è senz'altro le difficoltà sia tecniche che giuridiche nell'attribuzione di una condotta informatica allo Stato[339]. Il processo di attribuzione può dunque muoversi su due differenti, ma interconnessi piani: quello tecnico e quello giuridico.

Da un punto di vista tecnico, sebbene non sia questa la sede per parlarne in modo diffuso, è necessaria solo qualche considerazione di carattere generale. Invero, se da un lato non è difficile rilevare che l'individuazione del soggetto che materialmente compie l'attacco informatico è un'operazione complessa, dall'altro è possibile constatare che lo sviluppo tecnologico ha certamente facilitato il processo tecnico attraverso cui

di un collegamento legale o istituzionale e la seconda, invece, basata su di un collegamento fattuale. Si veda DE FROUVILLE, *Op.Cit.*, p. 269.

[338] Cfr. NIELSEN, *Rethinking Homeland Security in an Age of Distruption*, U.S. Department of Homeland Security, 5 settembre 2018.

[339] FINALY, PAYNE, *The Attribution Problem and Cyber Armed Attacks*, in *American Journal of International Law Unbound*, 2019, p. 202.

risalire quantomeno al computer dal quale l'attacco è stato sferrato. Si può affermare infatti che la maggior parte degli Stati tecnologicamente sviluppati è ormai capace di individuare territorialmente la macchina fisica dalla quale l'operazione informatica è partita[340].

Se ciò è vero, è altrettanto vero che non sempre – anzi quasi mai – il mondo del diritto riesce a stare al passo con lo sviluppo tecnologico e a questa diacronia non fa eccezione il diritto internazionale. Bisogna quindi chiedersi se gli istituti giuridici, anche precedenti, possano essere utilizzati per affrontare le nuove sfide poste dalla tecnologia oppure se è necessaria l'individuazione di nuovi istituti.

Come visto, la questione relativa all'attribuzione di un comportamento illecito ad uno Stato è particolarmente complessa, soprattutto in relazione a quelle condotte che vengono poste in essere da soggetti che non rientrano nella struttura organizzativa dello Stato.

Queste difficoltà vengono incrementate allorché ci si confronta con un contesto, quello del cyberspazio, che si caratterizza per la presenza di

[340] A tal proposito è stato sostenuto, infatti, che « DOJ can draw on its institutional expertise to attribute hacks. The FBI has invested heavily in malware technical analysis capabilities. The FBI also hosts the National Cyber Investigative Joint Task Force, through which nineteen federal agencies coordinate cyber threat investigations. According to former National Security Agency General Counsel Stewart Baker, the view that hackers can operate with complete anonymity is antiquated: "[W]e can know who our attackers are (…)The massive amount of data available online makes the job of attackers easier, but it can also help the defenders if we use it to find and punish our attackers."These attribution efforts ensure that we have as complete a picture as possible of who cyber threat actors are and how particular actors conduct malicious cyber activity. For example, a key way the FBI attributed the Sony hack to North Korea was by comparing the malware used in that hack to malware used in other North Korea– sponsored cyber intrusions» (cfr. CARLIN, *Detect, Distrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, in *Harvard National Security Journal*, 2016, p. 416. Più in generale sulle questioni tecniche che attengono l'attribuzione degli attacchi informatici si rimanda a LIN, *Attribution of Malicious Cyber Incidents:From Soup to Nuts*, in *Journal of International Affairs*, 2017, p. 82-83. Secondo l'Autore è possibile individuare tre diversi *step* per l'attribuzione: il primo che fa capo all'individuazione della macchina, la seconda che mira invece all'individuazione del soggetto specifico che ha compiuto l'attacco e infine l'attribuzione al responsabile in ultimo individuato.

differenti aspetti. Si possono individuare, infatti, almeno tre elementi che contraddistinguono questo nuovo dominio: in primo luogo, l'anonimato inteso come possibilità da parte di chi effettua materialmente un attacco di poter nascondere o mascherare la propria identità[341]; in secondo luogo, la possibilità di compiere gli attacchi utilizzando un elevato numero di computer, precedentemente infettati, che trovandosi su territori diversi rendono più difficile l'individuazione dell' origine stessa dell'attacco (*multi-stage cyber attacks*)[342]; e, infine, la rapidità intesa come quella caratteristica temporale che permette il materializzarsi dell'attacco in tempi decisamente più brevi rispetto agli attacchi tradizionali[343] e, contestualmente, una maggiore quantità di tempo per rilevare e valutare l'attacco informatico rispetto a quello tradizionale[344].

Va da sé che gli aspetti problematici dell'attribuzione non riguardino quei casi, invero difficilmente verificatesi, in cui a compiere un attacco informatico sia un vero e proprio organo dello Stato. In queste circostanze non vi sarebbero dubbi circa l'applicazione per analogia dell'art. 4 del Progetto.

È nostra intenzione invece concentrarci esclusivamente sulle ipotesi che riguardano l'attribuzione allo Stato di un attacco informatico posto in essere da attori non statali, e quindi da un soggetto (o un gruppo) privato che non rientrano nella struttura organizzativa dello Stato.

---

[341] TSAGOURIAS, *Cyber attacks, Self-Defense and the problem of attribution* in *Journal of Conflict and Security Law*, 2012, p. 233 ss.

[342] *Ibidem*, p. 233; Tale circostanza è quella che si verifica quando siamo dinanzi all'ipotesi di un attacco informatico di tipo DDos. Ipotesi quest'ultima verificatasi nel caso dell'attacco in Estonia nel 2007.

[343] *Ibidem*, p. 233.

[344] FINALY, PAYNE, *op.cit.*, p. 203.

5.2. *Segue:*

L'attribuzione di una condotta ad un soggetto privato è stata, come visto, affrontata dapprima dalla giurisprudenza internazionale e successivamente dal Progetto. In particolare, sono due i criteri di imputazione individuati, e cioè quello del controllo globale e quello del controllo effettivo, quest'ultimo poi è stato utilizzato anche dalla Commissione del diritto internazionale.

Prima di prendere in esame l'art. 8 del Progetto è necessario qualche chiarimento circa l'utilizzo del criterio di imputazione del controllo globale. Non sono mancati infatti autori che, in virtù delle oggettive difficoltà di carattere tecnico prima ancora che di diritto, concernenti la individuazione concreta di chi pone in essere l'attacco, hanno definito il criterio suindicato come il più appropriato per determinare l'attribuzione allo Stato della condotta posta in essere dai soggetti privati[345]. A noi sembra, invero, che tale criterio di attribuzione non sia pienamente adeguato. In primo luogo, nel già richiamato caso *Tadic*, si è specificato che il criterio in parola è utilizzabile solo laddove vengano in rilievo dei 'gruppi armati gerarchicamente organizzati'; inoltre, è dubbia la corrispondenza di tale criterio al diritto consuetudinario[346].

Ora, se da un lato una differenziazione rispetto al grado di controllo che lo Stato deve attuare affinché le condotte siano a lui direttamente imputabili possa ritenersi una soluzione condivisibile, d'altro canto, nel nostro caso, la totale o comunque scarsa diffusione di gruppi di *hackers*

[345] SHACKELFORD, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem* in *Georgetown Journal of International Law*, 2011, p. 206.

[346] Nel commento all'art. 8 del Progetto, la CDI esclude l'utilizzabilità del criterio del cd. controllo globale alle ipotesi di responsabilità degli Stati, ritenendolo piuttosto adeguato nel solo ambito del diritto internazionale penale. Cfr. Commentary to art. 8, par. 5; Corte internazionale di giustizia, *cit.*

con una struttura organizzativa ben delineata sia dal punto di vista gerarchico che funzionale[347] ne renderebbe difficile l'applicazione al caso concreto.

Esclusa quindi questa ipotesi dobbiamo chiederci se il criterio del controllo effettivo, più nello specifico la sua previsione all'interno dell'art. 8 del Progetto, può invece avere una qualche utilità.

Com'è noto l'art. 8 del Progetto di articoli sulla responsabilità degli Stati stabilisce che «[i]l comportamento di una persona o di un gruppo di persone sarà considerato un atto di uno Stato ai sensi del diritto internazionale se la persona o il gruppo di persone di fatto agiscono su istruzione, o sotto la direzione o il controllo di quello Stato nel porre in essere quel comportamento»[348].

Come si può notare la lettera dell'articolo prende in considerazione tre differenti categorie che, sebbene in dottrina e secondo lo stesso commentario al Progetto sono spesso usati come sinonimi[349], stanno ad indicare tre situazioni tra parzialmente differenti[350]. È possibile delineare

[347] ROSCINI, *Cyber Operations: Identifying the Problem and the Applicable Law* in *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, p. 38.

[348] Cfr. *Progetto di Articoli sulla responsabilità degli Stati*, art. 8.

[349] Invero, l'idea di ritenere i tre termini utilizzabili in modo interscambiabile è prassi abbastanza comune in dottrina. Ciò si deve soprattutto all'impostazione seguita da Crawford e ai suoi studi. Secondo altri invece la *direzione* e il *controllo* sarebbero, piuttosto che sinonimi, termini volti ad indicare il medesimo criterio di attribuzione (cfr. TONKIN, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge University Press, 2011, p. 58-59. Altri invece muovono dall'idea che i termini *istruzione* e *direzione* sono caratterizzati da una natura specifica, secondo cui «the issuance of instructions or the fact of directing persons or groups of persons to do something involves ordering or commanding those persons to undertake a certain conduct». Invece, il criterio del *controllo* sarebbe qualificato come «rather loose», giustificando così una stratificazione del grado di controllo che uno Stato deve avere per poter essere ritenuto responsabile (cfr. CASSESE, *The Nicaragua and Tadic´ Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, in *European Journal of International Law*, 2011, p. 663.

[350] MACAK, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict and Security Law*, 2016, 408 ss.

il modo in cui le tre ipotesi vengono in rilievo e si articolano l'una rispetto all'altra.

In primo luogo, sia il criterio della direzione che quello del controllo sono entrambi caratterizzati dall'esistenza di una costante relazione tra lo Stato e il soggetto privato. Di contro, il criterio dell'istruzione permetterebbe di stabilire la responsabilità dello Stato anche sulla base di un rapporto meno stringente con il privato e cioè attraverso una specifica e singola istruzione data a quest'ultimo per compiere l'illecito internazionale. In secondo luogo la relazione che si concretizza attraverso il 'controllo' si caratterizza per una maggiore e più alta prossimità tra l'agente e lo Stato, così come indicato dalla giurisprudenza internazionale. Infine, tutte e tre le ipotesi sono accomunate dalla medesima base concettuale, vale a dire l'esistenza di una relazione di *subordinazione* tra lo Stato e il privato[351]. Ciò significa che qualsiasi forma orizzontale di collusione come addestramento e supporto non è sufficiente per nessuno degli standard previsto dall'art. 8[352].

Ciò detto, è innegabile che quanto previsto dall'art. 8 sia particolarmente complesso nell'ambito del cyberspazio, invero riuscire a

[351] *Ibidem,* p. 427.

[352] Significativa in tal senso è la sentenza della Corte internazionale di Giustizia in merito al caso riguardante le *attività armate nel territorio del Congo,* ove la Corte ha affermato «that there is no credible evidence to suggest that Uganda created the MLC. Uganda has acknowledged giving training and military support and there is evidence to that effect. The Court has not received probative evidence that Uganda controlled, or could control, the manner in which Mr. Bemba put such assistance to use. In the view of the Court, the conduct of the MLC was not that of "an organ" of Uganda (Article 4, International Law Commission Draft Articles on Responsibility of States for internationally wrongful acts, 2001), nor that of an entity exercising elements of governmental authority on its behalf (Art. 5). The Court has considered whether the MLC's conduct was "on the instructions of, or under the direction or control of" Uganda (Art. 8) and finds that there is no probative evidence by reference to which it has been persuaded that this was the case. Accordingly, no issue arises in the present case as to whether the requisite tests are met for sufficiency of control of paramilitaries». Cfr. ICJ, *Case Concerning Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), 19 dicembre 2005, par. 160.

provare che un privato abbia agito dietro una specifica istruzione, il controllo o la direzione di uno Stato non è di semplice risoluzione. È certo tuttavia che tra le tre ipotesi quella che potrebbe risultare maggiormente espressiva del contesto informatico sia quella che fa capo all'ipotesi dell'istruzione. Ciononostante, a noi pare che il problema possa essere in qualche modo affrontato e parzialmente risolto solo se ci si pone sul piano degli aspetti probatori. Bisogna capire quale *standard* probatorio sia necessario affinché una condotta informatica possa essere attribuita e ricondotta ad uno Stato. A tal fine nei prossimi paragrafi ci occuperemo dapprima dell'onere probatorio, ci chiederemo se nel caso di attacchi informatici è necessario una inversione dell'onere, e successivamente ci soffermeremo più nel dettaglio sullo *standard* probatorio richiesto.

5.2.1. L' (inversione dell') onere della prova

Il problema dell'individuazione degli elementi probatori necessari affinché una condotta possa essere attribuita ad uno Stato è ricorrente nella giurisprudenza internazionale. Nel caso *Nicaragua*, ad esempio, la Corte internazionale di giustizia (d'ora in poi CIG) osservò che ad assumere importanza «(…) is (…) not the legal process of imputing the act to a particular State for the purpose to establishing responsibility, but the prior process of tracing material proof of the identity of perpetrator»[353]. Non molto diversamente, secondo il Tribunale dei Reclami Iran-Stati Uniti, «[i]n order to attribute an act to the State, it is necessary to identify with reasonable certainty the actors and their association with the State»[354].

[353] Corte internazionale di giustizia, sentenza del 17 giugno 1986, *Case concerning* military *and paramilitary activities in and against Nicaragua* (Nicaragua v. United States of America).
[354] Tribunale dei Reclami Iran-Stati Uniti, *Yeager c. Repubblica islamica dell'Iran*, 1987.

Queste considerazioni ci sembrano senz'altro applicabili al contesto degli attacchi informatici, con la dovuta precisazione che, in questo ambito, occorre tener conto dell'architettura stessa che permette di compiere una tale tipologia di attacco; in altre parole, di quelle caratteristiche di 'natura tecnica'[355] che permettono, ancora prima di attribuire una condotta ad uno Stato, di determinarne l'autore.

Prima di analizzare la problematica relativa al *quantum* della prova, è necessario tuttavia chiedersi quale sia lo Stato in capo al quale incombe l'onere probatorio.

Da un punto di vista generale, la regola secondo cui *onus probandi incumbit actori*, a dispetto dei suoi diversi approcci e dai diversi gradi della sua applicazione, è stata utilizzata da molteplici tribunali internazionali[356], potendosi ritenere una regola generale del processo internazionale.

Tuttavia, com'è noto, nell'ambito del processo internazionale l'individuazione delle parti e la distinzione tra attore e convenuto non sempre è agevole[357]. Se invero nell'ambito della teoria generale del processo la contrapposizione è particolarmente pregnante, soprattutto con riguardo all'onere della prova, determinando così un vantaggio nei confronti del convenuto, qualora l'attore fornisse una insufficiente ovvero una parziale dimostrazione dei fatti[358]; in ambito internazionale questa distinzione non solo non è sempre chiara (si pensi ad esempio all'ipotesi

[355] Per un approfondimento, si veda ROWE, *The Attribution of Cyber Warfare,* in GREEN (a cura di), *Cyber Warfare: A multidisciplinary Analysis,* Londra, 2015, p. 61-73.

[356] RIDDELL, *Evidence, fact-finding, and experts*, in ROMANO, ALTER e SHANY (a cura di), *The Oxford Handbook of International Adjudication*, Oxford, 2013, p. 858.

[357] Cfr. BRAVO, *La prova nel processo internazionale*, Napoli, 1958, p. 96 ss.

[358] *Ibidem*, p. 97.

in cui gli Stati stipulino uno *special agreement*), ma spesso non risulta nemmeno decisiva[359].

Ebbene, il principio in esame può ritenersi applicabile non solo allo Stato (attore) ma più in generale alla parte che affermi l'esistenza o il verificarsi di quel determinato fatto[360].

Allo stesso tempo non può escludersi che tale regola conosca delle eccezioni, con conseguente inversione dell'onere della prova. Ci si chiede allora se tale ultima ipotesi possa essere giustificata nell'ambito delle operazioni informatiche. In altre parole, se sia lo Stato accusato di aver perpetrato un attacco informatico ad essere investito dell'obbligo di dimostrare la propria estraneità ai fatti o se invece l'onere spetti allo Stato che abbia subito l'attacco.

In dottrina non sono mancate ipotesi che hanno suggerito tale inversione dell'onere probatorio. Tali teorie ci sembrano riconducibili a due differenti filoni: il primo basato sull'introduzione di un diverso criterio di attribuzione, dal quale ne discende, come corollario, un onere della prova in capo allo Stato dal quale è partito l'attacco[361]; e un secondo più generale basato sull'applicazione dell'obbligo di *due diligence* al cyberspazio[362].

Il primo orientamento dottrinale muove dalla constatazione che le peculiarità degli attacchi informatici determinerebbero l'esistenza di una

[359] WOLFRUM, MOLDNER, *International Courts and Tribunals, Evidence*, in WOLFRUM (a cura di), *Max Planck Encyclopedia of Public International Law*, 2013, para. 70-74

[360] In questo senso si veda, Corte internazionale di giustizia, sentenza del 20 aprile 2010, *Case concerning pulp mills on the river Uruguay* (Argentina v. Uruguay), secondo cui: «the Court considers that, in accordance with the well-established principle of onus probandi incumbit actori, it is the duty of the party which asserts certain facts to establish the existence of such facts».

[361] MARGULIES, *Sovereignty and Cyber Attack: Technology's Challenge to the Law of State Responsibility*, in *Melbourne Journal of International Law*, 2013, p. 4

[362] ZIOLKOWSKI, *General principles of international law as applicable in cyberspace*, in *op. cit.*, p. 169-170

attribution asymmetry[363]. Per far fronte a questa asimmetria è stata suggerita l'applicazione di un ulteriore criterio di imputazione, diverso dai criteri classici, che meglio risponderebbe alle esigenze del cd. *cyber domain*[364], vale a dire il cd. 'controllo virtuale'.

Secondo l'autore (Margulies) agisce in controllo virtuale lo Stato che finanzi ovvero equipaggi un individuo o un gruppo di individui con uno specifico *software* informatico che successivamente, senza ricevere istruzioni dallo Stato 'controllante', ponga in essere un attacco informatico[365].

Lo Stato vittima di tale attacco, una volta appurato che l'azione è riconducibile a un individuo (o gruppo di individui) soggetto al controllo virtuale di un altro Stato, potrà chiedere a quest'ultimo informazioni sull'attacco[366].

Lo Stato che esercita il controllo virtuale, a questo punto, potrà decidere di fornire le informazioni richieste, dimostrando *a)* la propria estraneità rispetto alle attività poste in essere dai soggetti privati; ovvero *b)* l'incapacità di controllare le azioni del soggetto o gruppo di soggetti che ha compiuto l'attacco. In alternativa, lo Stato potrà rifiutarsi di fornire tali informazioni. In tal caso, esso sarà ritenuto direttamente responsabile per l'attacco informatico, con la conseguenza che lo Stato vittima potrà reagire attraverso l'adozione di contromisure[367]. In altri termini, il criterio in esame si traduce in un'inversione dell'onere della prova a carico dello Stato in controllo virtuale. Su di esso, infatti, graverebbe una presunzione di responsabilità superabile soltanto attraverso la prova dell'assenza di

[363] MARGULIES, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State* Responsibility, in *Melbourne Journal of International Law*, 2015, p.4

[364] *Ibidem*.

[365] *Ibidem*, p. 5.

[366] *Ibidem*, p. 19.

[367] *Ibidem*, p. 19-21; GILL, DUCHEINE, *Anticipatory Self-Defense in the Cyber Context*, in *International Law Studies*, 2013, p. 452-458.

coinvolgimento o dell'incapacità di controllare le azioni dell'individuo (o del gruppo di individui) autore dell'attacco informatico.

Il secondo orientamento ha fatto leva – più in generale – sull'esistenza di un obbligo di *due diligence* per lo Stato, il quale sarebbe tenuto ad adottare tutte le misure di sicurezza nazionale per evitare, ancor prima che si verifichi un attacco, che le proprie infrastrutture cibernetiche possano non solo essere danneggiate, ma anche utilizzate per sferrare un attacco nei confronti di un terzo Stato[368]. È facile vedere come questa proposta si traduca, in ultima analisi, in un'inversione dell'onere della prova: sarà infatti lo Stato da cui è partito l'attacco a dover dimostrare di aver assunto tutte le misure (preventive) necessarie[369].

Così brevemente delineati gli estremi del problema, va sottolineato che, nonostante le peculiarità tecniche degli attacchi informatici, un'inversione dell'onere della prova non appare giustificabile. Anzitutto, com'è noto, anche laddove lo Stato sia a conoscenza delle condotte (in questo caso di tipo informatico) perpetrate, esso non può ritenersi direttamente responsabile per la condotta medesima[370]. In questo caso si determinerà una violazione dell'obbligo di *due diligence*, ma non ci sembra che questa violazione comporti di *per sé* una responsabilità dello Stato per ogni azione informatica illecita commessa sul proprio territorio, né tantomeno l'onere di provare l'adozione di tutte le misure necessarie per evitarlo.

Ma vi è di più. A ben vedere, una costante giurisprudenza della CIG, inaugurata dal noto caso del *Canale di Corfù*, stabilisce che, sebbene uno

---

[368] ZIOLKOWSKI, *General Principles of International Law as Applicable in Cyberspace, op. cit.*, p. 169-170

[369] In una prospettiva analoga si è suggerito di risolvere i problemi posti dall'attribuzione di un attacco informatico attraverso un rovesciamento dell'onere della prova «*from the investigator and accuser to the nation in which the attack software was launched*». In questo senso si veda, CLARKE, KNAKE, *Cyber War: The Next Threat to National Security and What to Do About It*, New York, 2010, p. 249.

[370] ROSCINI, *op. cit.*, p. 245

Stato eserciti un controllo effettivo sul proprio territorio, ciò «*neither involves prima facie responsibility nor shifts the burden of proof*»[371]. Il principio stabilito dalla Corte ci sembra ancora più incisivo nell'ambito degli attacchi informatici. E infatti, prendendo in considerazione la struttura di internet, che si caratterizza per essere un sistema decentralizzato dove le comunicazioni avvengono attraverso 'pacchetti di dati' che viaggiano tra differenti computer e che generalmente ogni computer è identificato da un Indirizzo IP, il problema sorge in virtù della possibilità di mascherare ovvero occultare la propria identità (ad esempio attraverso l'utilizzo dei cd. *proxy*), con la conseguenza che l'origine dell'attacco potrebbe solo apparentemente provenire da quel territorio dello Stato. Ad esempio nel noto caso *Stuxnet* alcuni dati provenivano da server situati in Danimarca e in Malesia[372]. Dunque, qualora si applicasse tale inversione probatoria ne discenderebbe l'erroneo coinvolgimento di Stati del tutto estranei e (probabilmente) innocenti, che solo apparentemente avrebbero preso parte all'operazione informatica in quanto 'territorialmente coinvolti' nell'attacco[373].

5.2.2. Standard di prova: il caso delle elezioni statunitensi del 2016 e l'affare *Stuxnet*

[371] Corte internazionale di giustizia, sentenza del 9 aprile 1949, *The Corfù Channel Case* (United Kingdom v. Albania). Va tuttavia precisato come in virtù di tale controllo sul territorio, e la conseguente difficoltà per lo Stato di reperire prove dirette e valide a provare la responsabilità dello Stato, la Corte ammetta il ricorso a deduzione e a prove indirette. Questo aspetto verrà approfondito al paragrafo 4.

[372] FAILLIERE, MURCHU, CHIEN, *W32. Stuxnet Dossier*, Symantec Publication, 2012, p. 21.

[373] Nel medesimo senso si veda, ROSCINI, *op. cit.*, p. 248; GEIß, LAHMANN, *Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention*, in ZIOLKOWSKI (a cura di), *Peacetime Rigime for State Acrivities in Cyberspace*, Tallin, 2013, p. 628. Si veda anche Manuale di Tallin, *Rule 7 e Rule 8.* In senso contrario, CLARKE, KNAKE, *op. cit*., p. 249.

Sebbene il problema dell'individuazione dell'autore materiale di una condotta sia anzitutto una questione fattuale, non può prescindersi dalla sua dimensione giuridica[374], e cioè dall'esigenza di determinare lo standard di prova necessario affinché la condotta in questione possa essere attribuita ad un certo soggetto. Si tratta di una esigenza che viene in rilievo anche in presenza di un attacco informatico e che richiede anzitutto di individuare i diversi *standard* di prova generalmente utilizzabili a livello internazionale, standard che solo in parte risultano modellati su quelli adottati a livello interno, in particolare nei paesi di *common law*. Se infatti negli ordinamenti di *civil law*, con riferimento alle controversie civilistiche, non è previsto uno specifico standard di prova, ma il giudice ha la possibilità di volta in volta di valutare le prove secondo un proprio personale convincimento[375], con l'obbligo di motivare il ragionamento logico-giuridico che lo ha condotto a quel giudizio, i sistemi di *common law* prevedono generalmente criteri prestabiliti. Si tratta soprattutto del criterio noto come *preponderance of evidence* (o anche *balance of probabilities*)[376], tipicamente utilizzato in ambito civilistico e secondo il quale un fatto può dirsi provato quando le prove addotte forniscano, rispetto a quelle fornite della controparte, un convincimento maggiore[377]; e il *beyond reasonable doubt standard*, utilizzato soprattutto per i procedimenti di tipo penalistico[378].

[374] GEIß, LAHMANN, *Freedom and Security in Cyberspace: Non-Forcible Countermeasures and Collective Threat-Prevention, op. cit*., p. 623.

[375] RIDDELL, *op. cit.* p. 860.

[376] *Ibidem*

[377] *Ibidem*.

[378] Invero, il principio secondo cui il fatto debba essere provato 'al di là di ogni ragionevole dubbio' in ambito penalistico è stato utilizzato anche in ordinamenti di *civil law*, si pensi appunto a quello italiano, soprattutto con riguardo al nesso di causalità. Cfr. *ex multis*, Cassazione penale, Sezioni unite, sentenza dell'11 settembre 2002 n° 30328 (Sentenza Franzese).

Ebbene, nel diritto internazionale, pur non essendovi norme di carattere generale che determinano uniformemente il *quantum* probatorio necessario per affermare la responsabilità di uno Stato[379], non solo *standard* probatori vengono costantemente utilizzati a livello giudiziale[380], ma sono suscettibili anche di essere classificati per lo meno secondo quattro modelli[381]:

a) il cd. *prima facie* rappresenta lo standard meno stringente essendo sufficiente che la prova fornita sia solo indicativa dell'esistenza di quel determinato fatto; *b)* il già richiamato standard del cd. *preponderance of evidence*, che secondo alcuni sarebbe il più appropriato da utilizzare nell'ambito delle controversie inter-statali[382]; *c)* lo standard del cd. *beyond reasonable doubt*, anch'esso mutuato dai sistemi di *common law*, e sovente utilizzato, date le conseguenze derivanti dalla decisione, in ambito penale internazionale. Lo stesso Statuto di Roma stabilisce infatti che *«in order to convict the accused, the Court must be convinced of the guilt of the accused beyond reasonable doubt*»[383]; *d)* infine, lo standard definito

[379] GREEN, *Fluctuating Evidentiary Standards for Selfe-Defence in the Inernational Court of Justice*, in *International and comparative Law Quarterly*, 2009, p. 165

[380] Corte internazionale di giustizia (CIG), sentenza del 27 giugno 1985, *Case concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. USA); CIG, sentenza del 9 aprile 1949, *The Corfù Channel Case* (United Kingdom v. Albania); CIG, sentenza del 6 novembre 2003, *Case concerning Oil Platform* (Iran v. USA); CIG, sentenza del 19 dicembre 2005, *Case concerning Armed Activities on the Territory of the Congo* (Democratic Republic of Congo v. Uganda).

[381] A questi va aggiunto il *fully conclusive* standard menzionato dalla Corte internazionale di giustizia nel caso dello *Stretto di Corfù* e richiamato da ultimo nelle decisioni sul *Bosnian Genocide* e *Crotian Genocide*. Cfr. Corte internazionale di giustizia, sentenza del 26 febbraio 2007, *Case concerning application of the convention on the prevention and punishment of the crime of genocide* (Bosnia and Herzegovina v. Serbia and Montenegro); Corte internazionale di giustizia, sentenza del 3 febbraio 2015, *Application of the convention on prevention and punishment of the crime of genocide* (Croatia v. Serbia); per i recenti sviluppi della Corte internazionale di giustizia in materia di standard di prova nei crimini di genocidio si veda TZENG, *Proving Genocide: The High Standards of the Inernational Court of Justice*, in *Yale Journal of International Law*, 2015, p. 419-425.

[382] WOLFRUM, *op. cit*., para. 77.

[383] Rome Statute of International Criminal Court, 1998, art. 66;

clear and convincing[384], che si colloca a metà strada tra quelli 'meno stringenti' (*prima facie* e *preponderance of evidence*) e quello previsto dallo Statuto della Corte penale internazionale. Affinché si possa ritenere raggiunto tale *quantum* probatorio è necessario convincere «*the aribiter (…) that it is substantially more likely than not that the factual claims that have been made true*»*[385]*. Quest'ultimo standard è stato utilizzato in diverse pronunce internazionali (soprattutto in materia di legittima difesa)[386], e a dispetto dello standard del *preponderance of evidence*, si rivela particolarmente adeguato laddove vengano in rilievo questioni attinenti alla responsabilità internazionale dello Stato[387].

Una volta delineati i modelli di standard probatorio astrattamente utilizzabili, occorre ora stabilire quale tra questi risulti il più adeguato rispetto al contesto degli attacchi informatici. E, successivamente, se la specificità del contesto informatico di *per sé* giustifichi l'utilizzo di uno standard probatorio meno stringente.

Esclusa l'applicabilità dei due criteri diametralmente opposti (*prima facie* e *beyond resonable doubt* standard), in quanto con l'utilizzo del primo vi sarebbe un'alta possibilità di incorrere in errate o false attribuzioni, mentre invece con il secondo sarebbe richiesto uno standard di prova oggettivamente irraggiungibile[388] (per il contesto degli attacchi informatici), non ci resta che prendere in esame i due criteri residuali.

---

[384] GREEN, *op. cit*., p. 167

[385] *Ibidem*.

[386] Nel caso *The Trail Smelter Arbitration Case* (Stati Uniti c. Canada) del 1905, il Tribunale arbitrale ha affermato «*no State has the right to use or permit the use of its territory in a manner as to cause injury (…) to the territory of another, when the case is of serious consequence ant the injury is established by clear and convincing evidence*»; in modo simile si veda, Inter-American Court of human rights, sentenza del 29 luglio 1988, *Velasquez Rodriguez Case*.

[387] ROSCINI, *op. cit*., p. 249; a favore dell'utilizzo di tale criterio si veda, tra gli altri, O' CONNELL, *Evidence of Terror*, in *Journal of Conflict and Security Law*, 2002, p. 22-28; id, *Rules of Evidence for the Use of Force in International Law's New Era*, in *Scholarly Works*, 2006, p. 45; GREEN, *op. cit.*, p. 167.

[388] ROSCINI, *op. cit*., p. 252.

Se da un lato è condivisibile quanto affermato dalla CIG, secondo cui non dovrebbe essere richiesto uno standard probatorio così rigoroso da rendere la prova indebitamente stringente[389], dall'altro lato non appare giustificabile l'adozione di uno standard più elastico, come il *preponderance of evidence*, solo a causa delle difficoltà tecniche che caratterizzano gli attacchi informatici. Infatti l'adozione di un determinato standard non è previsto per favorire o meno il suo raggiungimento, ma piuttosto per salvaguardare la controparte da false attribuzioni.

Tuttavia, data la mancanza di decisioni da parte di tribunali internazionali relative allo specifico argomento degli attacchi informatici, occorre stabilire se vi sono indicazioni nella prassi degli Stati che depongono nel senso di adottare uno standard più rigoroso come quello di una prova che sia *clear and convincing.*

Invero, diversi paesi sembrano procedere proprio in questa direzione. Se si guarda all'Italia, ad esempio, il Comitato Parlamentare per la sicurezza della Repubblica ritiene necessario dimostrare «in modo inequivocabile che l'attacco sia originato in un Paese sovrano e che sia stato ordinato da strutture governative e non da gruppi di hacker»[390] richiedendo a tal fine delle «prove informatiche inconfutabili»[391]. Allo stesso tempo, il Comitato Parlamentare riconosce la difficoltà nel soddisfare tale condizione, sostenendo la possibilità dell'esistenza di tracce digitali su server dislocati in diversi Stati.

Anche la Germania in maniera non dissimile ha evidenziato come nel caso di una 'non affidabile attribuzione' si potrebbe incorrere nel rischio

[389] Corte internazionale di giustizia, sentenza del 6 luglio 1957, *The case of certain norwegian loans* (France v. Norway), opinione separata giudice Sir Hersch Lauterpatcht.

[390] Comitato Parlamentare per la sicurezza della Repubblica, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, 2010, p. 26;

[391] *Ibidem*.

di una «*false flag attacks*» con evidenti problematiche per la sicurezza nazionale e conseguenti errori[392].

Infine il Governo olandese, avallando le conclusioni di un gruppo di esperti (composto da membri dell'*Advisory council on international affairs* e dell'*Advisory committee on issues of public international law*, i quali hanno fornito un *report* sul cd. *cyber warfare*), ha ritenuto che l'utilizzo della forza in legittima difesa potrebbe essere usata solo laddove l'origine dell'attacco e l'identificazione del responsabile siano «*sufficently certain*»[393].

In definitiva, se la prassi sembra deporre per l'utilizzo di uno standard di prova più stringente rispetto a quello del *preponderance of evidence*, resta da chiedersi come possa 'concretamente' essere soddisfatto tale standard nel complesso contesto degli attacchi informatici.

Le difficoltà degli Stati nel fornire gli elementi probatori adeguati vengono alla luce laddove si esaminano alcuni dei casi assai significativi di attacchi informatici, come ad esempio il caso che ha coinvolto la Russia nelle recenti elezioni del presidente degli Stati Uniti e il caso *Stuxnet*.

Per quanto riguarda il primo, in particolare, è noto che secondo i risultati inseriti nel *Joint Analysis Report* (formulato dal Dipartimento della sicurezza interna e l'FBI), l'attribuzione dell'attacco alla Russia da parte del governo americano sarebbe sorretta da diverse indicazioni di carattere tecnico: attraverso l'individuazione di *tools* e le infrastrutture utilizzate, gli Stati Uniti hanno ritenuto i *Russian civilian and military intelligence services* (un gruppo di *hacker* russi) responsabili di aver

[392] Permanent Mission of Federal Republic of Germany to the United Nations to the Office for Disarmament Affairs, *note no. 516*, 5 novembre 2012.

[393] RIJKSOVERHEID, *Government response to the AIP/CAVV report on cyber warfare*, 17 gennaio 2012, p. 5. Questa indicazione pur non rientrando pienamente nello *clear and convincing* standard richiede indubbiamente un *quantum* probatorio più elevato rispetto a quello riferibile al *preponderance of evidence*.

compromesso le elezioni americane[394], e di aver agito dietro istruzioni del governo russo.

In un successivo documento, fornito dall'*Intelligence* americana, intitolato *Background to "Assessing Russian Activities and Intentions in Recent US Election": The Analytic Process and Cyber Incident Attribution*, il cui obiettivo sarebbe stato quello di ridurre le incertezze che riguardano le attività provenienti da paesi stranieri, anche con riguardo agli aspetti cibernetici[395], è stata ricostruita a partire dal 2012 la propaganda che il governo russo, attraverso l'utilizzo di *mass media*, ha perpetrato ai danni della democrazia statunitense[396] e sono stati indicati seppur parzialmente i criteri che gli analisti hanno adottato per risalire agli autori dell'attacco.

A bene vedere, tuttavia, non sembrano sussistere delle prove dirette 'chiare e convincenti' dell'attribuzione degli attacchi informatici al governo russo. Piuttosto sembra evincersi un utilizzo di prove indirette e deduzioni per corroborare l'idea della paternità russa dell'attacco. In particolare infatti il documento, una volta analizzato il contesto politico e i rapporti internazionali tra le due potenze, sottolinea un comportamento recidivo della Russia volto ad influenzare la politica interna di Stati stranieri attraverso un'ingerenza nel processo elettorale.

In modo non dissimile sembrano essere state utilizzate prove indirette anche in un altro caso di attacco informatico del 2010, l'affare *Stuxnet*[397]. Dall'analisi effettuata da esperti iraniani è emerso che, dato il livello di complessità del software e la specificità delle informazioni in esso

[394] Dipartimento della sicurezza interna statunitense e Federal Bureau of Investigation, *Grizzly steppe- Russian Malicious Cyber Activity*, 29 dicembre 2016, p. 1.

[395] Office of the Director of National Intelligence of USA, *Background to "Assessing Russian Activities and Intentions in Recent US Election": The Analytic Process and Cyber Incident Attribution*, 6 gennaio 2017, p. 1

[396] *Ibiedm*, p. 6.

[397] Per una breve ricostruzione del caso si rimanda al par. 2.1.1 del presente capitolo.

contenute, gli attacchi potevano essere imputati esclusivamente ad uno Stato e non a soggetti privati, in quanto solo gli appartenenti a cariche governative potevano essere a conoscenza di quelle informazioni[398].

Quello che emerge chiaramente da entrambi gli esempi proposti è che, a differenza di quanto sostenuto in astratto, quando gli Stati si sono trovati a sostenere l'attribuzione di un attacco informatico ad uno Stato straniero hanno fatto spesso ricorso all'utilizzo di prove indirette e deduzioni.

A noi sembra, invero, che anche alla luce delle indicazioni fornite dalla CIG allorquando nel caso del *Canale di Corfù* ha riconosciuto la possibilità allo Stato vittima di ricorrere a «*inferences of fact and circumstantial evidence*», in virtù dell'effettivo controllo esercitato da uno Stato sul proprio territorio, il principio possa essere riproposto nel contesto degli attacchi informatici. In particolare ritenendo che, laddove lo Stato riesca a provare in maniera 'chiara e convincente' la propria impossibilità nel fornire prove dirette a causa, ad esempio, del controllo effettivo esercitato dall' altro Stato sul proprio territorio (e quindi anche delle infrastrutture cibernetiche su di esso presenti), questi possa avvalersi di deduzioni e prove indirette.

5.3. Il possibile ricorso a criteri alternativi: il regime della responsabilità oggettiva

Le difficoltà nell'attribuzione delle condotte informatiche agli Stati per atti commessi da soggetti privati, ha portato alcuni autori a proporre soluzione alternative rispetto a quelle sviluppate dalla giurisprudenza internazionale e da quelle espressamente prevista nel Progetto di articoli

[398] RICHARDSON, *Stuxnet as Cyberwfare: Applying the Law of War to the Virtual Battlefield*, in *The John Marshall Journal of Information Technology and Privacy law*, 2011, p. 6.

sulla responsabilità degli Stati[399]. In particolare, vista la soglia particolarmente alta richiesta dai criteri di imputazione tradizionali, è stato suggerito che nello specifico settore degli attacchi informatici sarebbe possibile ridurre il grado di collegamento richiesto tra lo Stato e un attore non statale al fine di poter attribuire quella condotta allo Stato stesso. In questo modo, se da un lato, si potrebbe comunque incorrere in un problema di attribuzione erronea, dall'altro lato si colmerebbe una lacuna giuridica e si permetterebbe agli Stati vittima di un attacco informatico di poter agire in legittima difesa (se trattasi di un attacco 'armato') oppure attraverso contromisure (in tutti gli altri casi in cui vi sia stata la violazione di uno degli obblighi internazionali)[400]. A fronte di queste considerazioni, è stata proposta l'applicazione di *standard* di attribuzione variabili fondata sui possibili rimedi riconosciuti allo Stato vittima. Nel dettaglio, se lo Stato vittima decida di reagire attraverso attacchi informatici che siano espressione dell'uso della forza allora sarà necessario che l'attribuzione sia certa e si fondi sui criteri tradizionali e in particolare il criterio del

[399] Si vedano, ad esempio, EICHNESEHR, *Decentralized Cyberattack Attribution*, in *American Journal of International Law Unbound*, 2019, p. 213 ss.; KEITNER, *Attribution by Indictment*, in *American Journal of International Law Unbound*, 2019, p. 207 ss.; BOUTIN, *Shared Responsibility for Cyber Operations*, in *American Journal of International Law Unbound*, 2019, p. 197 ss.. In particolare, quest'ultima proposta appare particolarmente interessante. Essa mira all'applicazione della cd. *shared responsibility* al contensto delle operazioni informatiche. Più nel dettaglio, gli scenari che potrebbero verificarsi sono essenzialmente tre: il caso in cui due o più Stati siano parte della medesima operazione informatica. In questo caso lo Stato vittima può ritenere responsabili tutti gli Stati che hanno preso parte all'operazione e quindi può richiedere una riparazione da ognuno di essi. Il secondo caso invece riguarda l'ipotesi in cui uno Stato presti la sua assistenza o il suo aiuto ad un altro per condurre l'attacco informatico. Questo scenario potrebbe verificarsi allorquando uno Stato fornisca assistenza tecnica o assistenza informatica ad un altro Stato, ad esempio attraverso la condivisione del codice malevole utilizzato per compiere l'attacco informatico. In questo caso lo Stato che ha fornito assistenza potrà essere ritenuto responsabile solo allorché egli sia a conoscenza oppure avrebbe dovuto sapere che quel determinato *software* sarebbe stato usato per compiere un illecito internazionale.

[400] FINALY, PAYNE, *The Attribution Problem and Cyber Armed* Attack, in *American Journal of International Law Unbound*, 2019, p. 205.

controllo effettivo[401]. Nel caso in cui invece lo Stato intenda rispondere con mezzi differenti come sanzioni economiche o strumenti diplomatici allora è possibile utilizzare un criterio di attribuzione meno stringente come, ad esempio, quello della responsabilità oggettiva[402]. In questo caso la responsabilità ricadrà indirettamente sullo Stato dal quale l'attacco ha avuto territorialmente origine[403]. Secondo questa ricostruzione, l'utilizzo di questo modello incoraggerebbe gli Stati ad una maggiore cooperazione.

Ebbene, nonostante l'indubbia utilità di questa ricostruzione che ha senz'altro il pregio di fornire degli spunti interessanti circa i modi attraverso cui un attacco informatico possa essere attribuito ad uno Stato, essa non ci pare essere priva di criticità. Se da un lato, infatti, può essere condiviso l'assunto secondo cui quando si tratta di un attacco che raggiunga la soglia dell'uso della forza debbano essere usati i criteri di attribuzione tradizionali, dall'altro lato non può dirsi lo stesso per l'altra ipotesi. Questo modo di procedere, infatti, a nostro avviso, perde di vista un aspetto giuridico particolarmente rilevante, vale a dire la certezza giuridica di poter conoscere la qualificazione di una condotta *ex ante* e non

[401] *Ibidem*, p. 206.

[402] *Ibidem*.

[403] *Ibidem*. Più precisamente secondo gli Autori questo modello, utilizzato altresì nel contesto del terrorismo, riconoscerebbe a «[u]nder this approach an injured state may, for example, be able to use countermeasures against the state from which the cyberattack allegedly originated (assuming the other legal requirements for countermeasures are met), even if there was no evidence that the host state had any involvement in the attack beyond its territory being used. A strict liability model also encourages state cooperation by creating potential liability for reparations». Inoltre, il modello della *strict liability* andrebbe tenuto distinto dall'ipotesi della *due diligence* in quanto « as it does not establish a separate wrongful act on the part of the host state. Rather, this approach would apply strict liability to questions of attribution where a state has suffered a prohibited use of cyber force but chooses to pursue remedies through nonforcible legal processes rather than forceful retaliation. Used in this way, strict liability avoids the scenario where the injured party could neither protect itself before the fact, nor receive justice after it». Per quanto concerne gli aspetti inerenti all'utilizzo del modello in questione agli atti di terrorismo si rimanda a PROULX, *Babysitting Terrorists: Should States Be Strictly Liability for Failing to Prevent Transborder Attack?*, in *Berkley Journal of International Law*, 2005, p. 643-659.

solo sulla base delle reazioni che da essa possono scaturire. Secondo questa ricostruzione, infatti, si parte dal presupposto che uno Stato sia capace di qualificare in modo certo se l'attacco informatico abbia superato la soglia dell'uso della forza oppure no. Ma, come si è avuto modo di vedere in precedenza, non sempre è agevole giungere a conclusioni certe nemmeno con riguardo all'elemento oggettivo dell'illecito. Se è vero che un attacco informatico può certamente essere considerato un illecito internazionale, è però altrettanto vero che attribuendo una condotta allo Stato attraverso una responsabilità oggettiva, solo perché la condotta ha avuto origine dal suo territorio, creerebbe una disparità eccessivamente elevata. Inoltre, gli Stati potrebbero in questo qualificare una condotta in un modo o in un altro solo sulla base di un proprio interesse e cioè del modo attraverso cui reagire all'offesa subita.

6. Il principio di *due diligence* e la sua rilevanza nel contesto degli attacchi informatici

Com'è noto il principio della *due diligence*[404] è un corollario del principio di sovranità. Secondo quanto affermato dal giudice Huber nel noto caso *Island of Palmas* «[t]erritorial sovereignty (…) involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war»[405].

[404] La bibliografia sul tema è particolarmente diffusa, in questa sede si rimanda, tra gli altri, PISILLO MAZZESCHI, *"Due Diligence" e responsabilità internazionale degli Stati*, Milano, 1989; KULESZA, *Due Diligence in International Law*, Leida, 2016;

[405] Cfr. *Island of Palmas case*, p. 839.

L'obbligo della 'dovuta diligenza' è stato poi affermato e sviluppato in molti e successivi casi, tra cui quello relativo al Canale di Corfù ove la CIG ha sottolineato che ogni Stato ha l'obbligo di non consentire consapevolmente che il proprio territorio venga utilizzato per atti contrari ai diritti di altri Stati[406]. È altresì pacifico che quanto affermato dalla Corte sia un principio generale del diritto internazionale[407] ed esso ricomprenda non solo tutte le attività poste in essere nel territorio dello Stato, ma si estenda anche a tutte quelle condotte poste in essere sotto la giurisdizione ed il controllo dello Stato[408], sia che esse provengano dagli organi statali sia che provengano da enti pubblici e privati[409]. Quanto invece alla locuzione 'diritti di altri Stati', utilizzata dalla Corte, essa intende riferirsi a tutti quegli atti illeciti che producano effetti dannosi nei confronti di un altro Stato. Senonché, se è vero che gli effetti dannosi costituiscono un elemento necessario, è altrettanto vero che essi non sono sufficienti affinché possa determinarsi una violazione del principio *de quo*. Ciò in quanto esso si configura come un obbligo di condotta e non di risultato[410].

[406] CIG, *Corfu Channel* case, Judgment of 9 April 1949, *ICJ Reports* 1949, p. 22.

[407] Cfr. KOIVUROVA, *Due Diligence*, in *Max Planck Encyclopaedia of Public International Law*, 2010; BANNELIER-CHRISTAKIS, *Cyber Diligence: A Low-Intensity due diligence principle for low-intensity cyber operations?*, in *Baltic Yearbook of International Law*, 2014, p. 4.

[408] Cfr. ICJ, *Pulp Mills on the River Uruguay (Argentina* v. *Uruguay)*, Judgment of 20 April 2010, *ICJ Reports* 2010, para. 197, ove la Corte ha affermato che « (…) the obligation to "preserve the aquatic environment, and in particular to prevent pollution by prescribing appropriate rules and measures" is an obligation to act with due diligence in respect of all activities which take place under the jurisdiction and control of each party».

[409] Secondo Lammers «States are not only obliged to prevent violations of those rights committed by their organs but are also obliged to prevent inroads on the interests protected by those rights by the conduct of individuals or private entities from within their territories». Cfr LAMMERS, *Pollution of International Watercourses*, L'Aia, 1984, p. 527.

[410] La Commissione del diritto internazionale nel commentario dell'art. 7 del *Draft Articles on the Law of the Non-Navigational Uses of International Watercourse sand Commentaries thereto and Resolution on Transboundary Confined Groundwater* afferma che « The obligation of due diligence contained in article 7 sets the threshold for lawful State activity. It is not intended to guarantee that in utilizing an international watercourse significant harm would not occur. It is an obligation of conduct, not an obligation of result» (cfr. *Report of the International Law Commission on the Work of its Forty-sixth Session*, 1994). In modo non dissimile si è

In capo allo Stato dunque sorge un obbligo di condotta nel senso che lo Stato non è tenuto a far sì che quel determinato comportamento illecito non venga posto in essere, ma piuttosto è tenuto ad utilizzare tutte le misure necessarie per evitare che il comportamento illecito *in sé* si concretizzi. Ciò vuol dire che lo Stato non incorrerà in una ipotesi di responsabilità per il solo fatto che il risultato sperato non sia stato raggiunto, ma piuttosto per il fatto che non ha posto in essere tutti quei comportamenti, rientranti nelle sua facoltà, di cui esso aveva (o avrebbe dovuto avere) conoscenza, per prevenire il verificarsi di quella determinata condotta[411].

Così brevemente individuato il principio in esame, è agevole constatare come l'elemento dirimente consista proprio nella effettiva conoscibilità da parte dello Stato delle azioni poste in essere sul proprio territorio. Tuttavia, dal momento che non si può presumere, in virtù dell'esercizio effettivo svolto dallo Stato sul proprio territorio, che esso debba essere a conoscenza di tutte le attività compiute all'interno dei propri confini

pronunciata anche la CIG che nel caso *Pulp Mills* ha affermato « The Court considers that the obligation laid down in Article 36 is addressed to both Parties and prescribes the specific conduct of co-ordinating the necessary measures through the Commission to avoid changes to the ecological balance. An obligation to adopt regulatory or administrative measures either individually or jointly and to enforce them is an obligation of conduct. Both Parties are therefore called upon, under Article 36, to exercise due diligence in acting through the Commission for the necessary measures to preserve the ecological balance of the river». Cfr. ICJ, *Pulp Mills on the River Uruguay (Argentina* v. *Uruguay)*, par. 187.

[411] In questi termini si veda la sentenza della CIG sul caso relativo *all'applicazione della Convenzione sulla prevenzione e punizione del genocidio*, ove la stessa afferma « [I]t is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance».

statali[412], è necessario chiedersi se tale standard di comportamento possa essere applicato al cyberspazio e in che modo debba concretamente essere declinato. Detto altrimenti, che tipo di attività svolte nel cyberspazio uno Stato è tenuto a conoscere.

Ebbene, partendo dal presupposto ormai ampiamente condiviso in dottrina per cui il principio di *due diligence* vada applicato anche al contesto del cyberspazio[413], ci si deve chiedere se, affinché tale obbligo venga rispettato, lo Stato sia tenuto a monitorare tutte le attività informatiche che hanno luogo all'interno del proprio territorio. In altre parole, se lo Stato è tenuto a monitorare e sorvegliare tutte le attività che hanno luogo attraverso il proprio cyberspazio, *rectius* attraverso quel livello infrastrutturale del cyberspazio che risiede nei server ubicati all'interno del territorio di una nazione e su cui lo Stato esercita la propria sovranità[414].

Secondo la CIG l'obbligo di *due diligence* implica «the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party»[415], ne dovrebbe conseguire dunque che lo Stato per rispettare lo *standard* di comportamento sia tenuto a monitorare tutte

[412] Cfr. *Corfù Channel case*, p. 18.

[413] Si veda, tra gli altri, JENSEN, *State Obligations in Cyber Operations*, in *Baltic Yearbook of International Law*, 2014; KOLB, *Reflections on due diligence duties and cyberspace*, in *German Yearbook of International Law*, 2015, p. 113 ss.; BENDIECK, *Due Diligence in Cyberspace*, in *Stiftung Wissenschaft und Politik German Institute for International and Security Affairs*, 2016, p. 11 ss.; BUCHAN, *Cyberspace, Non-State Actors and the Obligation to prevent Transboundary Harm*, in *Journal of Conflict & Security Law*, 2016, p. 429 ss.; SHACKLEFORD, S. RUSSELL, A. KUEHN, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, in *Chicago Journal of International Law*, 2016, p. 1 ss.. Anche il Tallinn Manual 2.0, all'articolo 7 stabilisce che «[t]he principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States».

[414] A tal proposito si rimanda a quanto detto nel primo capitolo.

[415] *Pulp Mills case*, par. 197.

le attività sia pubbliche che private che vengono esercitata nel proprio territorio. Senonché procedendo analogicamente ciò vorrebbe dire autorizzare indirettamente gli Stati ad utilizzare programmi di sorveglianza di massa, come ad esempio il noto PRISM, per monitorare le attività informatiche dei propri cittadini (v. cap. III). Tuttavia, è agevole constatare come una conclusione siffatta non sia pienamente condivisibile, in quanto contrasti con l'intero corpus normativo che tutela il rispetto dei diritti umani e in particolare il diritto alla *privacy*[416].

Cosa resta allora del principio di *due diligence* nel contesto degli attacchi informatici? A noi pare che nonostante il riconoscimento di una generale applicazione del principio in esame, esso non possa dirsi ancora inteso in modo omogeneo da parte di tutti gli Stati[417]. Il principio quindi impone allo Stato, sì, un obbligo di condotta circa la prevenzione degli atti informatici compiuti sul suo territorio o attraverso lo stesso, ma lo Stato al fine di ottemperare a tale obbligo non può spingersi fino alla violazione del rispetto dei diritti fondamentali della persona come lo è il diritto alla *privacy.*

Ciò detto, quest'ultima ipotesi verrà presa in considerazione nel successivo capitolo dell'elaborato, ove verranno esaminate le circostanze in cui gli Stati per far fronte ad esigenze di sicurezza nazionale hanno violato le disposizioni della Convenzione Europea dei diritti dell'uomo e

[416] Il tema sul rapporto tra privacy e sorveglianza di massa verrà più diffusamente approfondito nel corso del terzo capitolo.

[417] Dall'analisi delle condotte degli Stati invero non pare possa riscontrarsi una uniformità di comportamenti tale da poter sostenere l'esistenza di una specifica norma consuetudinaria in questo contesto. Solitamente gli Stati affrontano il problema della *due diligence* nel contesto cibernetico secondo le loro specifiche esigenze. A tal proposito è stato opportunamente osservato che « The United States is more voluntary, Germany takes a more regulatory approach featuring a comprehensive cybersecurity policy that has long eluded U.S. policymakers, and China's approach encompasses broader economic and national security effort». Cfr. SHACKELFORD, RUSSELL, KUEHN, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from Public and Private Sectors*, in *Chicago Journal of International Law*, 2016, p. 34

si esamineranno i rimedi riconosciuti in capo ai soggetti, nonché la loro concreta effettività.

CAPITOLO III

LA SORVEGLIANZA DI MASSA E LA TUTELA DEL DIRITTO ALLA *PRIVACY*

SOMMARIO: 1. La nascita del concetto di *privacy* e la sua evoluzione. – 2. Lo sviluppo del diritto alla *privacy* nel diritto internazionale. – 2.1 Brevi cenni al caso *Datagate*. – 3. La sorveglianza di massa e l'intelligence sharing nella cornice dell'art. 8 CEDU. – 4. La sentenza *Big Brother Watch e altri c. Regno Unito*. – 4.1. La questione della sorveglianza di massa. – 4.2. La questione dell'*intelligence sharing*.

1. La nascita del concetto di *privacy* e la sua evoluzione.

L'ultimo aspetto da prendere in esame riguarda la contrapposta esigenza sviluppatasi nel cyberspazio tra tutela degli interessi statali, tra cui quello della sicurezza nazionale rappresenta l'esempio più appropriato, e la tutela delle posizioni giuridiche soggettive che possono venire in rilievo in internet.

La contrapposizione, più precipuamente, riguarda la necessità da parte degli Stati di tutelare la propria sicurezza soprattutto rispetto alle minacce terroristiche da un lato e il diritto alla privacy dall'altro. Ed è proprio da quest'ultimo aspetto che è necessario prendere le mosse per meglio comprendere il modo in cui attraverso lo sviluppo delle nuove tecnologie gli Stati con il passare degli anni hanno sempre più spesso limitato o intaccato uno dei diritti fondamentali degli individui.

Il concetto di *privacy*, secondo la più diffusa opinione, ha origini piuttosto recenti. Una sua prima, seppur non compiuta, elaborazione

giuridica può infatti rinvenirsi solo verso la fine del diciannovesimo secolo.

È precisamente nel 1890, in occasione della pubblicazione di un articolo da parte di due giuristi statunitensi (D. Warren e L. D. Brandeis), dal titolo *The Right to Privacy* [418], che il concetto di *privacy* trova una prima analisi compiuta volta a riconoscere "il diritto ad essere lasciato solo" [419].

Tale iniziale concezione aveva lo scopo di garantire la protezione dei sentimenti e delle emozioni, come estensione del diritto alla proprietà privata, contro la crescente invadenza della carta stampata[420]. In particolare, i nuovi profili che assumeva la stampa, proiettata verso un'ottica commerciale, apparivano come i principali segnali d'allarme per l'ingerenza nello spazio relativo alla vita privata e domestica dell'individuo. La capacità del giornalismo di impresa di diffondere in modo sempre più rapido e ampio una determinata notizia, unitamente alla possibilità di corroborare il testo scritto con immagini fotografiche, aveva fatto sì che anche dei semplici accadimenti di vita privata diventassero oggetto di curiosità della borghesia bostoniana dell'epoca.

In questo modo diventavano di dominio pubblico fatti riguardanti non solo soggetti che ricoprivano un qualche ruolo di pubblico interesse, ma anche vicende che non avevano alcun tipo di rilevanza pubblica o comunque da giustificare gli ampi spazi dedicatigli dalle testate giornalistiche.

È proprio in questo contesto, e in particolare a causa dei numerosi articoli di cronaca riguardanti la vita privata di uno dei due giuristi autori

[418] Si veda, WARREN, BRANDEIS. *The Right to Privacy*, in *Harvard Law Review*,1890, p. 193-220

[419] Cfr. PATRONO, *Privacy e vita privata (dir.pen.)*, in *Enciclopedia del diritto*, XXXV, 1986.

[420] Cfr. MASTRACCI, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La Comunità internazionale*, 2016, p. 555.

del menzionato articolo, che si iniziò ad avvertire l'esigenza di elaborare e definire in modo concreto gli spazi ed i limiti tra riservatezza, libertà di stampa e libertà di manifestazione del pensiero.

Secondo gli autori, sono due i criteri fondamentali da rispettare affinché la libera informazione non sia di ostacolo all'esercizio del diritto alla riservatezza di un individuo. Anzitutto, la notizia deve avere ad oggetto fatti di interesse pubblico poiché in questo caso il soggetto interessato, che riveste una carica o qualifica pubblica, ha una responsabilità specifica nei confronti della intera collettività. In secondo luogo, e cumulativamente, è necessario che vi sia il consenso del diretto interessato. La preoccupazione principale dei due giuristi, infatti, era l'asserita mancanza all'interno dei sistemi di *common law* di una tutela legale effettiva dei sentimenti che, a causa dell'intrusione e della curiosità altrui, subivano un vero e proprio danno suscettibile di un risarcimento. Il sistema americano aveva sviluppato una forma di protezione solo per quegli aspetti che riguardavano ingerenze tangibili e fisiche che riversava, di conseguenza, nel diritto di proprietà la tutela più adeguata.

Il carattere originariamente individualistico e 'proprietario' del diritto alla riservatezza, dovuto soprattutto al contesto sociale da cui emerge l'esigenza di tutela [421], non è tuttavia indicativo di un fenomeno legato alla necessità del singolo individuo, ma piuttosto anche dell'acquisizione di un privilegio da parte di un gruppo. Infatti, la *privacy*, anche nel suo contenuto originario e minimale di diritto ad essere lasciato solo, sembra voler esprimere un valore della persona nella sua dimensione non solo

[421] Si vuole far riferimento all'episodio legato ai pettegolezzi di un giornale locale sulla vita mondana di uno dei due autori, che apparteneva ad una delle famiglie più ricche di Boston, dal quale poi scaturì la necessità e l'esigenza di riconoscere in un certo modo un carattere giuridico al concetto. Cfr. WARREN, BRANDEIS, *op. cit.*, p. 200

individuale, ma anche sociale. Ed è proprio tale dimensione sociale che sembra caratterizzare il concetto di *privacy* nel mondo contemporaneo.

È noto infatti come a causa dell'enorme sviluppo tecnologico, verificatosi dapprima negli Stati Uniti e poi diffusosi nel resto del mondo, la tematica della tutela della sfera privata dell'individuo abbia assunto caratteristiche del tutto nuove che mettono in crisi i vecchi schemi ricostruttivi e i rapporti stessi tra pubblico e privato, nonché tra segretezza e informazione [422].

In altre parole, il diritto alla *privacy* si è evoluto dall'iniziale concezione di un diritto ad essere lasciato solo ad un diritto al controllo sulle informazioni che riguardano la nostra persona.

Il suo contenuto, infatti, si è via via esteso fino a ricomprendervi la tutela dei dati personali contro l'indebito utilizzo da parte di terzi. In questo modo la *privacy* è diventata anche il diritto ad esercitare un controllo sulle informazioni che attengono alla propria sfera personale, permettendo di conoscere in ogni momento se qualcuno sta raccogliendo informazioni sul proprio conto e, in caso di risposta positiva, di decidere se si vuole acconsentire alla raccolta delle stesse.

La nascita di internet – e in particolare lo sviluppo degli ultimi anni dei *social network* – ha rivoluzionato ancora di più il concetto di *privacy*, chiamandolo alla difficile sfida di un mondo virtuale in cui le informazioni personali sono, da un lato, diventate sempre più di dominio pubblico e, dall'altro lato, una vera e propria moneta di scambio della cd. economia digitale in cui gli utenti cedono le proprie informazioni personali in cambio di servizi, che solo all'apparenza appaiono gratuiti[423]. Il modello

[422] Su questo punto si veda, tra gli altri, RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 78 ss; ID, *Tecnologia dell'informazione e frontiere del sistema socio-politico*, in *Politica del diritto*, 1982, p. 28 ss.

[423] MASTRACCI, *op.cit.*, p. 556.

di *business* che caratterizza il mondo virtuale e in particolare internet sembra basarsi proprio sulla raccolta e lo sfruttamento di ingenti quantità di dati personali che, attraverso sistemi di sorveglianza di massa e condivisione delle informazioni tra Stati, mette sempre più a rischio la nostra *privacy* [424].

L'esempio più concreto di questo fenomeno è senz'altro rappresentato dalle rivelazioni dell'ex agente della CIA, Edward Snowden (*infra*), le quali hanno dimostrato come la sorveglianza di massa è in uso non solo nei regimi autoritari, ma riguarda altresì alcune democrazie occidentali, in particolar modo gli Stati Uniti e la Gran Bretagna [425].

In prima approssimazione quindi sembra possibile affermare che la *privacy* consta di due fondamentali elementi: in primo luogo quello tradizionale, e cioè il diritto ad essere lasciato solo, che può sinteticamente definirsi come diritto alla conoscenza esclusiva delle vicende relative alla propria vita privata; in secondo luogo, poi, quello che è emerso e sta emergendo in concomitanza con lo sviluppo tecnologico, vale a dire il diritto/interesse al controllo sulla circolazione dei propri dati personali.

Su queste premesse, scopo del presente capitolo è quello di analizzare in che modo la contrapposizione tra diritto alla sicurezza (attraverso la

[424] Solo per dare una stima approssimativa del business che si cela dietro lo scambio e la raccolta dei dati, secondo il Report del Garante Europeo della protezione dei dati del 2014 « Whereas previously data had been collected as part of the provision of a particular service, 'the added value of big data,' says one commentator, 'resides in the potential to uncover new correlations for new potential uses once the data have been collected … [which] may have nothing to do with the original purposes for which the data were collected.'Estimates of this added value vary according to context and methodology: revenues or net income per record/user for two global companies whose business models rely on personal data have been calculated at EUR 3-5 per year; while the digital value that EU consumers place on their data has been estimated at EUR 315 billion in 2011, forecast to rise to EUR 1 trillion by 2020». Cfr. European Data Protection Supervisor, *Privacy and Competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy*, Marzo 2014, p. 9.

[425] MASTRACCI, *op.cit.*, p. 556.

sorveglianza di massa) e sicurezza dei diritti (tutela del diritto alla privacy) possa essere declinata. In particolare, si cercherà di mettere in rilievo come il diritto alla privacy, nonostante una crescente tutela sul piano formale, concretizzatasi attraverso delle esplicite previsione nei diversi accordi internazionali, venga sempre più spesso messo in discussione dall'atteggiamento degli Stati, i quali, rifacendosi a istanze garantiste volte a proteggere la propria sicurezza nazionale, ne violano costantemente i contenuti. L'utilizzo di tecniche di sorveglianza di massa e di condivisione delle informazioni con altri Paesi (*intelligence sharing*) rappresentano alcuni degli strumenti attraverso cui gli Stati, provando a tutelare la propria sicurezza, agiscono in realtà in danno alla *libertà* dei propri (e non solo) cittadini.

Dinanzi a questa netta contrapposizione tra interessi statali e interessi individuali, la Corte Europea dei Diritti dell'Uomo, almeno in ambito regionale, avrebbe potuto svolgere un ruolo più pregnante, provando a consolidare alcuni principi sviluppati nel corso della sua pregressa giurisprudenza, applicandoli anche ai casi più recenti, nonché garantire forme di tutela più incisive rispetto a problemi emergenti, come quello dell'*Intelligence sharing*. Tuttavia, va sin da subito rilevato come questa possibilità sia rimasta una mera ipotesi.

Ciò detto, nel presente capitolo si procederà, dapprima, ad una disamina di carattere generale sulla emersione del diritto alla privacy nel diritto internazionale, analizzando le fonti più rilevanti che ne hanno permesso lo sviluppo. Passeremo poi alla trattazione dei profili problematici relativi ai regimi di sorveglianza di massa e dell'*intelligence sharing*, prendendo le mosse dal noto caso *Datagate*; successivamente, i due regimi verranno esaminati attraverso il prisma dell'art. 8 CEDU. Si passerà poi allo studio della sentenza *Big Brother Watch e altri* c. *Regno Unito* e si analizzeranno, separatamente, i profili attinenti alla sorveglianza di massa, ricostruendo

il percorso giurisprudenziale compiuto dalla Corte EDU, e quello relativo all'*intelligence sharing*.

2. Lo sviluppo del diritto alla *privacy* nel diritto internazionale

La tutela del diritto alla *privacy* nel diritto internazionale si caratterizza per essere a più livelli e, in questa sede, è possibile individuarne almeno due: uno regionale e uno universale.

Per quanto concerne il primo, che qui viene solo menzionato per poi essere più diffusamente analizzato in seguito, va anzitutto sottolineato come sin dagli anni settanta il tema della *privacy* è stato oggetto di specifica attenzione da parte del Consiglio d'Europa. Nel quadro degli strumenti elaborati in seno a tale organizzazione, possono essere individuati tre differenti accordi che hanno ad oggetto il tema della *privacy*. Il più importante e noto è senz'altro la Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (d'ora in poi, anche, CEDU) a cui si aggiungono le cc.dd. Convenzione 108 [426] e la Convenzione 185/2001 sulla criminalità informatica e i rispettivi protocolli addizionali [427]. In questa sede (*infra)*, si prenderà in esame solo la CEDU e, in particolare, l'articolo 8 della stessa.

Da un punto di vista universale, invece, la tutela del dritto alla privacy ha trovato il suo primo riconoscimento, sebbene in modo non vincolante, nell'art. 12 della Dichiarazione universale dei diritti umani. Secondo il

[426] La citata convenzione appare particolarmente rilevante per due ordini di ragioni. In primo luogo perché essa è stata ratificata da un gran numero di Stati, tra i quali compare, da ultimo, anche l'Italia, e quindi per la grande rilevanza che tale strumento ha assunto sul piano interno e sull'influenza che ha avuto sugli altri atti dell'organizzazione. E, in secondo luogo, per il ruolo determinante che ha assunto prima dell'approvazione del Trattato di Lisbona. Per un'analisi approfondita sul tema si rimanda a DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018, p. 89 ss.

[427] *Ibidem*, p. 93 ss.

testo dell'articolo, infatti, «[n]essun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni» [428].

Lo sviluppo successivo, questa volta su base vincolante, è da ricondurre invece al Patto internazionale sui diritti civili e politici del 1966, il cui articolo 17 stabilisce che: «1. Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione. 2. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese» [429].

Se è vero che sia a livello universale che regionale il diritto alla *privacy* è stato sempre più spesso oggetto di una specifica previsione, è altrettanto vero che il riconoscimento di una sua concreta tutela è tardato ad arrivare. A tal proposito basti pensare all'atteggiamento delle Nazioni Unite e più in particolare dell'Assemblea Generale, la cui scarsa attività ha messo in luce la poca attenzione che per almeno diversi anni è stata dedicata al problema. Anche volendo prescindere dal dato quantitativo relativo al numero limitato di atti dell'Assemblea Generale in tema di riservatezza

[428] Cfr. *Dichiarazione universale dei diritti umani*, UN Doc. A/RES/217 (III) del 10 dicembre 1948. Per un esame di tale disposizione si veda, tra gli altri, REHOF, *"Article 12",* in ALFREDSSON, EIDE (a cura di) *The Universal Declaration of Human Rights: A Common Standard of Achievement*, L'Aia, 1999, p. 251 ss.; ID, *"Article 12"*, in EIDE, ALFREDSSON, MELANDER, REHOF, ROSAS, SWINEHART (a cura di) *The Universal Declaration of Human Rights: A Commentary*, Oslo, 1992, p. 187 ss.

[429] Cfr. *Patto sui diritti civili e politici*, 16 dicembre 1966, art. 17. Per una approfondita e puntuale analisi si rimanda a BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti umani e diritto internazionale*, 2011, p. 454-463; vedi anche NOWAK, *UN Covenant on Civil and Political Rights. CCPR Commentary*, seconda edizione, Kehl, 2005, p. 385 ss.

(per giunta adottati in un arco temporale abbastanza ampio) [430], anche l'aspetto qualitativo dell'incisività sostanziale degli interventi dell'Assemblea stessa in tema di *privacy* lascia molto a desiderare. In altre parole, l'Assemblea Generale non ha né realmente affrontato la portata sostanziale di tale diritto né ha contribuito ad una sua reale evoluzione [431].

Dal 1990 ad oggi, poi, l'Organo dell'ONU si è sostanzialmente disinteressato del problema non pronunciandosi più sul tema. Questa circostanza appare ancora più rilevante se si considera l'enorme evoluzione tecnologica in materia di comunicazione e trasmissione dei dati personali a cui stiamo assistendo, nonché ai connessi rischi relativi al godimento del diritto alla vita privata e del diritto alla tutela delle informazioni di carattere personale [432].

A dire il vero, nessun risultato positivo si rinviene nemmeno se si volge lo sguardo all'attività giurisprudenziale posta in essere dal Comitato Onu sui diritti umani che nel 1988 ha adottato il *General Comment No. 16*, riguardante il contenuto e la portata dell'art. 17 del Patto internazionale sui diritti civili e politici.

Senonché, è in questo contesto di particolare inerzia che deve essere favorevolmente inquadrata la risoluzione dell'Assemblea Generale 'sulla protezione del diritto alla privacy nell'era digitale', la cui importanza, anche solo perché trattasi della prima Risoluzione adottata dalle Nazioni

[430] Si fa riferimento in particolare alle seguenti risoluzioni adottate dell'Assemblea: *Human Rights and Scientific and Technological Developments*, UN Doc. A/RES/2450 (XXIII) del 19 dicembre 1968; *Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind*, UN Doc. A/RES/3384 (XXX) del 10 novembre 1975; *Guidelines for the Regulation of Computerized Personal Data Files*, UN Doc. A/RES/45/95 del 14 dicembre 1990.

[431] Cfr. NINO, *La risoluzione dell'Assemblea Generale delle Nazioni Unite sulla tutela della privacy nell'era digitale: importanti luci, ma non poche ombre*, in *Diritto del commercio internazionale*, 2014, p. 768.

[432] *Ibidem*.

Unite in materia, ci impone di esaminarne le principali caratteristiche e novità, nonché alcune delle sue principali criticità.

Il documento è stato inteso da parte della dottrina come uno spartiacque rispetto al passato e un punto di partenza ideale per un'effettiva salvaguardia della *privacy* nell'era di internet [433].

La Risoluzione, adottata per consenso nel dicembre del 2013, mira all'applicazione degli *standard* di tutela previsti in materia di diritti umani anche alle attività di intercettazione delle comunicazioni e di archiviazione dei dati personali [434].

Il documento inoltre ha avuto il pregio di svolgere un ruolo catalizzatore che ha determinato come conseguenza il coinvolgimento dell'Alto Commissario per i diritti Umani, al quale è stato richiesto di presentare un *report* sulla protezione e promozione del diritto alla *privacy* «in the context of domestic and extraterritorial surveillance and/or interception of digital communications and the collections of personal data, including on mass scale (…)» [435].

Il *report* quindi si inserisce in un contesto caratterizzato dall'interessamento, seppur ad uno stato embrionale, alla materia da parte di diversi organi delle Nazioni Unite. Esso inoltre fornisce diverse indicazioni sul rapporto intercorrente tra sorveglianza di massa e diritto alla *privacy*, giungendo a conclusioni di non poca importanza.

Più dettagliatamente, nel documento si asserisce che finanche la mera possibilità che una comunicazione venga intercettata possa integrare una

[433] *Ibidem*; JOYCE, *Privacy in the Digital Era: Human Rights Online*, in *Melbourne Journal of International Law*, 2015, p. 2. Secondo l'Autore infatti «[r]esolution 68/167 represents an important development in the move to protect privacy in the digital era and at the international level».

[434] Assemblea Generale delle Nazioni Unite, *The Right to Privacy in the Digital Age*, A/RES/68/167, 13 dicembre 2013.

[435] *Ibidem*, p. 3.

interferenza con il diritto alla *privacy*, non essendo necessario che la comunicazione sia stata effettivamente sottoposta a intercettazioni [436].

Il report sottolinea inoltre come la perdurante differenza tra il contenuto delle comunicazioni e i *metadata* [437] deve ritenersi ormai superata in quanto del tutto anacronistica ed irrilevante rispetto all'attuale contesto in cui si sviluppano le comunicazioni [438]. Questa affermazione ha non poca rilevanza se si considera che la caratteristica insita dei *metadata* è proprio quella di non rivelare il contenuto delle comunicazioni.

Infine, il documento, sebbene qualifichi il diritto alla *privacy* come un diritto derogabile, sottolinea che per non considerare una interferenza con il come arbitraria o illecita è necessario far riferimento ai principi di legalità, necessità e proporzionalità così come definiti e sviluppati nel diritto internazionale dei diritti umani [439].

Se questi sono gli aspetti positivi della Risoluzione, va segnalato che la stessa presenta anche diversi punti controversi. In primo luogo, ad esempio, allorquando fa riferimento all'applicabilità dei principi di base

---

[436] High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, A/HRC/27/37, 2014.

[437] Con il termine *metadato* si suole indicare quell'insieme di informazioni di carattere personale capaci di descrivere un determinato dato senza però rivelarne il contenuto.

[438] High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 2014.

[439] Affinché una interferenza con il diritto alla privacy possa essere compatibile con il diritto internazionale dei diritti umani è necessario che la stessa superi i test di legalità, necessità e proporzionalità. Questo vuol dire che l'azione consistente in una violazione deve essere prevista in una legge chiara, pubblicamente accessibile e precisa nonché che le sue conseguenze siano prevedibili. Inoltre, l'interferenza deve perseguire uno scopo legittimo e deve essere necessaria e proporzionata al fine di raggiungere tale scopo. Com'è noto, i tre requisiti sono espressamente previsti dall'art. 8 (2) della Convezione, tuttavia è possibile ritenere che gli stessi facciano parte del diritto internazionale dei diritti umani in una prospettiva più ampia dato che i tribunali hanno spesso interpretato anche la Convenzione americana dei diritti dell'uomo e la Convenzione internazionale sui diritti civili e politici nello stesso modo. Cfr. BRUNNER, *Digital Communications and the Evolving Right to Privacy*, in LAND, ARONSON (a cura di) *New Technologies for Human Rights Law and Practice*, Cambridge University Press, 2018, p. 226, nota n. 51; *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Martin Scheinin, par. 16–19, U.N.Doc. A/HRC/13/37, dicembre 2009.

riconosciuti per la tutela della privacy alle comunicazioni in rete, il documento avrebbe potuto spingersi oltre e indicare anche le caratteristiche che la legge nazionale avrebbe dovuto assumere, individuando altresì i presupposti alla base di dette normative [440]. Un riferimento alla natura, alla durata, alle finalità delle misure di sorveglianza delle comunicazioni, nonché l'indicazione dei modi di conservazione, della durata dell'archiviazione dei dati già acquisiti, avrebbe senz'altro agevolato gli Stati nella concreta regolamentazione delle attività di sorveglianza delle comunicazioni in rete. A ciò va aggiunto che alcuni aspetti particolarmente controversi, come quello relativo alla responsabilità dei fornitori di servizi di comunicazioni[441], non sono stati nemmeno accennati dalla Risoluzione. Forse, anche in questo caso, almeno un'indicazione che denotasse l'esigenza di regolamentazione sarebbe stata particolarmente importante per tracciare la strada agli Stati.

Dalla breve analisi sin qui condotta si evince dunque almeno una graduale emersione del problema, tant'è che secondo parte della dottrina l'insieme di regole e principi che il diritto internazionale dei diritti umani già conosce permetterebbe di ampliare la protezione del diritto alla *privacy* fino a ricomprendervi una tutela avverso le più innovative tecniche di sorveglianza, di intercettazioni e di collezione dei dati [442]. Ma, nonostante tali garanzie, va rilevato come la prassi di alcuni Stati non appaia altrettanto omogenea e in linea con i diritti poc'anzi individuati, essendovi legislazioni inadeguate e incerte, se non addirittura talvolta illegittime [443].

[440] Così si veda NINO, *op.cit.*, p. 775.

[441] Il problema è di non poco peso se si considera che molte legislazioni nazionali sulla sorveglianza delle comunicazioni obbligano i fornitori di servizi, pena il mancato rilascio della licenza di esercizio, a riconoscere alle agenzie governative l'accesso ai dati delle comunicazioni dei loro clienti.

[442] Si veda DELLA MORTE, *op.cit.*, p. 177 ss.

[443] *Ibidem*.

In particolare, secondo le indicazioni fornite dal già citato *Report* dell'Alto Commissario delle Nazioni Unite per i diritti umani, se si volge lo sguardo e si analizza in modo approfondito la prassi statale degli ultimi anni non si può non rilevare come negli ordinamenti di molti Paesi la sorveglianza digitale, sia palese che segreta, si è proliferata attraverso forme di sorveglianza governative, diventando così una costante piuttosto che una eccezione [444]. Gli esempi in tal senso sono diversi. Si va dai casi in cui i governi hanno minacciato di bloccare alcuni servizi di telecomunicazione qualora i titolari di tali servizi non avessero consentito l'accesso ai dati relativi al traffico sulle proprie reti; all'uso della sorveglianza delle comunicazioni per individuare gli oppositori o i dissidenti politici; all'intercettazione di tutte le comunicazioni telefoniche effettuate e ricevute in un dato territorio; fino al caso più grave in cui è stato inserito all'interno di tutti i computer in vendita un *software* in grado di filtrare e conservare – per fini di sorveglianza – alcune informazioni [445].

A fronte di queste violazioni ciò che viene richiesto agli Stati è di adottare un impianto legislativo chiaro e non eccessivamente discrezionale, che preveda misure di sorveglianza solo quando queste siano strettamente necessarie[446]. In altre parole, la portata e le modalità

[444] Traduzione dell'Autore. Cfr. *Report* dell'Alto Commissario delle Nazioni Unite per i diritti umani, *The Right to Privacy in the Digital Age*, p. 3, ove viene dichiarato che «[d]eep concerns have been expressed as policies and practices that exploit the vulnerability of digital communications technologies to electronic surveillance and interception in countries across the globe have been exposed. Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure».

[445] *Ibidem*.

[446] Per qualificare le misure come necessarie, l'Alto Commissario per i Diritti Umani richiama il commento generale n. 27 all'art. 12 della Convenzione internazionale sui diritti politici e civili. A tal proposito viene indicato che «the restrictions must not impair the essence of the right […]; the relation between right and restriction, between norm and exception, must not be reversed." The Committee further explained that "it is not sufficient that the restrictions

attraverso cui gli Stati esercitano il loro potere devono essere indicate (in una legge o in linee guida vincolanti e pubbliche) con ragionevole chiarezza. A tal fine non è sufficiente che la legge sia semplicemente accessibile, ma è necessario che anche gli effetti prodotti siano altrettanto conoscibili [447]. Allo stesso tempo, allorquando ci si trova dinanzi a ipotesi di sorveglianza segreta, che possano determinare quindi maggiori rischi di arbitrarietà e discrezionalità, sarà necessaria una più adeguata precisione della norma disciplinante e una supervisione *ex post* più incisiva[448].

Ciò detto, la costante contraddizione tra riconoscimento e ampliamento del diritto alla *privacy* da un lato e intensificazione delle misure statali volte alla sorveglianza di massa dall'altro, ci impone di esaminare brevemente l'origine del problema, nonché il ruolo svolto sia dalla Convenzione Europea dei Diritti dell'Uomo che dai giudici di Strasburgo.

2.1. Brevi cenni al caso Datagate.

Per poter affrontare il problema relativo alla sorveglianza di massa nel novero di tutele apprestate dalla CEDU, non si può prescindere dal tratteggiare un breve *excursus* sulle vicende relative al citato caso *Snowden,* che hanno poi determinato il pronunciamento della Corte in merito al caso giurisprudenziale che verrà successivamente esaminato.

serve the permissible purposes; they must also be necessary to protect them. (…) In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate». Cfr. *The right to privacy in the Digital Age*, p. 8-9.

[447] *Ibidem*, p. 10.

[448] *Ibidem*.

Le note rivelazioni dell'agente della *National Security Agency* (*NSA*) [449], Edward Snowden, che hanno dato vita al caso *Datagate,* hanno infatti senza dubbio modificato la percezione a livello globale del fenomeno della sorveglianza di massa e creato un intenso dibattito sia dottrinale[450] che pubblico circa la legittimità e i limiti di tali attività di *intelligence*.

Tema centrale della vicenda è stata la rivelazione dell'esistenza del programma statunitense di sorveglianza elettronica di massa, cd. PRISM, il quale è stato costantemente applicato a partire dal 2006 sino al 2013. Successivamente le rivelazioni si sono arricchite di dettagli ed hanno denunciato l'esistenza di un coinvolgimento del programma PRISM da parte dell'agenzia di *intelligence* britannica, la l'*UK Government Communications Headquarters* (GCHQ) e della predisposizione da parte di alcuni Stati europei di programmi autonomi di sorveglianza delle telecomunicazioni su larga scala, con funzioni e natura non dissimili dal programma PRISM.

---

[449] La *National Security Agency* è un'agenzia di *intelligence* e controspionaggio creata e istituzionalizzata dal Presidente Truman nel 1952. L'origine della sua attività è da rintracciare nella decriptazione di messaggi cifrati nel corso della II guerra mondiale. Oggi, invece, agisce sotto la direzione del Dipartimento di difesa statunitense ed è responsabile del monitoraggio e dell'interpretazione dei cd. segnali intelligenti, e cioè di tutte quelle informazioni sensibili, generalmente criptate, e per lo più in formato digitale. Dopo l'approvazione del cd. *Freedom Act* nel 2015, l'Agenzia dispone di poteri più limitati, in particolare non è più responsabile dell'archiviazione dei tabulati telefonici che sono invece custoditi direttamente dalle aziende di comunicazione. Un'ulteriore spinta riformista è stata poi data dalla giurisprudenza statunitense e in particolare dalla decisione con la quale una Corte d'appello federale ha dichiarato l'interpretazione offerta dalla NSA della sezione 215 del *Patriot Act* fosse illegittima. Sul punto si veda United States Court of Appeals for the Second Circuit, *American Civil Liberties Union et al.* v. *James R. Clapper, in his official capacity as Director of National Intelligence et. al.* 7 maggio 2015, par. 12-42; DELLA MORTE, *op.cit.*, p. 179, nota 510.

[450] Sul caso *Datagate* si veda, in termini generali, GREENWALD, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* New York, 2015. In relazione al diritto internazionale, tra gli altri, NINO, *Il caso Datagate: i problemi di compatibilità nel programma di sorveglianza di Prism con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti Umani e Diritto Internazionale*, 2013, p. 727; BLASI-CASAGRAN, *Global Data Protecion in the Field of Law Enforcment: an EU Perspective*, Londra, 2016; MILLER (a cura di), *Privacy and Power*, Cambridge, 2017; WAGNER, *Global Free Expression-Governing the Boundaries of internet Content*, Berlino, 2016.

Il più noto tra questi è senz'altro il programma denominato *Tempora*, attraverso cui la GCHQ raccoglie dati personali direttamente dai cavi sottomarini transatlantici utilizzati per il trasferimento delle comunicazioni elettroniche [451].

Secondo alcuni attivisti impegnati nella difesa del diritto alla *privacy*, tali programmi avrebbero notevolmente indebolito le libertà fondamentali della persona, generando un movimento di indignazione globale e rendendo poco credibili le motivazioni spesso addotte dai governi, i quali giustificano tali azioni al fine di prevenire atti terroristici [452].

Merita altresì menzione l'esistenza di un rapporto di *intelligence sharing* tra la NSA e l'*UK Government Communications Headquarters* (GCHQ), nonché la rivelazione che gli Stati Uniti insieme ad alcuni dei Paesi facenti parte della cd. Five Eyes[453] spiavano gli esponenti di governo di alcuni degli Stati loro alleati, come ad esempio Germania, Messico, Brasile e Indonesia [454].

Tali circostanze hanno portato, da un lato, alla riforma della NSA e, dall'altro, al mancato rinnovo della sezione 215 del *Patriot Act* statunitense[455], testo normativo che ha rappresentato fino a quel momento la base giuridica di quanti sostenevano la legittimità di tali attività. La

---

[451] EMACASKILL, BORGER, HOPKINS, DAVIES, BALL, *GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications*, *The Guardian*, 21 giugno 2013

[452] Cfr. MILANOVIC, *Human Rights and Foreign Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal*, 2015, p. 8.

[453] La Five Eyes è un'alleanza tra diversi paesi anglofoni (Stati Uniti, Regno Unito, Australia, Canada e Nuova Zelanda) il cui principale obiettivo è quello di cooperare nel settore dell'*intelligence*). In generale si veda NYST, *The Five Eyes Fact Sheet*, in *Privacy International Law*, 2013, consultabile online al seguente indirizzo https://www.privacyinternational.org.; FARRELL, *History of 5 Eyes-Explainer*, in *The Guardian*, 2 dicembre 2013, consultabile online al seguente indirizzo http://www.theguardian.com.

[454] MILANOVIC, *op.cit.*, p. 81.

[455] La sezione 215 del *Patriot Act* stabilisce che: «[a]uthorizes the Director of the FBI (or designee) to apply for a court order requiring production of certain business records for foreign intelligence and international terrorism investigations. Requires the Attorney General to report to the House and Senate Intelligence and Judiciary Committees semi-annually».

sezione 215 infatti attribuiva alle autorità governative americane il potere di richiedere ed ottenere dagli organismi competenti la produzione di qualsiasi «cosa tangibile, compresi libri, registrazioni, documenti» che sia necessaria per lo svolgimento di un'indagine collegata al terrorismo internazionale, sulla base di un'ordinanza emessa dal Tribunale competente[456]. Quest'ultimo adotta le sue decisioni in un contesto giudiziario che non permette ai diretti interessanti di sollevare osservazioni e di esercitare i loro diritti fondamentali, siano essi di natura sostanziale ovvero processuale[457]. A ciò va aggiunto che tanto la richiesta di provvedimento da parte delle autorità competenti quanto la pronuncia stessa sono di natura 'riservata' per esigenze di sicurezza nazionale, imponendo così un obbligo di segretezza a chiunque ne venga a conoscenza [458].

Senonché in tale problematico contesto, nel giugno del 2015 è stato approvato il *Freedom Act,* il cui scopo principale è quello di riformare e limitare l'uso della sezione 215 del *Patriot Act* [459]. Più nel dettaglio, l'obiettivo del nuovo testo normativo mira al rafforzamento dei requisiti necessari per l'ottenimento di informazioni, eliminando così una presunzione di rilevanza di qualsiasi richiesta proveniente dalle autorità

[456] Cfr. NINO, *Il caso Datagate: i problemi di compatibilità nel programma di sorveglianza di Prism con la normativa europea sulla protezione dei dati personali e della privacy*, *op.cit.*, p. 737.

[457] *Ibidem*.

[458] Si veda a tal proposito WHITEHEAD, ADEN, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Initiatives*, in *American University Law Review*, 2002, p. 1081 ss.

[459] Si può leggere infatti che il *Freedom Act* è stato approvato «[t]o reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes. o reform the authorities of the Federal Government to require the production of certain records, conduct electronic surveillance». Cfr. *Intelligence Oversight and Surveillance Reform Act*, 2015, consultabile online al seguente indirizzo www.congress.gov.

governative. Secondo il nuovo testo infatti il governo statunitense deve altresì dimostrare dinanzi alla *United States Foreign Intelligence Surveillance Court* (FISC)che vi sia un ragionevole motivo per credere che una comunicazione sia tale da poter essere sottoposta ad intercettazione e che vi sia un ragionevole sospetto che la medesima sia connessa ad atti di terrorismo internazionale [460].

Il caso *datagate* ha assunto particolare rilievo anche oltre i confini statunitensi, interessando anche i cittadini europei. Infatti, una delle pratiche più spesso utilizzate dagli Stati Uniti era proprio quella di condividere le informazioni ottenute con altri governi europei, tra questi, in particolare, vanno segnalati la Gran Bretagna, il Canada, l'Australia e la Nuova Zelanda (e cioè tutti gli Stati facenti parti della cd. Five Eyes Alliance). Ma vi è di più. Secondo le indicazioni fornite dall'agente della CIA, i sistema di sorveglianza di massa riguardavano non solo altri Paesi europei (Francia[461], Svezia [462], Russia [463],), ma anche Stati extra europei (Cina [464], Etiopia [465] e Colombia [466]) mettendo in luce così l'esistenza di una vera e propria rete globale di sorveglianza[467].

---

[460] LEVINSON-WALDMAN, *NSA Surveillance in the War on Terro*r, in GRAY e HENDERSON(a cura di) *The Cambridge Handbook of Surveillance Law*, Cambridge, 2017, p. 37

[461] JOHANNES, FOLLOROU, *In English: Revelations on the French Big Brother*, *Le Monde*, 4 luglio, 2013.

[462] BORGER, *GCHQ and European spy agencies worked together on mass surveillance*, *The Guardian*, 1 novembre, 2013.

[463] POETRANTO, *The Kremlin's new internet surveillance plan goes live today, The Citizen Lab*, 1 novembre 2012, https://citizenlab.ca/2012/11/the-kremlins-new-internet-surveillance-plangoes- live-today/; WALKER, *Russia to monitor 'all communications' at Winter Olympics in Sochi*, *The Guardian*, 6 ottobre, 2013.

[464] OpenNet Initiative, *internet Filtering in China*, 2009 pp. 14–17; Human Rights Watch, *Freedom of Expression and the internet in China*, 2001.

[465] Human Rights Watch, *They Know Everything We Do: Telecom and internet Surveillance In Ethiopia*, 2014.

[466] Privacy International, *Shadow State: Surveillance, Law and Order in Colombia*, 2015, pp. 27–31.

[467] BRUNNER, *Digital Communications and the Evolving Right to Privacy*, *op.cit.*, p. 222-223.

Infine, è interessante soffermarsi sulle conseguenze scaturite dalle rivelazioni di Snowden. Se da un lato infatti esse hanno portato ad una parziale riforma dell'impianto normativo statunitense in materia – come visto con l'emanazione del *Freedom Act* – con la conseguente diminuzione di un uso indiscriminato della sorveglianza di massa, dall'altro lato invece in Europa si sta assistendo ad un costante uso di questi strumenti. Solo per fare un esempio, l'*Investigatory Powers Act* britannico riconosce al governo ampi poteri in materia di intercettazioni delle comunicazioni di massa, un ampio margine di manovra volto all'ottenimento dei dati da parte delle compagnie di servizi che svolgono la loro attività all'interno del Paese, nonché stabilisce un rafforzamento degli strumenti tecnici adoperati per svolgere tale attività[468].

Ebbene, è proprio in questo contesto che appare particolarmente importante sia la tutela fornita dall'art. 8 CEDU che l'attività interpretativa svolta dalla Corte Europea dei Diritti dell'Uomo che, attraverso la propria giurisprudenza, ha fornito un consistente sviluppo al tema che qui si sta esaminando.

3. La sorveglianza di massa e l'intelligence sharing nella cornice dell'art. 8 CEDU

Com'è noto, l'art. 8 CEDU stabilisce che «1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza; 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico

[468] Cfr. *Investugatory Powers Act*, 29 novembre 2016, consultabile online al seguente indirizzo www.legislation.gov.uk/ukpga/2016/25/contents/enacted/data.htm.

del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».

È altresì noto che la giurisprudenza della Corte EDU abbia allargato la portata applicativa dell'art. 8, provando ad adeguare il dettato normativo ai diversi problemi che di volta in volta l'innovazione tecnologica ha palesato [469]. Ciò in quanto la Convenzione va intesa come «uno strumento vivente da interpretare alla luce delle condizioni della vita attuale»[470]. Soprattutto grazie all'interpretazione evolutiva, l'ambito di applicazione dell'art. 8 si è progressivamente ampliato «di riflesso alla crescente accettazione sociale e culturale del diritto di ciascuno di vivere nel modo più consono alle proprie inclinazioni» [471].

Ora, sebbene la formulazione dell'art. 8 CEDU non prenda in considerazione direttamente il problema della sorveglianza di massa e soprattutto la questione relativa alla sorveglianza attraverso strumenti informatici, secondo l'interpretazione fornita dalla stessa Corte è possibile affermare che la sorveglianza strategica[472] e la sorveglianza via GPS[473] costituiscano una ingerenza nel diritto alla *privacy* tale da poter essere

[469] In termini più ampi, sull'impatto che le nuove tecnologie hanno assunto sul rispetto dei diritti garantiti dalla CEDU, si veda, tra gli altri, MAROTTA, *Innovazioni tecnologiche e diritto al rispetto del domicilio nella Convenzione Europea*, in *Rivista di diritto internazionale*, 2005, p. 1044 ss. Da una prospettiva di diritto internazionale privato, invece, si rimanda a ORNELLA, *La Legge applicabile alla tutela dei diritti della personalità nella prospettiva comunitaria*, in *Rivista di diritto internazionale*, 2009, p. 1020 ss.; ZARRA, *Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo internet*, in *Rivista di diritto internazionale*, 2015, p. 1234 ss..

[470] Cfr. TOMMASI, *Articolo 8*, in BARTOLE, DE SENA, ZAGREBELSKY (a cura di), *Commentario breve alla Convenzione Europea dei diritti dell'Uomo*, 2012, p. 298.

[471] Così citato in *Ibidem*.

[472] Cfr. CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Liberty e altri* c. *Regno Unito*, 1 luglio 2008, par. 63.

[473] ID, *Uzun* c. *Germania*, 2 settembre 2010, par. 49-53

giustificata solo in base ai parametri fissati dal capoverso del medesimo articolo (segnatamente, legalità, necessità e proporzionalità)[474].

Per quanto riguarda l'ambito soggettivo di applicazione, esso annovera tutti quei soggetti che anche solo *potenzialmente* si considerino vittime delle misure di sorveglianza, che a loro volta sono contrarie alla Convenzione, e ciò è vero anche allorquando l'interessato non sia in grado di stabilire se concretamente ha subito un'intercettazione[475]. Secondo l'interpretazione fornita dalla Corte EDU infatti anche la mera esistenza di una disciplina sulle intercettazioni determina, per tutti coloro che sono anche solo potenzialmente i destinatari di quella normativa, una minaccia di sorveglianza capace di ostacolare la libertà di telecomunicazione e pertanto costituisce un'ingerenza nel diritto al rispetto della vita privata e familiare e della corrispondenza[476]. Laddove invece il ricorrente si dolga

[474] Cfr. TOMMASI, *Articolo 8, op.cit.,* p. 356.

[475] *Ibidem*.

[476] *Ibidem*; Corte europea dei diritti dell'uomo, sent. 6 settembre 1978, *Klass and others v. Germany*, ricorso n. 5029/71, al paragrafo 41 è infatti possibile leggere « the first matter to be decided is whether and, if so, in what respect the contested legislation, in permitting the above-mentioned measures of surveillance, constitutes an interference with the exercise of the right guaranteed to the applicants under Article 8 para. 1 (art. 8-1).Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision. In its report, the Commission expressed the opinion that the secret surveillance provided for under the German legislation amounted to an interference with the exercise of the right set forth in Article 8 para. 1 (art. 8-1). Neither before the Commission nor before the Court did the Government contest this issue. Clearly, any of the permitted surveillance measures, once applied to a given individual, would result in an interference by a public authority with the exercise of that individual's right to respect for his private and family life and his correspondence. Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menance of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence. The Court does not exclude that the contested legislation, and therefore the measures permitted thereunder, could also involve an interference with the exercise of a person's right to respect for his home. However, the Court does not deem it necessary in the present proceedings to decide this point»; Corte europea dei diritti dell'uomo (iv sezione), sent. 18 maggio 2010, *Kennedy v. Regno Unito*, ricorso n. *26839/05*, ove ai

della contrarietà all'art. 8 CEDU di una misura di intercettazione a cui era stato sottoposto, sarà suo onore provare l'esistenza di quella intercettazione oppure la ragionevole probabilità che quella misura sia stata applicata nei suoi confronti [477].

Prima di affrontare gli sviluppi interpretativi della Corte e analizzare con maggior dettaglio la recente sentenza *Big Brother Watch*, è necessario tuttavia sottolineare alcuni aspetti di carattere generale. In primo luogo, la Corte riconosce agli Stati contraenti una ampia discrezionalità, in rispetto della dottrina del margine di apprezzamento[478], nella scelta delle modalità

---

paragrafi 118 e 119 si può leggere « It is not disputed that mail, telephone and email communications, including those made in the context of business dealings, are covered by the notions of "private life" and "correspondence" in Article 8 § 1. The Court has consistently held in its case-law that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention (see, *inter alia*, *Klass and Others*, cited above, § 33; *N.C. v. Italy* [GC], no. 24952/94, § 56, ECHR 2002-X; and *Krone Verlag GmbH & Co. KG v. Austria (no. 4)*, no. 72331/01, § 26, 9 November 2006). However, in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has permitted general challenges to the relevant legislative regime».

[477] Corte europea dei diritti dell'uomo, sent. 25 giugno 1997, *Halford* c. *Regno Unito*, ricorso n. 20605/92, 25, al cui paragrafo 57 viene sottolineato che « However, the essence of Ms Halford's complaint, unlike that of the applicants in the Klass and Others case (cited above, p. 20, para. 38), was not that her Article 8 rights (art. 8) were menaced by the very existence of admitted law and practice permitting secret surveillance, but instead that measures of surveillance were actually applied to her. Furthermore, she alleged that the Merseyside police intercepted her calls unlawfully, for a purpose unauthorised by the 1985 Act (see paragraphs 26 and 53 above). In these circumstances, since the applicant's complaint concerns specific measures of telephone interception which fell outside the law, the Court must be satisfied that there was a reasonable likelihood that some such measure was applied to her».

[478] Com'è noto la dottrina del margine di apprezzamento è stata sviluppata per lo più dalla giurisprudenza della Corte EDU, ma si rinvengono sue applicazioni anche negli ordinamenti nazionali, ad esempio in Francia e in Germania, nonché nell'ambito di giurisdizioni internazionali, come la Corte Internazionale di Giustizia e nel sistema di risoluzione delle controversie del WTO (cfr. COT, *Margin of appreciation*, in *Max Planck Encyclopedia of Public International Law*, 2007). Tra le differenti definizioni che sono state fornite possiamo qui richiamare quella di Arai-Takahashi, secondo il quale il margine di apprezzamento può essere descritto «as the measure of discretion allowed to the Member States in the manner in which they implement the Convention standards, taking into account their own particular national circumstances and condition» (cfr. ARAI-TAKAHASHI, T*he defensibility of the margin of appreciation doctrine in the ECHR: value-pluralism in the European integration*, in *Revue*

di sorveglianza segreta sia della corrispondenza che delle telecomunicazioni, la sua attività è volta dunque a verificare che il sistema di sorveglianza prescelto sia tale da offrire garanzie adeguate ed effettive contro gli abusi, prendendo in considerazione la natura, l'ampiezza e la durata delle misure di sorveglianza, nonché, infine, le vie di ricorso offerte ai cittadini dall'ordinamento nazionale [479]. In secondo luogo – e sempre in

Européenne de Droit Public, 2001, pp. 1162 ss); o quella di Macdonald, per cui «the doctrine of margin of appreciation illustrates the general approach of the European Court of Human Rights to the delicate task of balancing the sovereignty of Contracting Parties with their obligations under the Convention» (MACDONALD, *The margin of appreciation in the jurisprudence of the European Court of Human Rights*, in *Collected Courses of the Academy of European Law*, 1992, p. 95 ss.). In breve dunque, e per quel che riguarda l'ambito della Convenzione Europea dei diritti dell'uomo, si può dire che la dottrina del margine di apprezzamento indica quello spazio lasciato agli Stati nell'applicazione della CEDU al fine di bilanciare il rispetto degli obblighi previsti dalla Convenzione con la tutela di ulteriori esigenze dello Stato.

[479] Riprendendo le parole della Corte, infatti, è possibile notare come «[t]he Court, in its appreciation of the scope of the protection offered by Article 8 (art. 8), cannot but take judicial notice of two important facts. The first consists of the technical advances made in the means of espionage and, correspondingly, of surveillance; the second is the development of terrorism in Europe in recent years. Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime. As concerns the fixing of the conditions under which the system of surveillance is to be operated, the Court points out that the domestic legislature enjoys a certain discretion. It is certainly not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field (cf., mutatis mutandis, the De Wilde, Ooms and Versyp judgment of 18 June 1971, Series A no. 12, pp. 45-46, para. 93, and the Golder judgment of 21 February 1975, Series A no. 18, pp. 21-22, para. 45; cf., for Article 10 para. 2, the Engel and others judgment of 8 June 1976, Series A no. 22, pp. 41-42, para. 100, and the Handyside judgment of 7 December 1976, Series A no. 24, p. 22, para. 48). Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate. The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds

linea generale – la Corte si è quasi sempre mostrata propensa ad accettare come causa di giustificazione la tutela della sicurezza nazionale. In questo modo dunque il suo sindacato si è spesso concentrato sulla legalità e la proporzionalità delle misure lesive della riservatezza [480].

È, infatti, oramai pacifico che ogni limitazione del diritto alla *privacy* debba essere prevista all'interno di una legge che sia sufficientemente accessibile, chiara e precisa al punto da rendere facilmente riconoscibili sia i soggetti autorizzati a porre in essere tali misure di sorveglianza sia le circostanze in cui questa attività può essere giustificata[481]. Da ciò dovrebbe conseguire che la disciplina in materia di sorveglianza da parte degli Stati (soprattutto con riferimento alla sorveglianza di cittadini stranieri) debba essere prevista in una fonte primaria, quale appunto la legge, e non invece in atti del potere esecutivo. Ciononostante va rilevato che un numero sempre crescente di Stati sembra muoversi esattamente nella direzione opposta, inserendo la regolazione delle attività di

required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law. The functioning of the system of secret surveillance established by the contested legislation, as modified by the Federal Constitutional Court's judgment of 15 December 1970, must therefore be examined in the light of the Convention». Cfr. Corte europea dei diritti dell'uomo, sent. 6 settembre 1978, *Klass and others v. Germany*, ricorso n. 5029/71, para. 48-50.

[480] Com'è noto, e per quanto attiene alla legalità, le misure di sorveglianza devono fondarsi su una base legale che sia accessibile ai consociati e che sia capace di assicurare la prevedibilità delle misure applicabili. Quando si parla di base legale si far riferimento sia alle fonti legislative e regolamentari, sia alla giurisprudenza nazionale pertinente. Inoltre, la legge deve determinare i presupposti per l'adozione delle misure di sorveglianza soprattutto con riferimento ai potenziali destinatari. Tuttavia, se da un lato non è necessario che la persona intercettata venga informata delle misure a suo carico (il che farebbe venir meno l'utilità stessa della misura), è altrettanto vero che, almeno in linea di principio, la stessa sia informata una volta che l'intercettazione sia finita. E ciò principalmente per permettere al soggetto interessato di poter contestare la legalità della misura. Cfr. BARTOLE, DE SENA, ZAGREBELSKY, *op.cit.*, p. 357.

[481] LUBIN, *We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the practice of Foreign Mass Surveillance*, in *Chicago Journal of International Law*, 2018, p. 542.

sorveglianza all'interno di atti emanati dal governo piuttosto che in fonti normative [482].

Ebbene, se da un lato tali principi sono senz'altro applicabili a tutte le ipotesi in cui si parli di sorveglianza di massa, dall'altro lato è innegabile che quando si è dinanzi a casi di sorveglianza di soggetti stranieri gli effetti e le considerazioni in materia di legalità subiscano delle declinazioni differenti[483]. E ciò perché non si può presumere che i soggetti potenzialmente sottoposti alla sorveglianza di un altro Stato sappiano dove rinvenire la normativa del paese straniero che pretende di spiarli. Né, allo stesso tempo, si dovrebbe supporre che siano in grado di leggere la lingua in cui è probabile che tale legislazione sia stata scritta. Di conseguenza, se il solito standard di 'accessibilità' nel contesto della sorveglianza interna è semplicemente la diffusione della legge «in una pubblicazione generalmente accessibile in modo ufficiale» dello Stato, ciò potrebbe rivelarsi insufficiente nel contesto della sorveglianza straniera [484].

[482] Quanto qui affermato è possibile desumerlo attraverso le parole usate nel *Report* dal titolo *The Right to Privacy in the Digital Age*, ove al paragrafo 29 è possibile leggere: «[c]onsequently, secret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn, demands greater precision in the rule governing the exercise of discretion, and additional oversight. Several States also require that the legal framework be established through primary legislation debated in parliament rather than simply subsidiary regulations enacted by the executive – a requirement that helps to ensure that the legal framework is not only accessible to the public concerned after its adoption, but also during its development, in accordance with article 25 of the International Covenant on Civil and Political Rights».

[483] LUBIN, *op.cit.*, p. 542.

[484] In dottrina, per far fronte a queste difficoltà, è stato suggerito agli Stati «to translate their laws to multiple languages, advertise their legislation in particularly vulnerable countries and to particularly vulnerable groups, and make it accessible to specialized advocacy groups (such as digital rights NGOs who can further scrutinize and challenge the country's foreign surveillance practices). In this regard a human rights tailored framework for foreign

A fronte di tali problematiche e al fine chiarire il modo in cui l'art. 8 CEDU deve essere declinato per affrontare i casi di sorveglianza di massa – e anche di sorveglianza nei confronti di soggetti stranieri – la Corte EDU ha elaborato sei *standard* minimi di salvaguardia da introdurre nell'impianto normativo degli Stati membri al fine di evitare abusi di potere da parte degli stessi. Secondo quanto affermato dalla Corte, nella decisione relativa al caso *Weber e Saravia* c. *Germania*, la legislazione in materia di sorveglianza dovrebbe indicare: *i)* la natura dei reati che possono dar luogo ad un ordine di intercettazione; *ii)* una definizione delle categorie di persone che possono essere soggette a intercettazioni dei loro telefoni; *iii)* l'indicazione di un limite massimo di durata; *iv*) la procedura da seguire per l'esame, l'utilizzo e la memorizzazione dei dati ottenuti; *v)* le precauzioni che devono essere adottate quando si ha intenzione di comunicare i dati ottenuti ad altre parti; e, infine, *vi)* le circostanze in cui le registrazioni possono ovvero debbano essere cancellate [485].

Come è facile intuire, nonostante l'indicazione da parte della Corte di tali standard di salvaguardia, che dovrebbero certamente far parte di qualsiasi regime in materia di sorveglianza, e che rappresentano senz'altro dei principi di carattere generale, non sono mancati nella prassi previsioni divergenti rispetto a quanto generalmente indicato dalla Corte. Il

surveillance might set a higher, not a lower, standard for "accessibility" than its domestic counterpart». Cfr. *Ibidem*, p. 543.

[485] Si riportano per completezza le parole utilizzate dalla Corte: «[t] he Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)». Cfr. Corte europea dei diritti dell'uomo, sent. 29 giugno 2006, *Weber and Saravia* c. *Germania*, ricorso n. 54934/00, par. 95.

riferimento va essenzialmente alla disciplina prevista dal Regno Unito in materia di intercettazioni [486] e in particolare al già citato *Investigatory Powers Act*. Quest'ultimo infatti contiene una lista di 'motivi' per cui è possibile ottenere i dati contenuti nelle comunicazioni:

a) in the interest of national security, *b*) for the purpose of preventing or detecting crime or of preventing disorder, *c*) in the interest of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security, *d*) in the interests of public safety, *e*) for the purposes of protecting public health, *f*) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department, *g*) for the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health, *h*) to assist investigations into alleged miscarriages of justice [487].

Il riferimento alla disciplina inglese non è casuale. Quanto in essa previsto infatti rileva non solo per quanto riguarda la sorveglianza individuale o di massa generalmente intesa, che è stata spesso oggetto di scrutinio da parte della Corte, ma appare altresì rilevante per una specifica

[486] Non mancano invero ulteriori casi degni di nota. Il riferimento va, in particolare, alla legislazione francese che ha introdotto nel marzo del 2015, a seguito del caso *Charlie* Hebdoo, la controversa disciplina in materia di intercettazioni (cd. *Intelligence Act*). Senonché qualche mese più tardi il governo francese ha adottato un secondo atto (cd. *International Intelligence Act*), in aggiunta alla precedente, in cui viene disciplinata in maniera più dettagliata sorveglianza di soggetti stranieri. I punti controversi della nuova disciplina riguardano principalmente l'estensione dei poteri del governo francese in materia di *Intelligence* e del mantenimento della sicurezza nazionale. Più nel dettaglio, la nuova disciplina prevede una diversificazione tra la sorveglianza dei cittadini francesi e quella dei cittadini stranieri. Per dare una indicazione più concreta, si può pensare ai diversi termini di archiviazione del materiale intercettato che, per quanto riguarda i cittadini francesi, ammonta a trenta giorni, mentre per gli stranieri fino ad un massimo di quattro anni. Cfr. KITTICHAISAREE, *Public International Law of Cyberspace*, Berlino, 2017, p. 95 ss.

[487] Cfr. *Investigatory Powers Act*, 2016, consultabile online al seguente indirizzo http://www.legislation.gov.uk

pratica che per la prima volta è stata presa in considerazione dai Giudici di Strasburgo in un recente caso (*Big Brothers Watch e altri c. Regno Unito*) che sarà da qui a breve oggetto della nostra analisi.

Si tratta della cd. *Intelligence sharing*, ossia uno dei possibili modi con cui due o più Stati possono cooperare per favorire lo scambio e/o l'analisi delle informazioni in loro possesso al fine di far fronte a questioni attinenti alla sicurezza e alla difesa nazionale [488]. Le informazioni e i dati che gli Stati possono condividere e scambiarsi varia a seconda di quanto stabilito di volta in volta negli specifici accordi stipulati.

In linea generale, tuttavia, è possibile distinguere tre diverse tipologie di informazioni: le informazioni strategiche, le informazioni operative e le informazioni tattiche.

Analizzando sommariamente le tre diverse tipologie è possibile inquadrare nel novero della prima categoria (informazioni strategiche) quelle relative alle valutazioni degli sviluppi di politica estera, degli ambienti di sicurezza e delle tendenze generali relative alla minaccia di proliferazioni di armi di distruzione di massa oppure a movimenti di estrema destra. Tali valutazioni sono volte per lo più ad informare i responsabili politici di uno Stato, in particolare gli addetti al settore dell'*Intelligence* ed esse, nonostante siano informazioni classificate, non rivelano informazioni particolarmente sensibili e possono pertanto esser più ampiamente condivise [489].

Nel secondo gruppo di informazioni, invece, si fanno generalmente rientrare quelle relative alle capacità e al *modus operandi* di specifiche forze armate, di gruppi non appartenenti all'organizzazione dello Stato o agli individui considerati una minaccia per la sicurezza nazionale. Le

[488] BORN, LEIGH, WILLS, *Making International Intelligence Cooperation Accountable*, DCAF, 2015, p. 18 ss.

[489] *Ibidem*, p. 18.

informazioni operative comprendono altresì valutazioni delle minacce relative ai Paesi terzi, alla sicurezza delle missioni diplomatiche e agli individui che intendono viaggiare in quel determinato Paese [490]. Tali informazioni, a differenza delle precedenti, sono particolarmente rilevanti per gli esperti di sicurezza, mentre hanno un peso minore per i responsabili politici [491].

Infine, le *informazioni tattiche* sono quelle che rivelano dettagli sull'identità, la posizione, le attività e gli obiettivi di specifiche persone coinvolte in operazioni terroristiche o militari. Queste informazioni sono rilevanti in quanto permettono di rispondere a tutti gli interrogati connessi all'azione che in quel momento si sta perpetrando (sul chi, cosa, dove, quando e come). In un contesto non militare invece le informazioni possono riguardare i movimenti di un sospetto terrorista oppure di un soggetto appartenente a gruppi criminali organizzati. Questa categoria è certamente quella che contiene le informazioni più sensibili in quanto capaci di compromettere, in caso di loro rivelazione, il successo o meno di una determinata operazione, nonché la sicurezza delle persone coinvolte. Di conseguenza, esse sono normalmente condivise con un numero ridotto di soggetti[492].

Così individuate le informazioni che possono essere condivise, è necessario identificare il *modo* in cui ciò avviene. Anche in questo caso è possibile individuare almeno tre diverse modalità. La prima riguarda l'accesso alle informazioni cd. grezze (*raw*) – e cioè quelle informazioni non ancora analizzate come ad esempio il traffico internet intercettato dai cavi ottici che 'trasportano' le informazioni – da parte di altri governi[493].

[490] *Ibidem*, p. 18-19.

[491] *Ibidem*, p. 19.

[492] *Ibidem*.

[493] Privacy international, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, 2018, p. 5.

La seconda invece mira ad accedere alle informazioni archiviate in *database* gestiti da un altro Stato oppure co-gestiti da diversi Stati[494]. Infine, l'ultima modalità si verifica allorquando uno Stato riceva da un altro i risultati dell'analisi delle informazioni intercettate, ad esempio attraverso un *Intelligence Report*[495].

Come si può agevolmente notare, tutte le forme qui considerate di *Intelligence sharing* sollevano non pochi dubbi circa la loro compatibilità con il diritto alla *privacy* e con altri diritti umani. È altrettanto agevole constatare come i rischi siano ancora più acuti allorquando uno Stato possa direttamente avere accesso alle informazioni acquisite oppure archiviate da un altro Paese. L'incremento di tale rischio va di pari passo con l'aumento della sorveglianza di massa e dalle condotte poste in essere dalle agenzie di *intelligence* degli Stati.

Non è un caso infatti che, nonostante questa pratica sia utilizzata oramai da diversi anni, è solo di recente che anche le Corti sovranazionali e segnatamente la Corte EDU si sia iniziata a preoccupare della questione.

È proprio in questo clima che si inserisce la complessa vicenda che ha dato luogo alla sentenza *Big Brother Watch e altri c. Regno Unito*, decisione in cui per la prima volta, almeno secondo le parole dei Giudici, la Corte si è pronunciata sul problema di cui si sta dibattendo. Data la rilevanza della questione, dimostrata anche dal rinvio alla Grande Camera, nel paragrafo seguente si prenderanno le mosse proprio dalla sentenza citata.

4. La sentenza sul caso Big Brother Watch e altri c. Regno Unito

[494] *Ibidem*.
[495] *Ibidem*.

La citata sentenza, *Big Brother Watch*, come anticipato, appare particolarmente complessa e non priva di criticità. Sebbene non sia questo il luogo per approfondire gli aspetti fattuali della vicenda, una breve descrizione può essere d'ausilio per il prosieguo della nostra analisi.

Il giudizio istauratosi dinanzi alla Corte EDU riunisce tre diversi gruppi di ricorrenti composti da aziende, organizzazioni no-profit e individui impegnati sul fronte delle libertà civili o - come nel caso del secondo gruppo - nel mondo giornalistico[496]. Essi lamentano, in ragione delle proprie attività lavorative, che il Regno Unito abbia *i)* intercettato le comunicazioni elettroniche attraverso i propri servizi di *intelligence*; *ii)* ottenuto le intercettazioni da un governo straniero; e, infine, *iii)* ricevuto il materiale intercettato dai fornitori dei servizi di comunicazione[497].

Nel Regno Unito il regime delle intercettazioni è disciplinato in tre diverse fonti, alcune normative altre di natura pattizia. Quanto alla disciplina per le intercettazioni di massa, essa è contenuta nella sezione 8(4) del *Regulation of Investigatory Act* (RIPA), la quale prevede che il Segretario di Stato possa emettere un mandato per intercettare determinate comunicazioni[498]. Tale mandato inoltre deve essere coadiuvato da una

[496] Corte europea dei diritti dell'uomo, sent. 13 settembre 2018, *Big Brother Watch e altri* c. *Regno Unito*, ricorso n. 58170/13, 62322/14 e 24960/15, par. 7-8.

[497] *Ibidem*.

[498] *Ibidem*. Secondo la sezione 8 del RIPA, che si riporta per una maggiore chiarezza, «8. - (1) An interception warrant must name or describe either- (a) one person as the interception subject; or (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place. (2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted. […] (4) Subsections (1) and (2) shall not apply to an interception warrant if- (a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and (b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying- (i) the descriptions of intercepted material the examination of which he considers necessary; and (ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c)». Per una interessante analisi

descrizione dei motivi necessari (ad esempio, sicurezza nazionale, prevenire o individuare gravi reati o salvaguardare il benessere economico del Regno Unito) affinché il materiale possa essere successivamente esaminato. Relativamente invece alla disciplina sulla procedura di condivisione dei servizi di *intelligence*, viene in rilevo l'accordo bilaterale tra Regno Unito e Stati Uniti denominato *British-US Communication Intelligence Agreement*. Secondo l'accordo le autorità britanniche e statunitensi si impegnano a condividere l'uno con l'altro tutto quel materiale intercettato che provenga da paesi stranieri, e più in generale da paesi esterni al Commonwealth[499]. Infine, la disciplina in materia di acquisizione del materiale intercettato dai fornitori di servizi di comunicazione è prevista dal secondo capitolo del RIPA. In particolare, secondo la sezione 22 del capitolo[500], l'autorizzazione per l'acquisizione

relativa al RIPA si veda AKDENIZ, TAYLOR, WALKER, *Regulation of Investigatory Powers Act* 2000 (1): *Bigbrother.gov.uk: State Surveillance in the age of Information and Rights*, in *Criminal Law Review*, 2001, p. 73 ss.

[499] *Big Brother Watch e altri* c. *Regno Unito*, p. 36.

[500]Anche in questo caso per una maggiore comprensione del problema se ne riporta integralmente il testo « (1) This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data. (2) It is necessary on grounds falling within this subsection to obtain communications data if it is necessary- (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic well-being of the United Kingdom; (d) in the interests of public safety; (e) for the purpose of protecting public health; (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

(3) Subject to subsection (5), the designated person may grant an authorisation for persons holding offices, ranks or positions with the same relevant public authority as the designated person to engage in any conduct to which this Chapter applies.

(4) Subject to subsection (5), where it appears to the designated person that a postal or telecommunications operator is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice to the postal or telecommunications operator, require the operator- (a) if the operator is not already in possession of the data, to

dei dati deve provenire da una specifica persona, individuata dal Segretario di Stato, e appartenente alle autorità pubbliche competenti. L'autorizzazione può essere concessa a persone facenti parte alla medesima autorità ovvero può, previa notifica ai fornitori di servizi, avere ad oggetto la divulgazione di materiale già in loro possesso o, infine, può essere volta ad ottenere e a divulgare i dati.

Ebbene, tutti e tre i gruppi di ricorrenti lamentavano che il sistema di intercettazioni di massa, la condivisione dei servizi di intelligence (cd. *Intelligence sharing*) e l'acquisizione dei dati dai gestori di comunicazioni erano contrarie all'art. 8 CEDU e – su richiesta del secondo gruppo di ricorrenti - all'art. 10 CEDU [501].

La sentenza non rappresenta di certo la prima nel suo genere, almeno per quanto concerne il regime relativo alla compatibilità delle misure di sorveglianza di massa e l'art. 8 CEDU [502]. Discorso parzialmente diverso,

---

obtain the data; and (b) in any case, to disclose all of the data in his possession or subsequently obtained by him.

(5) The designated person shall not grant an authorisation under subsection (3), or give a notice under subsection (4), unless he believes that obtaining the data in question by the conduct authorised or required by the authorisation or notice is proportionate to what is sought to be achieved by so obtaining the data.

(6) It shall be the duty of the postal or telecommunications operator to comply with the requirements of any notice given to him under subsection (4).

(7) A person who is under a duty by virtue of subsection (6) shall not be required to do anything in pursuance of that duty which it is not reasonably practicable for him to do.

(8) The duty imposed by subsection (6) shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(9) The Secretary of State shall not make an order under subsection (2)(h) unless a draft of the order has been laid before Parliament and approved by a resolution of each House».

[501] La questione relativa all'art. 10 CEDU non sarà parte della nostra indagine, che si limiterà ad alcune riflessioni in merito al rapporto con l'art. 8 della Convenzione.

[502]Oltre ad un precedente abbastanza datato (*Klass and Others* c. Germania,1978), la Corte a partire dal 2006 ha affrontato non pochi casi relativi all'oggetto *de quo*. Si pensi, ad esempio, al già citato *Weber and Saravia* c. *Germania* (2006), oppure ai casi *Liberty and Others* c. *Regno Unito* (2008), *Kennedy* c. *Regno Unito* (2010), *Roman Zakharov* c. *Russia* (2015), *Szabò and Vissy* c. *Ungheria*, (2016), *Centrum for Rattvisa* c. Svezia (2018). Questo ultimo è stato rinviato alla Grande Camera nel febbraio del 2019 e tuttora non è ancora stato deciso.

invece, va fatto per quanto riguarda il sistema di *Intelligence sharing* e la sua compatibilità con la Convenzione.

Data la rilevanza di ambedue le questioni, si procederà dapprima ad una breve analisi in merito alla disciplina della sorveglianza di massa e poi successivamente si analizzerà la questione dell'*intelligence sharing.*

4.1. La questione della sorveglianza di massa

Come anticipato la sentenza in oggetto non è la prima decisione della Corte in merito al regime della sorveglianza di massa nei Paesi europei. Dopo la già richiamata sentenza *Weber and Saravia* c. *Germania* sono state diverse le occasioni in cui la Corte ha affrontato il problema, tant'è che in dottrina si è parlato di un approccio 'progressivo' alla protezione del diritto alla *privacy* in contrasto con il sempre crescente interesse da parte degli Stati di raccogliere dati ed informazioni dei cittadini[503].

Tale qualificazione 'progressista' deriva essenzialmente da due ordini di ragioni. In primo luogo perché tale approccio si basa su decisioni vincolanti a dispetto della grande quantità di atti di *soft law* emanati dagli organi della Nazioni Unite e, in secondo luogo, perché la tutela per la prima volta è garantita a prescindere dal mezzo di telecomunicazione in uso, in contrasto con il concetto di '*reasonable expectations of privacy*' utilizzato per lo più negli Stati Uniti[504].

Senonché, nonostante questo approccio, va rilevato come nella sentenza *Big Brother Watch*, la Corte, riconoscendo la compatibilità *tout court* della

[503]Così RUSINOVA, *A European Perspective on Privacy and Mass Surveillance at the Crossroads*, in *Higher School of Economics Research Paper*, 2019, p. 3.

[504]*Ibidem*; Sul tema della *Reasonable Expectations of Privacy* si rimanda, tra tutti, SLOBOGIN, SCHUMACHER, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: an Emipiricla look at 'Understandings Recognized and Permitted by Society*, in *Duke Law Journal*, 1993, p. 727 ss.

sorveglianza di massa con la Convenzione, abbia deciso di fare un passo indietro.

Il punto di partenza dell'evoluzione giurisprudenziale della Corte è senz'altro rappresentato dalla decisione sull'ammissibilità del caso *Weber and Saravia*. La Corte ha esaminato la legislazione tedesca in materia di *strategic monitoring*, riconoscendo l'uso della sorveglianza di massa come misura di carattere generale al fine di individuare ed evitare pericoli per la Repubblica federale tedesca (ad esempio per far fronte ad attacchi armati oppure atti di terrorismo internazionale[505]). Nonostante i Giudici di Strasburgo abbiano deciso per la non violazione dell'art. 8 CEDU, rigettando la domanda in quanto infondata, essi hanno individuato una serie di criteri da utilizzare per determinare la legittimità delle misure di sorveglianza[506].

Le conclusioni a cui giunge la Corte sono state confermate anche nel successivo caso *Liberty and Others c. Regno Unito*. In quella occasione, i Giudici si sono trovati ad esaminare la compatibilità dell'art. 8 CEDU con l'intercettazione di massa di comunicazioni effettuate tramite telefono, fax ed email[507], ed espressamente affermavano che loro «does not consider that there is any ground to apply different principles concerning the

[505] Cfr. *Weber and Saravia* c. *Germania*, par. 95, ove inoltre la Corte aggiunge «[i]t notably concerns the extension of the powers of the Federal Intelligence Service (*Bundesnachrichtendienst*) with regard to the recording of telecommunications in the course of so-called strategic monitoring, as well as the use (*Verwertung*) of personal data obtained thereby and their transmission to other authorities. Strategic monitoring is aimed at collecting information by intercepting telecommunications in order to identify and avert serious dangers facing the Federal Republic of Germany, such as an armed attack on its territory or the commission of international terrorist attacks and certain other serious offences (see "Relevant domestic law and practice" below, paragraphs 18 et seq.). In contrast, so-called individual monitoring, that is, the interception of telecommunications of specific persons, serves to avert or investigate certain grave offences which the persons monitored are suspected of planning or having committed».

[506] I criteri sono stati già descritti nel corso di questo lavoro, per una loro lettura si rimanda quindi a p. 168 ss.

[507] *Liberty and Others* c. *Regno Unito*, parr. 5 ss.

accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other»[508].

In ambedue le decisioni dunque è possibile notare come la Corte nell'analizzare la compatibilità dei sistemi di sorveglianza con l'art. 8 CEDU non faccia alcun riferimento alla necessità che vi sia un 'ragionevole sospetto' nei confronti dei soggetti sottoponibili ad intercettazioni, riconoscendo invece una ampia possibilità agli Stati di utilizzare i sistemi di sorveglianza [509].

Proprio in ragione di questa carenza, un primo passo in avanti viene fatto in occasione della decisione relativa al caso *Roman Zakharov c. Russia* in cui la Grande Camera per la prima volta applica il criterio del «ragionevole sospetto» in materia di sorveglianza.

I Giudici di Strasburgo infatti affermano che il sistema legislativo russo non preveda la necessità di una autorizzazione *ex ante* da parte di un Giudice interno, la cornice normativa riconosce piuttosto al governo una discrezionalità quasi illimitata, che gli consente di sorvegliare tutti i telefoni cellulari che utilizzano un operatore telefonico nazionale, aumentando così notevolmente la possibilità di abusi da parte dello Stato[510].

Ed è proprio in materia di autorizzazione che i giudici di Strasburgo ritengono che vada applicato il criterio del 'ragionevole sospetto',

[508] *Ibidem*, par. 63.

[509] RUSINOVA, *op.cit.*, p. 5.

[510] *Roman Zakharov* c. *Russia*, par. 248, nel quale la Grande Camera specifica «It is significant that the OSAA does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse (…)».

precisando che vada utilizzato solo nei confronti di coloro che hanno commesso o hanno partecipato alla pianificazione di atti criminosi, nonché nei confronti di quegli individui che possono minare la sicurezza nazionale[511]. Senonché, a fronte di tale precisazione, essi ritengono che le Corti russe non hanno gli elementi necessari per valutare se vi sia un ragionevole sospetto avverso un determinato soggetto e di conseguenza va criticata la prassi di sottoporre a sorveglianza un'intera zona territoriale, indipendentemente dai soggetti coinvolti[512].

Il ragionamento seguito dalla Grande camera è stato altresì applicato in modo non dissimile dalla quarta sezione nel caso *Szabò and Vissy* c. *Ungheria*[513]. Secondo il pensiero della Corte, la legislazione ungherese, sebbene non facesse espressa menzione alla disciplina della sorveglianza di massa, individuava i soggetti sottoponibili a sorveglianza con un generico 'range of persons', il che significava riconoscere allo Stato la possibilità di sorvegliare un nutrito gruppo di cittadini senza che fosse necessario per le autorità statali alcun tipo di *target* specifico[514]. Questo aspetto, a parere della quarta sezione, era assolutamente contrario alle garanzie previste dall'art. 8 CEDU e in particolare al principio della 'stretta necessità', il quale dispone, secondo l'interpretazione dei Giudici, che per individuare un gruppo di persone sottoponibili a sorveglianza è necessario un *sospetto individuale* che sia suffragato dalla giusta quantità di materiale probatorio[515].

Infine, i giudici di Strasburgo tengono a precisare che la sorveglianza segreta è compatibile con la Convenzione solo allorquando questa sia

[511] *Ibidem*, par. 260.
[512] *Ibidem*, par. 265.
[513] Per la ricostruzione della questione fattuale si rimanda alla sentenza dai paragrafi 6-15.
[514] *Szabò and Vissy* c. *Ungheria*, par. 67.
[515] *Ibidem*, par. 71.

strettamente necessaria al fine di salvaguardare l'assetto democratico dello Stato[516].

Come si è avuto modo di notare, la Corte, negli ultimi anni e nonostante il riconoscimento di alcune forme di sorveglianza come lecite, ha sviluppato un cospicuo numero di garanzie avverso i possibili abusi da parte delle autorità statali, accrescendo così in modo graduale la fiducia di tutela nei suoi confronti[517].

Senonché, come si cercherà di dimostrare da qui a breve, dopo le ultime due pronunce della Corte (Corte (*Centrum for Rattvisa* e *Big Brother Watch*) tali garanzie hanno subito una battuta d'arresto.

E, infatti, nel caso *Big Brother Watch,* la Corte, chiamata a rispondere ancora una volta sulla compatibilità delle misure di sorveglianza di massa adoperate nel Regno Unito con la Convezione, ha riproposto il ragionamento utilizzato nella precedente decisione *Centrum for Rattvisa*. Gli argomenti centrali di entrambe le decisioni ruotano intorno al riconoscimento agli Stati di un ampio margine di apprezzamento per l'introduzione di un regime di intercettazioni e sorveglianza di massa al fine di proteggere la propria sicurezza nazionale[518]. In altre parole, l'approccio utilizzato dalla Corte si basa, da un lato, sul riconoscimento dell'ammissibilità del regime di sorveglianza di massa di *per sé*

[516] *Ibidem*, par. 73. La Corte inoltre al paragrafo 81 precisa che « (…) where situations of extreme urgency are concerned, the law contains a provision under which the director of the service may himself authorise secret surveillance measures for a maximum of 72 hours (see sections 58 and 59 of the National Security Act quoted in paragraph 17 above). For the Court, this exceptional power should be sufficient to address any situations in which external, judicial control would run the risk of losing precious time. Such measures must however be subject to a *post factum* review, which is required, as a rule, in cases where the surveillance was authorised *ex ante* by a non-judicial authority».

[517] RUSINOVA, *op.cit.*, p. 7.

[518] *Big Brother Watch and others* c. *Regno Unito*, par. 315 e 329; *Centrum for Rattvisa* c. *Svezia*, par. 113.

considerato e, dall'altro lato, sulla applicazione al caso di specie dei criteri della 'necessità in una società democratica' e 'della proporzionalità'[519].

Tale atteggiamento involutivo si evince poi in un altro passaggio della sentenza. Più precisamente in occasione della richiesta di aggiornamento degli standard di garanzia fissati nel caso *Weber and Saravia*[520], e cioè attraverso l'adozione sia del requisito del 'ragionevole sospetto' – basato su prove oggettive – che della notificazione *ex post* al soggetto interessato.

Secondo la Corte, tuttavia, l'introduzione di questi due nuove *standard* sarebbe in netto contrasto con il principio secondo cui in materia di sorveglianza di massa allo Stato è riconosciuto un ampio margine di apprezzamento[521]. Inoltre, essendo il regime di intercettazione di massa per sua stessa definizione non mirato, l'introduzione del criterio del 'ragionevole sospetto' avrebbe creato una incongruenza non superabile all'interno del sistema ([522]). Analogamente, la successiva notificazione ai soggetti interessati presuppone l'esistenza di individui ben individuati il ché, anche in questo caso, si contrappone all'essenza stessa e all'effettività del regime di sorveglianza di massa[523].

Ragionevolmente, la base per tale *update* sarebbe inquadrabile nel maggiore grado di intrusione operabile attraverso i più recenti strumenti informatici capaci di definire in modo ancor più preciso aspetti della vita privata degli individui e i loro comportamenti[524]. Nonostante la Corte non sia del tutto contraria a questo assunto, essa tiene a precisare che l'automatica analogia per cui la sorveglianza di massa odierna sia maggiormente intrusiva rispetto a quella utilizzata in passato non è

[519] *Ibidem*, par. 315.
[520] Si veda sopra p.168 ss.
[521] *Centrum for Rattvisa* c. *Svezia,* par. 317.
[522] *Ibidem*.
[523] *Ibidem*.
[524] *Ibidem*, par. 316.

condivisibile[525], e pertanto non vi è necessità di aggiornare i criteri stabiliti più di dieci anni prima.

A ben vedere, i giudici di Strasburgo sembrano non solo aver compiuto una battuta di arresto, ma addirittura aver fatto un passo indietro rispetto al recente passato, e ciò almeno per tre ordini di ragioni.

In primo luogo, per quanto riguarda l'applicabilità dei sei criteri minimi di salvaguardia, l'affermazione secondo cui la sorveglianza di massa in sé appare compatibile con la Convenzione – e in particolare con l'art. 8 – elimina automaticamente la necessità dei primi due requisiti stabiliti per mettere in atto misure di sorveglianza (e cioè la natura dell'offesa per emanare un ordine di intercettazione e la definizione della categoria di persone che possono essere sottoposti ad intercettazione), lasciando così solo quattro delle sei garanzie precedentemente previste.

In secondo luogo, in merito alla notificazione *ex post*, i giudici di Strasburgo sembrano contraddirsi con diversi precedenti in cui perentoriamente affermavano che «subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and, hence, to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively'; and that a notification should be carried out as soon as it does not jeopardize the purpose of these measures»[526].

Infine, seguendo un ragionamento parzialmente diverso, ma giungendo al medesimo risultato, i giudici di Strasburgo sembrano aver fatto un passo indietro anche rispetto alla imperativa previsione che aveva fino ad ora

[525] *Ibidem*.

[526] *Weber and Saravia* c. *Germania*, para. 135; *Szabò and Vissy* c. *Ungheria*, par. 86.

caratterizzato il sistema della sorveglianza di massa, e cioè la necessaria e preventiva autorizzazione giudiziale al fine di procedere. Se infatti precedentemente la Corte aveva definito l'autorizzazione come un «important safeguard against arbitrariness»[527], oggi la stessa ritiene che l'autorizzazione non è necessaria per la compatibilità con l'art. 8 CEDU, ma al più può essere considerato un esempio di buona prassi[528].

Nonostante le evidenziate criticità e - potremmo dire - l'involuzione di alcune garanzie riconosciute dalla Corte EDU, alcuni autori hanno accolto con parziale entusiasmo la sentenza in esame[529], in ragione di alcuni aspetti innovativi rispetto ai precedenti della Corte.

Tra questi aspetti rientra anzitutto l'assimilazione, già riconosciuta dall'Alto Commissario per i diritti umani, tra il contenuto delle informazioni intercettate e i cd. *metadata*[530]. Secondo la Corte, infatti, l'acquisizione di questa tipologia di dati non è da ritenere meno invasiva rispetto all'acquisizione del contenuto delle informazioni[531], e ciò in quanto attraverso i metadati è possibile ottenere informazioni come l'uso dei social network, la specifica posizione, l'uso di internet, tutti elementi che messi insieme possono disegnare un profilo dettagliato dell'individuo[532].

Senonché anche in questo caso una più attenta riflessione dimostra come tale estensione di protezione presenti in realtà almeno una forte

[527] *Roman Zakharov c. Russia*, par. 249.

[528] *Big Brother Watch and others*, par. 319-320.

[529] Si veda, ad esempio, MILANOVIC, *EctHR Judgment in Big Brother Watch v. UK*, in *EJIL:Talk! Blog of the European Journal of International Law*, 17 settembre 2018, consultabile online al seguente indirizzo https://www.ejiltalk.org/ecthr-judgment-in-big-brother-watch-v-uk/

[530] Va precisato che Corte non usa il termine *metadati*, ma si riferisce più genericamente a «related communications data». Per una breve definizione del termine, e relativamente a quanto sostenuto nella risoluzione dell'Assemblea Generale, si rimanda a pag. 7

[531] *Big Brother Watch and others* c. *Regno Unito*, par. 356

[532] *Ibidem*.

criticità che determina, in ultima analisi, l'assenza di una progressiva tutela del diritto alla privacy. Il passaggio mancante della Corte, e cioè la mancata applicazione alle intercettazioni dei *metadata* dei criteri minimi di garanzia creati nel caso *Weber and Saravia*, sta a significare che l'equiparazione tra le due tipologie di dati è tale solo in via di premessa, ma poi nella sostanza gli stessi vengono trattati in maniera difforme.

4.2. La questione dell'*intelligence sharing*

L'altro elemento di novità è rappresentato dall'analisi sulla compatibilità della Convenzione – e in particolare dell'art.8 – con l' *Intelligence sharing*[533].

La questione si riconduce seppur indirettamente alle rivelazioni del caso *Snowden*, di cui si è già parlato in precedenza, e in particolare sulla condivisione di informazioni tra il governo britannico e quello statunitense attraverso le rispettive agenzie di *Intelligence* (segnatamente, la GCHQ e la NSA). La Corte, trovandosi ad analizzare compiutamente il problema per la prima volta, ha anzitutto operato una differenziazione circa le modalità attraverso cui le informazioni sono state ottenute e/o scambiate, individuando tre categorie. La prima riguarda il materiale che la NSA ha fornito al Regno Unito senza che quest'ultimo lo avesse richiesto; la seconda, invece, concerne le comunicazioni che i servizi di intelligence

[533] Secondo la Corte, infatti, «[t]his is the first time that the Court has been asked to consider the Convention compliance of an intelligence sharing regime. While the operation of such a scheme might raise a number of different issues under the Convention, in the present case the applicants' complaints focus on the Article 8 compliance of the regime by which the United Kingdom authorities request and receive intelligence from foreign Governments. The applicants do not complain about the transfer of intelligence from the United Kingdom intelligence services to foreign counterparts; nor do they invoke any other Convention Articles». Cfr. *Ibidem*, par. 416.

britannici hanno chiesto alla NSA di intercettare; e infine il materiale, diverso dalle intercettazioni, ottenuto dalla NSA[534].

Nello svolgere tale analisi, e trattandosi pur sempre di una modalità di intercettazione dei dati seppur tra due diversi Stati, la prima sezione si è soffermata esclusivamente sulla seconda categoria, differenziando le ipotesi in cui l'intercettazione sia stata posta in essere autonomamente dagli Stati Uniti indipendentemente dalle richieste del governo britannico e il caso in cui invece lo Stato convenuto abbia chiesto agli Stati Uniti di intercettare e raccogliere informazioni[535].

Seguendo il ragionamento della camera, la prima ipotesi non determinerebbe alcuna violazione della Convenzione poiché la condotta (di intercettazione dei dati), essendo stata posta in essere da uno Stato straniero, sarebbe attribuibile al Regno Unito solo allorquando le agenzie di *intelligence* straniere avessero agito sotto l'autorità o il controllo dello Stato convenuto[536], richiamando a tal proposito l'art. 6 del Progetto di Articoli sulla Responsabilità degli Stati[537].

La Corte precisa poi che anche laddove lo Stato convenuto avesse 'richiesto' le informazioni, l'attività di intercettazione sarebbe in ogni caso non attribuibile al Regno Unito poiché il comportamento è da ricondurre

[534]Su questo aspetto la Corte al paragrafo 449 precisa che «The third category of material identified at paragraph 417 above is material obtained by foreign intelligence agencies other than by the interception of communications. However, as the applicants have not specified the kind of material foreign intelligence agencies might obtain by methods other than interception they have not demonstrated that its acquisition would interfere with their Article 8 rights. As such, the Court considers that there is no basis upon which it could find a violation of Article 8 of the Convention».

[535] *Ibidem*, par. 417.

[536] *Ibidem*, par. 420.

[537] Secondo il citato articolo, rubricato 'Comportamento di organi messi a disposizione di uno Stato da parte di un altro Stato, «[i]l comportamento di un organo messo a disposizione di uno Stato da parte di un altro Stato sarà considerato un atto del primo Stato ai sensi del diritto internazionale se tale organo agisce nell'esercizio di prerogative dell'autorità di governo dello Stato a disposizione del quale è messo». Cfr. Commissione del diritto internazionale, *Progetto di Articoli sulla Responsabilità degli Stati,* 2001, art. 6.

pur sempre alle agenzie straniere e quindi al più, nel caso di specie, agli Stati Uniti[538].

Per quanto concerne la seconda ipotesi – e cioè la semplice ricezione del materiale intercettato e la susseguente archiviazione, esaminazione e utilizzazione da parte del Governo britannico – la Corte non ha fatto altro che paragonare l'attività di sorveglianza e intercettazione generalmente intesa con l'ipotesi dell'*Intelligence Sharing*, esaminando quindi se la disciplina fosse compatibile con i criteri previsti nel caso *Weber and Saravia* e se tale regime fosse previsto dalla legge britannica, necessario in una società democratica e proporzionale[539].

Lo sforzo della Corte è senz'altro notevole ma affermando la compatibilità di tale regime con la convenzione[540], esso si conclude con un nulla di fatto.

Oltre al mancato riferimento ad un suo precedente ove, seppur incidentalmente aveva fatto riferimento all'*intelligence sharing*[541], e ai limitati paragrafi concessi all'analisi del problema, soprattutto per quel riguarda il test della proporzionalità di tali misure[542], le criticità della sentenza sono diverse.

---

[538] *Ibidem*.

[539] *Ibidem*, par. 422-446.

[540] *Ibidem*, par. 447.

[541] Si fa riferimento al caso *Centrum for Rattvisa* c. *Svezia*, ove la Corte al paragrafo 74 incidentalmente afferma «[f]inally, the report briefly considered the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques».

[542] Cfr. CHRISTAKIS, *A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on The Big Brother Watch Judgment*, in *European Law Blog*, 20 settembre 2018, consultabile online al seguente indirizzo https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/

Anzitutto, la Corte concentrandosi esclusivamente sui dati 'richiesti' dal Regno Unito sembra perdere di vista la reale e moderna portata dell'accordi in materia di *Intelligence sharing*. Come si è avuto modo di vedere, infatti, attraverso tali strumenti gli Stati posso condividere anche quella particolare tipologia di informazioni definite 'grezze' (*raw*) che, per definizione, non sono state ancora analizzate e quindi è ben possibile che l'analisi e l'esame di queste avvenga proprio da parte dello Stato richiedente[543]. Prendere in considerazione dunque la sola ipotesi in cui i dati vengono richiesti limita fortemente l'analisi della Corte e appare, in ultima analisi, un'occasione mancata per poter far luce su un argomento che tutt'oggi ha ancora molte ombre.

In secondo luogo, i giudici di Strasburgo sembrano commettere un errore metodologico di non poco peso. Essi infatti per affrontare la questione equiparano un preciso aspetto dell'*intelligence sharing* alla sorveglianza di massa, applicando così i criteri elaborati in precedenti giurisprudenziali. Tuttavia, ancorché si voglia condividere tale equiparazione, il problema sorge quando ci si confronta con le conclusioni a cui giunge la Corte: la sezione 8(4) che disciplina il regime di intercettazioni è contrario all'art. 8 CEDU, mentre la procedura di archiviazione ed uso dei dati richiesti ad altri Stati è compatibile con la Convenzione. Il fatto che alcuni punti della sentenza siano particolarmente critici è evidenziato altresì dalla richiesta di rinvio alla Grande Camera, e alla sua accettazione.

L'analisi fin qui condotta ha messo in luce alcuni aspetti problematici dell'attuale relazione tra tecniche di sorveglianza e tutela del diritto alla

[543] Nello stesso senso si veda FALCHETTA, *Intelligence Sharing and the Right to Privacy after the European Court Judgment in Big Brother Watch v. UK,* in EJIL:*Talk!* Blog of the European Journal of International Law, 24 settembre 2018, consultabile online al seguente indirizzo https://www.ejiltalk.org/intelligence-sharing-and-the-right-to-privacy-after-the-european-court-judgment-in-big-brother-watch-v-uk/

privacy. Se da un lato infatti i cambiamenti tecnologici hanno portato ad una maggiore propensione degli Stati ad utilizzare tecniche di sorveglianza di massa e alla raccolta quasi indiscriminata di dati riguardanti i singoli individui, dall'altro lato la tutela prevista dalla disciplina normativa dei singoli Paesi troppo poco spesso è riuscita a stare al passo con tale innovazione[544]. Ciò si è tradotto nella possibilità per gli Stati di accedere alle informazioni dei propri cittadini, degli stranieri e a quelle raccolte da altri Stati attraverso una molteplicità di modi e per gli scopi più disparati, sovente senza che vi sia una specifica autorizzazione da parte di un potere terzo ed imparziale come quello dei giudici[545].

Nonostante alcuni progressi successivi alle rivelazioni del caso *Datagate*, che si sono tradotti in una maggiore attenzione da parte delle istituzioni internazionali e delle Corti internazionali, attraverso l'adozione di documenti (non vincolanti) e l'emanazione di diverse pronunce, ad oggi la situazione non sembra orientarsi verso un effettivo rafforzamento del diritto alla privacy. Ne è sintomatico l'approccio solo parzialmente progressivo messo in atto dalla Corte Europea dei Diritti dell'Uomo che invece, in un primo momento, sembrava proprio voler rispondere a tale esigenza.

Senonché, i buoni propositi dei Giudici di Strasburgo si sono poi rivelati insoddisfacenti. Analizzando le ultime pronunce in materia, infatti, appare

[544] Un chiaro esempio di quanto si sta dicendo si può rinvenire nelle parole del Relatore speciale per la promozione e protezione del diritto alla libertà di opinione ed espressione, Frank La Rue, il quale sostiene «In many countries, existing legislation and practices have not been reviewed and updated to address the threats and challenges of communications surveillance in the digital age. Traditional notions of access to written correspondence, for example, have been imported into laws permitting access to personal computers and other information and communications technologies, without consideration of the expanded uses of such devices and the implications for individuals' rights (…)». Cfr. LA RUE, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/23/40, 2013, par. 17.

[545] *Ibidem*.

chiaro che lo sviluppo progressivo a cui si stava assistendo abbia lasciato il passo ad una involuzione del diritto alla *privacy*, riconoscendo indirettamente una eccessiva discrezionalità agli Stati.

L'errore principale in cui sembra incorrere la Corte è proprio quello di non prendere in debita considerazione gli aspetti più attuali dell'innovazione tecnologica. Quest'ultima infatti nella sua declinazione più recente ha permesso, da un lato, agli Stati di utilizzare strumenti sempre più efficaci e capillari per poter sorvegliare i cittadini e, dall'altro lato, ha rivoluzionato il modo di comunicare degli stessi, contribuendo ad una vera e propria rivoluzione nello stile di vita di ognuno di noi. L'automatica conseguenza è che sia le comunicazioni che le attività sottoponibili ad intercettazioni sono aumentate notevolmente. Allo stesso modo anche i rischi derivanti da comportamenti arbitrati degli Stati si sono intensificati. In definitiva quindi è agevole costatare che il contesto giuridico-fattuale in cui la sorveglianza segreta opera oggi è totalmente differente rispetto alle circostanze prese in esame ormai due decadi fa nel caso *Weber e Saravia*. A fronte di tale evoluzione tecnologica però non si è assistito ad una altrettanta evoluzione delle tutele apprestate dalla Corte, ma piuttosto ad una vera e propria involuzione.

L'asserita compatibilità *tout court* della sorveglianza di massa con la Convezione è uno degli aspetti più sintomatici di quanto si sta dicendo. E anche laddove si volesse prescindere dal peso dell'affermazione in sé, è il ragionamento della Corte a destare non poche incertezze. A tal proposito basta richiamare quanto detto in merito alla necessità di un'autorizzazione *ex ante*. In precedenti pronunce (*Zakharov*[546] e *Szabo e Vissy*[547]) la Corte aveva affermato la necessità di un'autorizzazione per procedere ad intercettazioni che provenisse da un Giudice o quanto meno da un'autorità

[546] Cfr. *Roman Zakharov* c. *Russia, par. 258.*
[547] Cfr. *Szabò and Vissy* c. *Ungheria, par. 77.*

amministrativa indipendente dal potere di governo. L'operato della Corte non si limitava all'esistenza di un requisito meramente procedurale, ma si soffermava anche sull'effettività della misura. Nel caso *Zakharov*, ad esempio, la Corte ha condannato la Russia poiché, nonostante la legge prevedesse la necessità di un'autorizzazione da parte del giudice, in concreto il controllo preventivo esercitato dal potere giudiziario non era effettivo e non compiva il suo scopo, cioè quello di prevenire il rischio di abusi da parte dello Stato.

Nella sentenza *Big Brother Watch*, invece, la Corte nega la necessità di questo requisito procedurale ed effettivo, affermando che nel caso di specie alcuni elementi dimostrano l'assenza di possibili abusi da parte del potere esecutivo[548].

Facendo un discorso più generale però è agevole osservare come una previsione del genere non può non determinare un detrimento in termini di certezza del diritto e prevedibilità: una cosa è indicare la necessità di una condizione di procedibilità sia in astratto che in concreto e altra cosa è invece rimuovere totalmente questa previsione, sebbene poi in concreto non si accertino abusi[549].

Inoltre, anche in merito al problema dell*'Intelligence sharing*, la Corte aveva l'occasione per chiarire in che modo il diritto alla privacy doveva essere tutelato rispetto all'uso di tecnologie di condivisione delle informazioni, esaminando in modo più adeguato il rapporto tra USA e Regno Unito e la cd. Five Eyes Alliance[550]. Invece anche in questo caso

[548] Cfr. *Big Brother Watch* c. *Regno Unito*, par. 381.

[549] Cfr. CHRISTAKIS, *op.cit.*.

[550] La questione non è di poco conto dato che il contenuto di questa intesa tra i due Stati non è pubblico e quindi non è generalmente accessibile. Solo di recente infatti attraverso lo sforzo di alcune ONG è stato possibile svelare alcune parti del suo contenuto. Sul punto, seppur brevemente, si veda KIM, LEE, LUBIN, PERLIN, *Newsly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, in *Lawfareblog*, 23

l'esito si è tradotto in un nulla di fatto: i giudici hanno deciso di trattare il problema solo da un punto di vista superficiale senza entrare nel merito delle più rilevanti questioni. La Corte ad esempio avrebbe potuto prendere in considerazione l'ultimo *report* dell'Alto Commissario per i Diritti Umani, emanato un mese prima della sentenza, ove vengono esplicitamente messi in luce i rischi derivanti dall'uso di questa speciale pratica di sorveglianza, nonché il conseguente indebolimento del diritto alla *privacy*[551]. Avrebbe potuto altresì fare luce sulla possibilità, nemmeno troppo remota, in cui la condivisione di informazioni avviene con Paesi in cui storicamente vengono violati i diritti umani e in cui lo stato di diritto è pressoché nullo, non escludendo ad esempio che anche lo Stato ricevente le informazioni, essendo le stesse state ottenute in violazione del diritto internazionale, fosse internazionalmente responsabile.

aprile 2018, consultabile online al seguente indirizzo https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing

[551] Cfr. *Report of the United Nations High Commissioner for Human Rights, The right to privacy in the digital Age*, A/HRC/39/29, 3 agosto 2018, par. 21.

CONCLUSIONI

L'indagine da noi condotta ha tentato di chiarire il rapporto tra internet/cyberspazio e diritto internazionale, avendo soprattutto riguardo tre aspetti differenti ma tra loro interconnessi: la regolamentazione dello spazio virtuale, i conflitti interstatali originati da attacchi informatici e la tutela dei diritti individuali che vengono in rilievo nel cyberspazio.

Il lavoro, in particolare, ha preso le mosse da alcune considerazioni di carattere tecnico necessarie non solo per comprendere le peculiarità dello 'spazio' in cui si opera, ma soprattutto per capire in che modo alcuni principi del diritto internazionale possano essere declinati. A tal proposito è stata anzitutto evidenziata la differenza esistente tra i termini "cyberspazio" e "internet", sul presupposto che quest'ultimo altro non è che una porzione più ristretta del primo. Questa distinzione terminologica ci ha portato poi ad indagare cosa si dovesse intendere per cyberspazio, giungendo alla conclusione per cui, a dispetto di quello che viene comunemente inteso, il cyberspazio, pur caratterizzandosi per essere uno spazio virtuale e a-territoriale, presenta altresì alcuni aspetti tangibili: le

infrastrutture tecniche (server, cavi, etc.) dislocate all'interno dei territori degli Stati, senza i quali l'intera Rete non esisterebbe.

Una volta effettuate queste precisazioni terminologiche, la prima questione che abbiamo affrontato ha avuto ad oggetto la ricostruzione di una disciplina giuridica applicabile al cyberspazio. Nel dettaglio, abbiamo visto come da una iniziale concezione anarchica dello spazio virtuale, ove veniva escluso l'intervento regolatore da parte degli Stati, si è assistito ad un incessante interesse da parte di questi ultimi nella materia *de* qua, fino al punto di spingere nel senso di una regolamentazione internazionale basata sulla cooperazione e sulla partecipazione di tutti i diversi attori coinvolti; e di porre, più in generale, la questione della cd. *governance* di internet.

La questione non è di poco peso se si considera che un importante impulso verso una regolamentazione internazionale è stato dato proprio dalle Nazioni Unite che, attraverso una sua agenzia specializzata, l'ITU, hanno dato vita a diversi momenti di discussione concretizzatisi nel *World Summit on the Information Society*. I punti nodali del dibattito si sono dipanati intorno al ruolo svolto dall'ICANN, organizzazione no profit, che ha il compito di determinare il funzionamento dei cd. nomi a dominio, che di internet costituiscono l'ossatura principale. Nonostante gli sforzi profusi dagli Stati nelle varie sedi negoziali, abbiamo constatato come le visioni contrapposte tra le potenze occidentali, da un lato, e quelle orientali, dall'altro, non hanno consentito un cambio di paradigma che permettesse una riforma concreta della *governance* attraverso la creazione di una nuova istitutuzione internazionale capace di meglio rappresentare i diversi attori coinvolti. I motivi di questo fallimento possono essere ricercati anzitutto in ragioni di carattere storico: gli Stati Uniti, ideatori e creatori della Rete, non hanno acconsentito alla nascita di un ente diverso

dall'ICANN, che svolgesse la funzione di gestore dell'impalcatura principale di internet, in altre parole dei nomi a dominio.

Dinanzi a queste difficoltà, un ulteriore tentativo in sede negoziale ha avuto luogo con la creazione, da parte dell'Assemblea Generale, del *Group of Government Experts* (UN GGE). Il gruppo di esperti si è riunto in diverse occasioni giungendo talvolta ad esiti positivi e talaltre a conclusioni del tutto opposte. In particolare, nonostante alcuni progressi individuabili nei relativi *Report,* è stato segnalato come nel corso dell'ultimo incontro (2017) il Gruppo non è riuscito a raggiungere il consenso necessario per emanare il relativo documento. Le ragioni del mancato accordo questa volta sono di carattere sostanziale. Gli Stati non hanno raggiunto una visione comune su alcuni temi di particolare rilevanza come la legittima difesa, le contromisure e più in generale l'applicazione del diritto internazionale umanitario al contesto virtuale.

Ebbene, sul presupposto della difficoltà, almeno per il momento, di giungere a una conclusione negoziale, ci si è interrogati, d'altra parte, circa la possibilità di ricostruire l'esistenza di norme consuetudinarie specifiche per il cyberspazio.

In relazione a questo aspetto sono state svolte due considerazioni. La prima è che rispetto al passato gli Stati sempre più spesso adottano documenti aventi ad oggetto lo specifico tema del cyberspazio. Ne sono un esempio la prassi degli Stati Uniti, della Francia, dell'Olanda e dell'Italia. Senonché, a fronte di questi comportamenti, bisogna rilevare che la prassi ad oggi non solo non appare univoca, ma difetta altresì dell'eterogeneità necessaria per ritener integrato l'elemento oggettivo della consuetudine.

Allo stesso modo, essendo tali comportamenti spesso esternati attraverso dichiarazioni non vincolanti, anche l'elemento soggettivo è particolarmente difficile da ricostruire. Questo primo aspetto ci ha portato

alla seconda considerazione, ossia alla questione se nel contesto cibernetico si stia assistendo all'applicazione di quel fenomeno noto nella teoria generale del diritto come *the pluralization of international law making*. Nel dettaglio, a noi pare che nel contesto virtuale sia sempre più diffuso un processo di verticalizzazione nella creazione di norme internazionale, ove i soggetti partecipanti non sono solo ed esclusivamente gli Stati ma anche attori non statali. Sintomatiche di questo fenomeno sono le diverse iniziative poste in essere da aziende operanti nel settore come Microsoft e dalla società civile (si pensi al caso del Tallinn Manual).

Senonché, come è noto, al fine di ricostruire una norma consuetudinaria la prassi rilevante riposa in genere su quella degli Stati e dalle organizzazioni internazionali. Ciononostante va rilevato che i comportamenti degli altri attori, che nel contesto del cyberspazio assumono una importanza altrettanto ragguardevole, «may be relevant when assessing the practice» (CDI, *Identification of customary international law: Text of the Draft Conclusion Provisionally Adopted by the Drafting Committee*, p. 2). Con questo non si vuole affermare che ad oggi esistano delle norme consuetudinarie specifiche per il cyberspazio, ma piuttosto che un processo del genere è *in fieri* e il ruolo degli attori (non statali) coinvolti non può essere sottovalutato.

In questo senso, e ragionando attraverso il prisma delle norme consuetudinarie *già esistenti,* ci si è chieste se le stesse possano trovare applicazione relativamente a uno spazio nuovo e virtuale. Partendo da una delle norme cardine del diritto internazionale, vale a dire il principio di sovranità, abbiamo visto come esso sia applicabile quantomeno al primo livello che compone il cyberspazio, vale a dire alle infrastrutture fisiche situate all'interno del territorio di ciascuno Stato. Su di esse dunque non vi è dubbio che lo Stato possa esercitare il suo potere di imperio. Discorso diverso invece è stato fatto con riferimento al cyberspazio nel suo

complesso, e cioè in relazione a quello spazio virtuale, non tangibile, a-territoriale ed interconnesso. E infatti, nonostante la prassi di alcuni Stati deponga nel senso di creare diversi spazi virtuali in relazione ad ogni singolo Stato, a noi pare che una conclusione siffatta sia in netta contrapposizione con la natura intrinsecamente globale del cyberspazio. Per questi motivi dunque non ci sembra possa affermarsi l'esistenza di un diritto unilaterale da parte di un singolo Stato sull'intero cyberspazio, ma piuttosto la tendenza e soprattutto la necessità ad una maggiore cooperazione per la sua gestione e regolamentazione.

Ciononostante, la prassi rivela come negli ultimi anni sempre più spesso si sia utilizzato questo spazio come un vero e proprio 'campo di battaglia' in cui gli Stati, attraverso attacchi informatici, hanno posto in essere condotte contrarie al diritto internazionale. A fronte di questa costatazione, si è presa in esame la norma di carattere consuetudinario, nonché convenzionale, che impone il divieto di uso della forza. Abbiamo visto che affinché un attacco informatico possa essere espressione della forza è necessario che esso produca effetti analoghi a quelli prodotti da un attacco tradizionale, e cioè la distruzione materiale di cose ovvero l'uccisione di persone. A nulla servirebbero quelle teorie, specificamente create per le operazioni informatiche, volte ad estendere la qualificazione degli attacchi informatici come casi di uso della forza anche allorquando questi non producano effetti tangibili.

Nello specifico, l'analisi di alcuni casi della prassi ha messo in luce che, a dispetto delle qualificazioni proposte in dottrina, ad oggi nessun attacco informatico ha raggiunto la soglia della forza armata. Ciò, tuttavia, non vuol dire escludere aprioristicamente l'applicazione dell'art. 2(4) della Carta delle Nazioni Unite al contesto informatico, ma piuttosto che allorquando non sia raggiunta tale soglia a venire in rilievo è un altro principio del diritto internazionale, e cioè quello della non ingerenza negli

affari interni di uno Stato. A noi pare infatti che sia proprio questa norma a spiegare gli effetti nell'attuale contesto delle operazioni informatiche.

Com'è noto, gli elementi che determinano la violazione del principio sono essenzialmente due: l'attività deve riguardare un aspetto di esclusiva competenza degli Stati (cd. dominio riservato) ed essa deve qualificarsi come coercitiva. È proprio quest'ultimo aspetto a determinare non poche difficoltà. La sua individuazione, già complessa nelle ipotesi delle azioni tradizionali, si amplifica quando ci si confronta con il contesto informatico. Ciononostante, l'esame della prassi ha mostrato come in alcuni casi questo principio sia stato violato. L'esempio più significativo è senz'altro rappresentato dalle elezioni americane del 2016, ove la Russia, attraverso un attacco informatico, è intervenuta negli affari interni degli Stati Uniti. Nel dettaglio, l'operazione informatica ha integrato sia l'elemento dell'interferenza in una delle materie di esclusiva competenza dello Stato (e le elezioni senz'altro rientrano in questo ambito) sia assunto le caratteristiche proprie di un atto *coercitivo*. Ed è tale, secondo noi, almeno nel contesto degli attacchi informatici, anche quell'operazione che produca effetti coercitivi solo indiretti. Detto diversamente, è ben possibile che un attacco informatico, ancorché non raggiunga la soglia dell'uso della forza armata, possa integrare l'elemento oggettivo dell'illecito internazionale. Ma ciò a condizione che l'operazione sia attribuibile ad uno Stato.

Sotto questo aspetto viene necessariamente in rilievo il Progetto di articoli sulla responsabilità degli Stati e, in particolare, gli artt. 4 e 8. L'applicazione del primo è senz'altro agevole, ma poco rilevante nel contesto informatico. E infatti allorquando un attacco informatico provenga da un organo rientrante nella struttura organizzativa dello Stato non vi è dubbio che l'azione possa essere a quest'ultimo attribuita. I problemi principali sorgono invece in relazione all'art. 8 che, da un lato,

senz'altro configura una ipotesi maggiormente rappresentativa della prassi degli attacchi informatici, ma dall'altro lato impone un criterio di attribuzione particolarmente stringente. A fronte di queste difficoltà è stato suggerito in dottrina l'utilizzo del criterio di attribuzione del controllo globale che meglio risponderebbe alle caratteristiche tecniche degli attacchi informatici. Ma, come indicato dal Tribunale penale internazionale della Ex-Jugoslavia, tale criterio è utilizzabile solo con riferimento a gruppi militari gerarchicamente organizzati. E i gruppi di hacker difficilmente sono suscettibili di ricadere in questa categoria.

Quanto invece alla possibile rilevanza dell'art. 8, si è osservato come il problema principale sotteso alla sua applicazione concerna soprattutto gli aspetti probatori, e cioè l'individuazione dello *standard* probatorio necessario affinché una condotta possa essere attribuita allo Stato. Invero, nel contesto delle operazioni informatiche non è possibile ravvisare una inversione dell'onere della prova. Detto onere, dunque, sorge in capo a quella parte che affermi l'esistenza o il verificarsi di quel determinato comportamento. Ciò pone inevitabilmente la questione dello *standard* probatorio, rispetto alla quale si è giunti alla conclusione per cui, in ragione delle caratteristiche tecniche del cyberspazio, è possibile attribuire una condotta ad uno Stato anche in presenza di prove indirette e deduzioni. Tale conclusione è corroborata dagli esempi della prassi presi in esame.

D'altra parte, vista l'importanza assunta in dottrina, ci si è interrogati sulla portata degli obblighi di *due diligence* e la loro rilevanza nel contesto degli attacchi informatici. Su questo aspetto, se da un lato è possibile affermare che il semplice fatto che un attacco informatico provenga dal territorio di uno Stato non sia indice della sua responsabilità, dall'altro lato il principio in esame sembra poter spiegare degli effetti anche in relazione al contesto virtuale. In altre parole, gli Stati sono tenuti ad agire secondo diligenza ed evitare pertanto che il proprio territorio venga usato per

compiere attacchi informatici, di cui essi sono a conoscenza, nei confronti di altri Stati. Allo stesso tempo però al fine di ottemperare a tali obblighi, e quindi prevenire il compimento di attacchi informatici di cui gli Stati sono a conoscenza, non si può riconoscere agli Stati la possibilità di usare indiscriminatamente programmi di sorveglianza di massa in danno dei diritti fondamentali degli individui come, tra gli altri, quello della *privacy*.

Quest'ultimo aspetto è stato oggetto di analisi nella parte conclusiva dell'elaborato. In particolare, si è evidenziato come nonostante una crescente attenzione per il riconoscimento del diritto alla *privacy* anche rispetto agli scenari più attuali determinati dall'innovazione tecnologica, ad oggi esso non appare adeguatamente tutelato.

Le due esigenze contrapposte, da un lato quella della sicurezza nazionale spesso invocata dagli Stati, e dall'altro lato quella della tutela effettiva del diritto alla vita privata e familiare infatti, non sono sempre state adeguatamente bilanciate. La Corte EDU, almeno nelle sue ultime pronunce, pare aver riconosciuto agli Stati una discrezionalità eccessiva nel porre in essere misure di sorveglianza di massa. È sintomatico di ciò la recente sentenza *Big brother watch* c. *Regno Unito*, in cui la Corte ha affermato che i programmi di sorveglianza di massa di *per sé* non sono incompatibili con la Convenzione.

BIBLIOGRAFIA

- AARONSON, LEBLOND, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, in *Journal of International Economic Law*, 2018;
- ALBRIGHT, BRANNAN, WALROND, *Did Stuxnet Take out 1.000 Centrifuges at the Natanz Enrichment Plant?* Institute for science and International Security, 22 dicembre 2010;
- AMBOS, *International Criminal Responsibility in Cyberspace*, in N. TSAGOURIAS, R. BUNCHAN (a cura di) *Research Handbook on International Law and Cyberspace*, Cheltenham e Northampton, 2015;
- ANTOLIN-JEKINS, *Defining the Parameters of Cyberwar Operations: Looking for Law in all Wrong Places?*, in *Naval Law Review*, 2006;
- ARAI-TAKAHASHI, T*he defensibility of the margin of appreciation doctrine in the ECHR: value-pluralism in the European integration*, in *Revue Européenne de Droit Public*, 2001;

- ARANGIO-RUIZ, *Second Report on State Responsibility, ILC Yearbook*, 1989;
- ARANGIO-RUIZ, *State Fault and the Forms and Degrees of International Responsibility: Questions of Attribution and Relevance* in *Le droit international au service de la paix, de la justicia et du development, Mélanges Michel Virally, Paris*, 1991;
- AUST, *Modern Treaty Law and Practice*, Cambridge, 2007;
- BANKS, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, in *Texas Law Review*, 2017;
- BANNELIER-CHRISTAKIS, *Cyber Diligence: A Low-Intensity due diligence principle for low-intensity cyber operations?*, in *Baltic Yearbook of International Law*, 2014;
- BARTOLINI, *Il concetto di controllo sulle attività di individui quale presupposto della responsabilità dello Stato* in SPINEDI, GAINELLI, ALAIMO (a cura di), *La codificazione della Responsabilità Internazionale degli Stati alla prova dei fatti. Problemi e spunti di riflessione*, Milano, 2006;
- BAYLES, *The Ethics of Computer Network Attack*, in *Journal of the US Army War College*, 2001;
- BENATAR, *The Use of Cyber Force: Need for Legal Justification?* in *Goettingen Journal of International Law*, 2009;
- BENDIECK, *Due Diligence in Cyberspace*, in *Stiftung Wissenschaft und Politik German Institute for International and Security Affairs*, 2016;
- BENTWICH, MARTIN, *A Commentary of the Charter of the United Nations*, Routledge, 1950;
- BESSON, *Sovereignty*, in *Max Planck Encyclopedia of Public International Law*, 2011;

- BESSON, *Theorising the Sources of International Law*, in S. BESSON, J. TASIOULAS (a cura di), *The Philosofy of International Law*, Oxford, 2010;
- BING, *Building a Cyberspace: History of internet*, in *BYGRAVE*, *BING* (a cura di) *internet Governance: Infrastructure and Istitution*, Oxford, 2009;
- BLASI-CASAGRAN, *Global Data Protecion in the Field of Law Enforcment: an EU Perspective*, Londra, 2016;
- BOBBIO, *Invece dello Stato: reti*, in *Parole chiave – nuova serie di 'Problemi del socialismo'*, 2005;
- BONFANTI, *Il diritto alla protezione dei dati personali nel Patto internazionale sui diritti civili e politici e nella Convenzione europea dei diritti umani: similitudini e difformità di contenuti*, in *Diritti umani e diritto internazionale*, 2011;
- BOOTHBY e altri, *When is a Cyberattack a Use of Force or an Armed Attack?*, in *Computer Journal*, 2012;
- BOUTIN, *Shared Responsibility for Cyber Operations*, in *American Journal of International Law Unbound*, 2019;
- BOWMAN, *Is International Law Ready for the Informational Age?*, in *Fordham International Law Journal*, 1995 BOWMAN, *Is International Law Ready for the Informational Age?*, in *Fordham International Law Journal*, 1995;
- BRAVO, *La prova nel processo internazionale*, Napoli, 1958;
- BROWN, *Why Iran Didn't Admit Stuxnet was an Attack*, in *Joint Force Quarterly*, 2011;
- BROWNLIE, *International Law and the Use of Force by States*, Clarendon, 1963;

- BRUNNER, *Digital Communications and the Evolving Right to Privacy*, in LAND, ARONSON (a cura di) *New Technologies for Human Rights Law and Practice*, Cambridge University Press, 2018;
- BRYANT, *What Kind of Space is Cyberspace*, in *internet Journal of Philosophy*, 2001;
- BUFALINI, *Uso della forza, legittima difesa e problemi di attribuzione in situazione di attacco informatico*, in TANZI, LANCIOTTI (a cura di), *Uso della forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2011;
- BUNCHAN, *Cyber Attakcs: Unlawful Uses of Force or Prohibited Invterventions*, in *Journal of Conlfict and Security Law*, 2012;
- BUNCHAN, *International Law and the Construction of the Liberal Peace*, Oxford, 2013;
- CANNIZZARO, *Metodi di Soluzione di Conflitti fra Giurisdizioni Internazionali: il Contributo della Sentenza della CIG sul caso del Genocidio (Bosnia Erzegovina c. Serbia e Montenegro)"* in *European Journal of Legal Studies*, 2007;
- CARLIN, *Detect, Distrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, in *Harvard National Security Journal*, 2016;
- CAROTTI, *Il sistema di governo di internet*, Milano, 2016;
- CARR, *Inside Cyber Warfare*, Sebastopol, 2010;
- CARRILLO, *La reforma de la corporacion para la asignacion de nombres y numeros de internet (ICANN): un analisis en terminos de legitimidad*, in *Revista espanola de derecho internacional*, 2018;
- CASSESE, *The Nicaragua and Tadic´ Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, in *European Journal of International Law*, 2011;

- CHRISTAKIS, *A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on The Big Brother Watch Judgment*, in *European Law Blog*, 20 settembre 2018;
- CLARKE, KNAKE, *Cyber War: The Next Threat to National Security and What to Do About It*, New York, 2010;
- CLAVER, *Governance of cyber warfare in the Netherlands: an exploratory investigation*, in *The International Journal of Intelligence, Security, and Public Affairs*, 2018;
- COHEN, *Cyberspace as/and Space*, in *Columbia Law Review*, 2007;
- CONDORELLI, KRESS, *Part III The Sources of International Responsibility, Ch.18 The Rules of a Attribution: General Consideration* in CRAWFORD, PELLET, OLLESON (a cura di), *The Law Of International Responsibility*, Oxford, 2010;
- CONDRON, *Getting It Right: Protecting American Critical Infrastructure, in Cyberspace,* in *Harvard Journal of Law and Technology*, 2007;
- CONDRON, *Getting It Right: Protecting American Critical Infrastructure, in Cyberspace,* in HJLT, 2007;
- CONFORTI, *Diritto Internazionale*, XI edizione (a cura di Massimo Iovane), 2018;
- COOPER, *Raphael Lemkin and the Struggle for the Genocide Convention*, 2008, New York, 2008;
- COT, *Margin of appreciation*, in *Max Planck Encyclopedia of Public International Law*, 2007;
- COUZIGOU, *The Challenges Posed by Cyber Attacks to the Law on Self-Defence,* in *European Society of International Law Conference Paper* n. 16/2014, 2014;

- D'ASPREMONT (a cura di), *Partecipans in the International Legal System − Multiple Perspectives on Non State Actors in International Law*, Londra, 2011;
- D'ASPREMONT, *Formalism and the Sources of International Law. A Theory of the Ascertainment of Legal Rules*, Oxford, 2011;
- DE FROUVILLE, *The Sources of International Responsibility, attribution of conduct to the State: Private Individuals* in CRAWFORD, PELLET, OLLESON (a cura di), *The Law Of International Responsibility*, Oxford, 2010;
- DELERUE, *The Codification of the International Law applicable to Cyber Operations: A Matter for the ILC?*, in *Esil Reflections*, 2018;
- DELLA MORTE, *Big data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018;
- DEV, *Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response*, in *Texas International Law Journal*, 2014;
- DINNISS, *Cyber Warfare and the Laws of War*, Cambridge: Cambridge University Press, 2012;
- DRAKE (a cura di), *Reforming internet Governance: Perspectives from the Working Group on internet Governance* (WGIG), New York: United Nations Information and Communication Technology Task Force, 2005;
- DUCHEINE, *Anticipatory Self-Defense in the Cyber Context*, in *International Law Studies*, 2013,;
- EFRONY, SHANY, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, in *American Journal of International Law*, 2018;

- EICHENSEHR, *The Cyber-Law of Nations*, in *Georgetown Law Journal*, 2015;
- EICHNESEHR, *Decentralized Cyberattack Attribution*, in *American Journal of International Law Unbound*, 2019;
- FALCHETTA, *Intelligence Sharing and the Right to Privacy after the European Court Judgment in Big Brother Watch v. UK,* in EJIL:*Talk!* Blog of the European Journal of International Law, 24 settembre 2018;
- FAYAZMANESH, *Containing Iran: Obama's Policy of "Tough Diplomacy*, Cambridge, 2013;
- FIDLER, *Was Stuxnet an Act of War? Decoding a Cyberattack*, in *IEEE Security and Privacy*, 2011;
- FINALY, PAYNE, *The Attribution Problem and Cyber Armed Attacks*, in *American Journal of International Law Unbound*, 2019;
- FLECK, *Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual*, in *Journal of Conflict & Security Law,* 2013;
- FOLTZ, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, in *Joint Force Quarterly*, 2012;
- FORNARI, *Conflitto in Ucraina, orsi fantasiosi e programmi malevoli*, in *Rivista di diritto internazionale*, 2017;
- FRULLI, *Un passo avanti e due indietro: responsabilità individuale e responsabilità statale nella sentenza della Corte Internazionale di Giustizia nel caso Bosnia- Erzegovina c. Serbia* in *Diritti Umani e diritto internazionale*, 2007;
- GIBSON, *Neuromante*, Milano, 1986;
- GILLIES, CAILLIAU, *How the Web Was Born*, Oxford, 2000;

- GODON, *Considération techniques à destination des juristes*, in Société Francaise pour le Droit International, *internet et le droit international – Colleque de Rouen*, Parigi, 2014 ;
- GOLDSMITH, *Cybersecurity Treaties: A Skeptical View*, in BERKOWITZ (a cura di), *Future Challenges in National Security and Law*, 2011;
- GOLDSMITH, *WCIT-12: An Opinionated Primer and Hysteria-Debunker*, in *Lawfare blog*, 30 novembre 2012;
- GOURLEY, *Cyber Sovereignty*, in YANNAKOGEORGOS, LOWTHER (a cura di) *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, Londra-New York, 2013;
- GRAHAM, *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 2010;
- GREEN, *Fluctuating Evidentiary Standards for Selfe-Defence in the Inernational Court of Justice*, in *International and comparative Law Quarterly*, 2009;
- GREENWALD, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State,* New York, 2015;
- HANDLER, *The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare*, in *Stanford Journal of International Law*, 2012;
- HATHAWAY, *The Law of Cyber-Attack,* in *California Law Review*, 2012;
- HENDERSON, *The Use of Force and International Law*, Cambridge, 2018;
- HENKIN, *The Reports of the Death of Article 2(4) are Greatly Exaggerated*, in *American Journal of International Law*, 1971;

- HENRIKSEN, *The End of the road for the UN GGE process: The future regulation of cyberspace*, in *Journal of cybersecurity*, 2019;
- HOLLIS, *Why States need International Law for Information* Operations, in *Lewis and Clark Law* Review, 2007;
- HYBRID *Net: the regulatory framework of ICANN and the DNS*, in *International Journal of Law and Technology*, 2014;
- JAMNEJAD, WOOD, *The Principle of Non-intervention*, in *Leiden Journal of International Law*, 2009;
- JENSEN, *State Obligations in Cyber Operations*, in *Baltic Yearbook of International Law*, 2014;
- JEUTNER, *The Digital Geneve Convention: A Criticatl Apprasial of Microsoft's Proposal*, in *Journal of International Humanitarian Legal Studies*, 2019;
- JHONSON, POST, *Law and Borders-The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996;
- JOYCE, *Privacy in the Digital Era: Human Rights Online*, in *Melbourne Journal of International Law*, 2015;
- KALJURAND, *United Nations Group of Governmental Experts: The Estonian Perspective*, in OSULA, RÕIGAS (a cura di), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, 2016;
- KEITNER, *Attribution by Indictment*, in *American Journal of International Law Unbound*, 2019;
- KIM, LEE, LUBIN, PERLIN, *Newsly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, in *Lawfareblog*, 23 aprile 2018;
- KLABBERS, PETERS, e ULFSTEIN (a cura di), *The Constitutionalization of International Law*, Oxford, 2009;

- KOESPELL, *The Ontology of Cyberspace: Law, Philosophy, and the Future of Intellectual Property*, Londra, 2003;
- KOH, *International Law in Cyberspace*, Speech at the USCYBERCOM Inter-Agency Legal Conference, 18 September 2012, in GUYMON (a cura di), *Digest of United States Practice in International Law*, 2012;
- KOIVUROVA, *Due Diligence*, in *Max Planck Encyclopaedia of Public International Law*, 2010;
- KOLB, *Reflections on due diligence duties and cyberspace*, in *German Yearbook of International Law*, 2015;
- KUEHL, *From Cyberspace to Cyberpower: Defining the Problem*, in KRAMER, STARR e WENTS (a cura di) *Cyberpower and National Security*, Nebraska, 2009;
- LAMMERS, *Pollution of International Watercourses*, L'Aia, 1984;
- LARAE-PEREZ, *Economic Sanctions as a Use of Force: Re-Evaluationg the Legality of Sanctions from an Effects-Based Perspective*, in *Boston University International Law Journal*, 2002;
- LEINER, CERF, CLARK, KAHN, KLEINROCK, LYNCH, POSTEL, ROBERTS, WOLFF, *Brief History of the internet;*
- LEVINSON-WALDMAN, *NSA Surveillance in the War on Terro*r, in GRAY, HENDERSON (a cura di) *The Cambridge Handbook of Surveillance Law*), Cambridge, 2017;
- LIAROPULOS, *Exploring the Complexity of Cyberspace Governance: State sovereignty, Multi-stekeholderism, and Power Politics*, in *Journal of Information Warfare*, 2016;
- LIN, *Attribution of Malicious Cyber Incidents:From Soup to Nuts*, in *Journal of International Affairs*, 2017;

- LUBIN, *We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the practice of Foreign Mass Surveillance*, in *Chicago Journal of International Law*, 2018;
- MACAK, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict and Security Law*, 2016;
- MACAK, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers*, in *Leiden Journal of International Law*, 2017;
- MACDONALD, *The margin of appreciation in the jurisprudence of the European Court of Human Rights*, in *Collected Courses of the Academy of European Law*, 1992;
- MARGULIES, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State* Responsibility, in *Melbourne Journal of International Law*, 2015;
- MASTRACCI, *Evoluzione del diritto alla privacy tra Europa e Stati Uniti: dal Safe Harbor al Privacy Shield*, in *La Comunità internazionale*, 2016;
- MCKAY, *International Cybersecurityu Norms: Reducing Conflict in an internet-Dependent World*, 2014;
- MILANOVIC, *EctHR Judgment in Big Brother Watch v. UK*, in *EJIL:Talk! Blog of the European Journal of International Law*, 17 settembre 2018;
- MILANOVIC, *Human Rights and Foreing Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal*, 2015;
- MILLER (a cura di), *Privacy and Power*, Cambridge, 2017;
- MOORE, *Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models*, in *Naval Law Review*, 2015;

- MURRAY, *The Regulation of Cyberspace: Control in the online environment*, Routledge, 2007;
- NATOLI, *La internet governance nel sistema internazionale*, in *Federalismi*. *Rivista di diritto pubblico, comparato ed europeo*, 2014;
- NAUGHTON, *The Evolution of the internet: from military experiment to General Purpose Technology*, in *Journal of Cyber Policy*, 2016;
- NINO, *La risoluzione dell'Assemblea Generale delle Nazioni Unite sulla tutela della privacy nell'era digitale: importanti luci, ma non poche ombre*, in *Diritto del commercio internazionale*, 2014;
- NOWAK, *UN Covenant on Civil and Political Rights. CCPR Commentary*, seconda edizione, Kehl, 2005;
- O' CONNELL, *Evidence of Terror*, in *Journal of Conflict and Security Law*, 2002;
- ODDENINO, *Diritto individuali, sicurezza informatica e accesso alla conoscenza in rete: la revisione delle International Telecommunication Regulations dell'ITU*, in *Diritti Umani e Diritto Internazionale*, 2013;
- OPPENHEIM, *International Law*, IX edizione (a cura di Robert Jennings, Arthur Watts), 1992;
- PALCHETTI, *L'Organo di fatto dello Stato nell'illecito internazionale*, Milano, 2007;
- PALCHETTI, *Organi di fatto e illecito dello stato* in SPINEDI, GAINELLI, ALAIMO (a cura di), *La codificazione della responsabilità internazionale degli stati alla prova dei fatti, problemi e spunti di riflessione*, Milano, 2006;
- PALOMBINO, *Introduzione al diritto internazionale*, Bari, 2019
- PATRONO, *Privacy e vita privata (dir.pen.)*, in *Enciclopedia del diritto*, XXXV, 1986;

- PERRITT, *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism*, in *Berkley Technology Law Journal*, 1997;
- PERRITT, *The internet as a Threat to Sovereignty? Thoughts on the internet's Role in Strengthening National and Global Governance*, in *Indiana Journal of Global Legal Studies*, 1998;
- PIRKER, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in ZIOLKOWSKI (a cura di) *Peacetime Regime for State Activities in Cyberspace*, Tallinn, 2013;
- POCHÉ, *This Means War! (Maybe?) – Clarifying Casus Belli in Cyberspace*, in *Oregon Review of International Law*, 2013;
- PROULX, *Babysitting Terrorists: Should States Be Strictly Liability for Failing to Prevent Transborder Attack?*, in *Berkley Journal of International Law*, 2005;
- RANDELZHOFER, *Article 2(4)*, in SIMMA (a cura di), *The Charter of the United Nations: A Commentary*, Oxford, 2002;
- REHOF, *"Article 12",* in ALFREDSSON, EIDE (a cura di)*The Universal Declaration of Human Rights: A Common Standard of Achievement*, L'Aia, 1999;
- RICHARDSON, *Stuxnet as Cyberwfare: Applying the Law of War to the Virtual Battlefield*, in *The John Marshall Journal of Information Technology and Privacy law*, 2011;
- RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973;
- RODOTÀ*, Tecnologia dell'informazione e frontiere del sistema socio-politico*, in *Politica del diritto*, 1982;
- ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2012;

- ROSCINI, *Cyber Operations: Identifying the Problem and the Applicable Law* in *Cyber Operations and the Use of Force in International Law*, Oxford, 2014;
- ROSCINI, *Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes*, in *Criminal Law Forum*, 2019;
- ROSENNE, *The perplexities of Modern International Law*, in *Recueil des Cours de l'Académie de Droit International*, 2004 ;
- ROSENZWEIG, *WCIT Treaty Breakdown – A summary and Some Analysis*, in *Lawfare blog*, 14 dicembre 2012;
- ROWE, *The Attribution of Cyber Warfare*, in GREEN (a cura di), *Cyber Warfare: A multidisciplinary Analysis*, Londra, 2015;
- RUOTOLO, *Internet-ional Law. Profili di diritto internazionale pubblico della Rete*, Bari, 2012;
- RUOTOLO, *Il sistema dei nomi a dominio alla luce delle recenti tendenze dell'ordinamento internazionale*, in *Il diritto dell'informazione e dell'informatica*, 2016;
- RUOTOLO, *internet (diritto internazionale)*, in *Enciclopedia del diritto – Annali vol. VII;*
- RUSINOVA, *A European Perspective on Privacy and Mass Surveillance at the Crossroads*, in *Higher School of Economics Research Paper*, 2019;
- SARTOR, *La rivoluzione informatica e la globalizzazione*, in TORRESETTI (a cura di), *Diritto, polita e realtà sociale nell'epoca della globalizzazione – Atti del XXII Congresso della Società Italiana di filosofia giuridica e politica*, Macerata, 2008;

- SCHACK, *Did the US Stay "Well Below the Threshold of War" With its June Cyberattack on Iran?*, in *Ejil:Talk! Blog of the European Journal of International Law*, settembre 2019;
- SCHMITT, VIHUL, *International Cyber Law Politicized: The Un Gge's Failure To Advance Cyber Norms*, in justsecuriy, 2017;
- SCHMITT, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, in *Chicago Journal of International Law*, 2018;
- SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999;
- SHACKELFORD, CRAIG, *Beyond the New 'Digital Divide': Analyzing the Evolving Role of National Governments in internet Governance and Enhancing Cybersecurity*, in *Stanford Journal of International Law*, 2004;
- SHACKELFORD, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law* in *Berkley Journal of International Law*, 2009;
- SHACKELFORD, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem* in *Georgetown Journal of International Law*, 2011;
- SHACKERLFORD, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge, 2014;
- SHACKLEFORD, RUSSELL, KUEHN, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, in *Chicago Journal of International Law*, 2016;
- SHARP, *Cyberspace and the Use of Force*, 1999;

- SILVER, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in SCHMITT, O'DONNELL (a cura di) *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, International Law Studies, 2002;
- SLOBOGIN, SCHUMACHER, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: an Emipiricla look at 'Understandings Recognized and Permitted by Society*, in *Duke Law Journal*, 1993;
- SMITH, *The Third Industrial Revolution: Law and Policy for the internet*, in *Recueil des cours, 2000*;
- SOLUM, *Models of internet Governance*, in L.A. BYGRAVE, J. BING (a cura di) *internet Governance. Infrastructure and Institutions*, Oxford University Press, 2009;
- SUKUMAR, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, in lawfare blog, 2017;
- TABANSKI, *Basic Concenpts in Cyber Warfare*, in *Military and Strategic Affairs*, 2011;
- TOMMASI, *Articolo 8*, in BARTOLE, DE SENA, ZAGREBELSKY (a cura di), *Commentario breve alla Convenzione Europea dei diritti dell'Uomo*, 2012;
- TONKIN, *State Control over Private Military and Security Companies in Armed Conflict*, Cambridge University Press, 2011;
- TRIFUNOSVSKA, *The Principle of Non-Interference and Cyber Operations*, in *Hungarian Yearbook of International Law and European Law*, 2017;
- TSAGOURIAS e R. BUNCHAN (a cura di), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2015;

- TSAGOURIAS, *Cyber attacks, Self-Defense and the problem of attribution* in *Journal of Conflict and Security Law*, 2012;
- TSAGOURIAS, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, in *Ejil:Talk! Blog of The European Journal of International Law*, 2019;
- TZENG, *Proving Genocide: The High Standards of the Inernational Court of Justice*, in *Yale Journal of International Law*, 2015;
- VON HEINEGG, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013;
- WAGNER, *Global Free Expression-Governing the Boundaries of internet Content*, Berlino, 2016;
- WALDEN, *International Telecommunications Law, the internet and the Regulation of Cyberspace*, in ZIOLKOWSKI (A CURA DI), *Peacetime Regime for State Activities in Cyberspace Interantional Law, International Relations and Dipomacy*, Tallinn, 2013;
- WARREN, BRANDEIS. *The Right to Privacy*, in *Harvard Law Review*,1890;
- WATTS, *Cyber Law Development and the United States Law of War Manual*, in OSULA, ROIGAS (A CURA DI) *International Cyber Norms: Legal, Policy and Industry Perspectives*, CCDCOE, Tallin, 2016;
- WAXMAN, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, in *Yale Journal of International Law*, 2011;
- WEBER, *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles*, Berlino, 2015;
- WEINBERG, *Non State Actors and Global Informal Governance: the case of ICANN*, in CHRISTIANSEN, NEUHOLD (A CURA DI), *International Handbook on Informal Governance*, Cheltenham, 2012;

- WEISSBRODT, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, in *Minnesota Journal of International Law*, 2013;
- WHITEHEAD, ADEN, *Forfeiting "Enduring Freedom" for "Homeland Security": A Costituional Analysis of the USA Patriot Act and the Justice Department's Anti-Terrorism Iniziatives*, in *American University Law Review*, 2002;
- WOLFRUM, MOLDNER, *International Courts and Tribunals, Evidence*, in WOLFRUM (a cura di), *Max Planck Encyclopedia of Public International Law*, 2013;
- WOLTAG, *Computer Network Operations Below the Level of Armed Force*, in *ESIL Conference Paper Series*, Conference Paper No. 1/2011, 2011;
- WOLTAG, *internet*, in *Max Planck Encyclopedia of Public International Law*, 2010;
- WU, *Cyberspace Sovereignty? The internet and the International System*, in *Harvard Journal of Law and Technology*, 1997;
- XINMIN, *Key Issues and Future Development of International Cyberspace Law*, in *China Quarterly of International Strategic Studies*, 2016;
- ZIOLKOWSKI, *Confidence Building Measures for Cyberspace - Legal Implications*, Tallin, 2013;
- ZIOLKOWSKI, *Stuxnet – Legal Considerations*, in *Journal of International Law of Peace and Armed Conflict*, 2012;
- ZURBUCHEN, *Vattel's 'Law of Nations' and the Principle of NonIntervention*, in *Grotiana*, 2010;