DIPARTIMENTO DI GIURISPRUDENZA

Cattedra di Organizzazioni internazionali

IL RUOLO EMERGENTE DELLE ORGANIZZAZIONI INTERNAZIONALI NELLA TUTELA DEL *CYBERSPACE*

RELATORE:
Chiar.mo Prof. **Pietro Pustorino**

CANDIDATO:
Marco Zanfini
Matricola 138273

CORRELATORE:
Chiar.mo Prof. **Roberto Virzo**

ANNO ACCADEMICO 2020-2021

INDICE

Introduzione

"Technology is a useful servant but a dangerous master"[1].

— Christian Lous Lange, Nobel Lecture, 1921.

La preoccupata ma accorta visione, espressa nel 1930 dal politico norvegese Christian Lous Lange, vincitore del Nobel per la pace nel 1921, è una visione che può essere facilmente accostata ai giorni nostri, a distanza di così tanto tempo. La tecnologia si è rivelata uno strumento fondamentale per il progresso sociale, un mezzo per tutti gli stati col fine di ottimizzare vantaggi e tempistiche e per cercare di essere sempre un passo avanti agli altri. La forza innovativa della tecnologia, espressa prevalentemente attraverso l'istituzione di internet, si valorizza tramite la capacità concreta di rompere barriere e confini territoriali, di connettere miliardi di persone a distanza in pochi secondi nonché di dare la possibilità di scambiarsi informazioni e notizie in brevissimo tempo.

Il primo tentativo, da un punto di vista prettamente storico, di connessione fra plurimi dispositivi tramite l'utilizzo di una rete si verifica a partire dalla creazione, effettuata da una compagnia americana **(***Bolt Beranek and Newman Inc*. al tempo, oggi denominata BBN TECHNOLOGIES), di *ARPANET*. Questo sistema fu istituito con un'idea ben precisa, ovvero creare un sistema di comunicazione aperto per quattro computer differenti connettendo di conseguenza gli users di quattro università distinte: *the University of California, Los Angeles (UCLA); the Stanford Research Institute in Menlo Park, California; the University of California, Santa Barbara;* e *the University of Utah.* Questi

[1] Lange, C. (1972). *Nobel Lecture, Peace 1901-1925*. NobelPrize.org. Nobel Media AB 2020. https://www.nobelprize.org/prizes/peace/1921/lange/lecture/ Editore Frederick W. Haberman, Amsterdam: Elsevier Publishing Company. (Traduzione inglese dell'originale del 1921).

quattro nodi hanno creato il *Network Working Group*[2]. Tramite questo sistema veniva data la possibilità agli users di accedere a computer e stampanti collocati materialmente in località differenti, dando anche la possibilità di trasportare files tra i vari dispositivi. Successivamente il network si è sviluppato e ampliato, dando la possibilità a nuove istituzioni tra le quali *Harvard* e l'università dell'*Illinois* di utilizzarlo. *Arpanet* si è rivelatala prima rete di computer avanzata al mondo ad utilizzare la *commutazione dei pacchetti*.[3] Già sul finire del 1973 il *network* contava 35 nodi e una connessione con ben 38 computer.

La prima volta in cui è stato utilizzato il termine "*internet-working*" risale al 1974, in una definizione fornita da Vint Cerf and Robert Kahn tramite il loro articolo "*Transmission Control Protocol*".[4] È tuttavia solo a partire dalla seconda metà degli anni Novanta che il fenomeno di internet e di connessione globale e costante, inteso come lo intendiamo ai giorni nostri, inizia a svilupparsi.

Questo modello di connessione incessante e di utilizzo continuo di strumenti informatici, alla luce della digitalizzazione che tutti gli stati del mondo sono portati ad affrontare, innesca, accanto ad innumerevoli vantaggi, una serie di problemi che andranno ad essere trattati nel seguente elaborato.

Il primo elemento da prendere in considerazione attiene essenzialmente all'ambito di una necessaria uniformità di definizioni di elementi che connotano il *cyberspace.* Essendo questo un mondo essenzialmente "recente", privo di

---

[2] Cohen-Amagor, R. (2015, giugno). *Confronting the internet's dark side moral and social responsibility on the free highway*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9781316226391. (Vedi p. 2).

[3] Treccani. (2020). *Commutazione di pacchetto*. Enciclopedie on line, Istituto della Enciclopedia Italiana: «Tecnica impiegata nelle telecomunicazioni per effettuare lo scambio di dati tra i nodi di una rete instaurando un circuito virtuale tra i nodi e/o le applicazioni da interconnettere. L'insieme dei dati da trasferire viene segmentato in più pacchetti, ognuno dei quali è immesso in rete dal nodo sorgente e raggiunge il nodo desiderato venendo instradato da ogni nodo di commutazione intermedio verso il nodo successivo, fino a destinazione; qui i pacchetti ricevuti sono assemblati a formare l'insieme di dati originale […]». Consul. da https://www.treccani.it/enciclopedia/commutazione-di-pacchetto_%28Lessico-del-XXI-Secolo%29/#:~:text=commutazi%C3%B3ne%20di%20pacch%C3%A9tto%20s.%20f.%20%E2%80%93%20Tecnica,o%20le%20applicazioni%20da%20interconnettere.

[4] Cerf, V. G., & Kahn, R. E. (1974, maggio). A Protocol for Packet Network Interconnection. *IEEE Transactions on Communications*, 22(5), 637–48.
https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf

delimitazioni fisiche e di confini territoriali, l'inquadramento delle possibili attività che possono essere legittimamente attuate dai due principali attori nel panorama cibernetico assume particolare rilevanza; tra queste le attività poste in essere dagli *state-actors* e dai *non-state actors*.

Difatti, accanto ad una visione tradizionale che dovrebbe essere data al tema dello sviluppo tecnologico come mezzo per implementare e migliorare le condizioni di vita di chiunque, si sta sviluppando sempre di più una visione distinta e differente, caratterizzata dalla possibilità di utilizzare gli strumenti cibernetici e il *cyber world* come armi o strumenti per colpire altri stati o attori non-statali. Stante questa seconda visione, è necessario ricordare come le varie attività abbiano concretamente il poter di causare ingenti danni non solo e unicamente agli strumenti necessari per corretto svolgimento di funzioni ad oggi prevalentemente digitalizzate degli stati, ma vi è altresì la possibilità concreta di causare danni a persone o all'intera economia di un paese.

Le condotte tipiche, che saranno trattate specificatamente nel capitolo 1, attengono al tema dei *cyber attacks*, ovvero attacchi cibernetici che possono essere effettuati con differenti fini. Le condotte possono essere di conseguenza di vario tipo e di forza distinta dal momento che possono svilupparsi in una "semplice" attività di spionaggio, inquadrabile tuttavia nel contesto di *cyber exploitation*, tramite collezione di dati o attività di *intelligence*, oppure possono comportare la cancellazione, l'alterazione, o l'inserimento di malware all'interno di *software* e sistemi che possono causare varie e forti ripercussioni sull'operatività del sistema informatico stesso[5].

Il secondo punto che merita di essere trattato attiene alla concreta mancanza di una normativa uniforme in grado di fornire una chiara regolamentazione in tema di *cyber-activity*. Pur avendo accertato che la normativa per attività cibernetiche effettuate fra vari soggetti che risiedono in stati differenti deve cadere

[5] Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press. (Vedi p. 2).

inevitabilmente all'interno del diritto internazionale, è altresì possibile vedere come nel corso del tempo plurimi tentativi di creare una normativa unitaria, la maggior parte dei quali a vuoto, siano stati effettuati. Difatti, unicamente un trattato è stato ratificato con l'obiettivo espresso di obbligare gli stati firmatari a criminalizzare, nella propria sfera di competenza legislativa, determinate attività cibernetiche. Si tratta della *Budapest Convention on Cybercrime* [6], tenuta nel 2001 ed entrata in vigore a partire dal primo di luglio 2004.

Quel che risulta particolarmente interessante, tuttavia, attiene al fatto che, pur mancando effettivamente una normativa uniforme, non vi è possibilità di realizzare una qualsiasi tipologia di attività senza concrete restrizioni. Dette restrizioni, che verranno meglio analizzate nel cap.3 , si ricavano da quanto stabilito in trattati precedentemente esistenti che non fanno espressamente riferimento alle *cyber-activities* ma che estendono la propria competenza anche al ramo cibernetico sulla base dei normali principi interpretativi che si possono ricavare dalla Convenzione di Vienna sui Trattati, ratificata il 23 Maggio 1969 e che si esplicano nella necessità di interpretare quanto stabilito dal trattato adattandolo ai tempi correnti.

Il terzo punto che sarà trattato è relativo al ruolo fondamentale che oggi viene svolto dalle varie organizzazioni internazionali in tema di *cyber-security* e *cyber-activity*. Sono due le grandi organizzazioni internazionali che nel corso del tempo si sono con particolar forza e vigore interessate al tema della *cyber-security* come tema necessario per la tutela degli obiettivi dalle stesse prefissati: le Nazioni Unite e la Nato. Questa legittimazione ad operare anche nel panorama del *cyberspace* viene fornita sulla base dell'evoluzione interpretativa dei trattati discussa precedentemente, in particolare dell'art. 2 e 51 della Carta delle Nazioni Unite[7], e dell'art. 5 del Trattato del Nord-Atlantico[8].

---

[6] Council of Europe. (2001, 23 novembre). *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

[7] United Nations, Charter art. II, para. 3: «*All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered*».

La NATO ha già adottato e creato al suo interno a partire dal 2007 il "*Cooperative Cyber Defence Centre of Excellence*" (CCDCOE), con il compito fondamentale di dare supporto alle nazioni che fanno parte della NATO, fornendo alle stesse un gruppo di esperti con competenze interdisciplinari uniche nel campo della ricerca, della formazione e delle esercitazioni in materia di difesa informatica, che coprono le aree di interesse della tecnologia, della strategia e del diritto[9]. Compito fondamentale è quello al tempo stesso di favorire la cooperazione cibernetica tra gli alleati NATO.

Alla stregua degli elementi sopra esposti, il seguente elaborato tratterà le concrete attività svolte in tema di mantenimento della sicurezza e della pace da parte delle Nazioni Unite ed in particolare l'eventuale creazione di un organo autonomo, dentro l'organizzazione stessa, con il compito di tutelare e mantenere la pace nel panorama del cyberspazio. In particolare, verrà fatto riferimento all'eventuale struttura, natura, personalità e regimi di responsabilità in cui potrebbe incorrere un organo come quello ipotizzato.

U.N. Charter art II, para *4: «All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations»*.
Consultato da https://www.un.org/en/sections/un-charter/chapter-i/index.html

[8] The North Atlantic Treaty. (1949, 4 aprile). Art. V*: «The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defense recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area […]»*.
Consultato da https://www.nato.int/cps/en/natolive/official_texts_17120.htm

[9] The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *About us*. Consultato da https://ccdcoe.org/about-us/

Capitolo 1
IL *CYBERSPACE*

SOMMARIO: 1.1. Cenni storici - 1.2. Il cyberspazio - 1.3. La guerra cibernetica : i concetti di *cyber war* e *cyber warfare* - 1.4. Diverse tipologie di *cyber-activities*: *cyber exploitation*, *cyber espionage* e *cyber attack* – 1.4.1. La nozione di *cyber exploitation* - 1.4.2. La nozione di *cyber espionage*– 1.4.3. La nozione di *cyber attack* - 1.5. Cyberterrorismo: I pericoli derivanti dall'ISIS - 1.6. I concetti di *cyber defence* e *cyber security* – 1.6.1 La nozione di *cyber defence* – 1.6.2 La nozione di *cyber security* – 1.7 I sistemi di difesa statali nel cyber spazio: Italia, Spagna, Russia e Cina

1.1 Cenni storici

Lo studio del mondo cibernetico, come rilevato in precedenza, è un fenomeno che si contraddistingue per il fatto di essere prevalentemente moderno. L'eliminazione sempre maggiore della scomodità logistica cartacea, la ricerca da parte degli stati (gli Stati Uniti su tutti) di primeggiare in un mondo tanto nuovo quanto pericoloso e il processo di digitalizzazione, con conseguente e apparente scorporo dall'elemento della materia, ha portato a confrontarsi con problemi di sempre più difficile soluzione e che comportano un necessario bilanciamento tra i vari interessi in gioco.

L'esempio più lampante e pratico che può essere fornito da un punto di vista giuridico attiene al bilanciamento necessario tra l'elemento della sicurezza nazionale e la necessaria tutela di un diritto riconosciuto non solo da un punto di vista statale ma anche e soprattutto da un punto di vista internazionale: il diritto alla *privacy*. Questo diritto, garantito tra l'altro dalla *European Convention of Human Rights* all'art.8 della stessa[10], si sviluppa in due cognizioni distinte: sia,

[10] Council of Europe. *European Convention for the Protection of Human Rights and Fundamental Freedoms*, modificata dai Protocolli No. 11 and 14, 4 Novembre 1950, ETS 5, https://www.refworld.org/docid/3ae6b3b04.html

Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, Art. VIII, para. I: *«Everyone has the right to respect for his private and family life, his home and his correspondence»*. Art. VIII, para. II *«There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for*

difatti, in ottica di un rapporto intrusivo Stato-Cittadino, sia in ottica di un rapporto Stato-Stato.

L'esempio più chiaro di quest'ultimo attiene al complicato rapporto Stati Uniti-Russia. Questo rapporto, già storicamente "problematico", si è sviluppato negli ultimi anni anche da un punto di vista cibernetico, con il famoso attacco da parte di due gruppi dell'intelligence Russa, effettuati contro la candidata Hillary Clinton durante le elezioni presidenziali del 2016[11]. Il 14 giugno del 2016 è stato lanciato un *cyber attack* contro la "*Democratic National Committee*" (DNC)[12], esattamente nel mezzo della campagna elettorale. Gli effetti di detto attacco si svilupparono a partire dal 22 di giugno, giorno in cui *Wikileaks*[13] decise di pubblicare 20.000 e-mail e 8.000 allegati scambiati tra i vari capigruppo della DNC. Quello che è necessario notare è che gli effetti concreti di queste pubblicazioni comportarono un danno non indifferente, tenuto conto della vicinanza alle elezioni stesse. Questo esempio porta inevitabilmente alla luce una serie di problemi e possibili difficoltà che saranno trattate nel seguente capitolo. Le evidenze maggiori che devono essere prese in considerazione attengono alla possibilità che determinate attività, seppur astrattamente lontane, siano in grado di andare a produrre effetti non solo nella vita di grandi esponenti politici ma nella vita di chiunque.

Per questo motivo, infatti, l'ambito della *privacy* e del diritto alla riservatezza deve essere tutelato. Al giorno d'oggi, come fa brillantemente notare il Professor Gerardo Iovane, «la gran parte delle infrastrutture che presidiano i fondamentali

---

the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others».

[11] Lam, C. (2018, giugno). A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election. *59 Boston College Law Review,* 2167-2201.

[12] Democratic National Committee, Official Website. (n.d.). Consultato da https://democrats.org/who-we-are/

[13] Wikileaks. (2015, 3 novembre). *What is WikiLeaks.* Definizione tradotta: «WikiLeaks è un organizzazione internazionale la quale, senza scopo di lucro, riceve, analizza e pubblica documenti ufficiali ristretti, riguardanti guerre, spionaggio e corruzione». Consultato da: https://wikileaks.org/What-is-WikiLeaks.html

settori delle società moderne, quali Economia, Energia, Trasporti, Telecomunicazioni, Salute sono dipendenti e interconnesse mediante sistemi di rete che garantiscono il corretto svolgimento della vita»[14]. La necessità di avere non solo adeguati sistemi di protezione e di difesa contro eventuali intrusioni, ma anche quella di ottenere dal legislatore una concreta e definita normativa sul regime applicabile ai contrasti cibernetici si fa sempre più impellente. In particolare, tenuto conto dell'importanza che da sempre assumono le infrastrutture suddette, la potenziale forza distruttiva che potrebbe avere un'intrusione esterna, tanto sull'economia nazionale quanto anche sul funzionamento concreto dei vari apparati statali, è difficilmente calcolabile. Questa forza, di conseguenza, non si esplica semplicemente nella possibilità di avere "banali" attività di hackeraggio di dati ma altresì si rafforza nella possibilità di comportare scenari più gravi: disattivare i generatori di energia, interrompere i sistemi militari di comando, controllo e comunicazione o ancora causare il deragliamento o la collisione tra due o più aerei, l'accensione di reattori nucleare o la paralisi totale di determinati sistemi bancari.

Un esempio attuale di *cyber attack* è quello che ha portato una nazione come il Kyrgyzstan fuori dalla Rete per un periodo di tempo di 12 ore a causa di un attacco *Denial of Service*[15] ai danni dei principali *provider*. Quello che ci si potrebbe chiedere è cosa sarebbe successo se il bersaglio di questo attacco fosse stata una delle superpotenze mondiali quali Stati Uniti, Russia o Cina.[16]

---

[14] Iovane, G. (2008). *Cyberwarfare e Cyberspace: Aspetti Concettuali, Fasi ed Applicazione allo Scenario Nazionale ed all'ambito Militare* [Tesi di dottorato, DIMA Università degli Studi di Salerno]. Cons. da http://www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/46644_ricerca_2pdf.pdf (Vedi p. 9).

[15] Treccani. (2020). *Denial of service.* Enciclopedie on line, Istituto della Enciclopedia Italiana: "attacco informatico consistente nell'occupare tutte le risorse di un sistema, impedendogli il corretto funzionamento.

[16] Iovane, *op. cit*. (Vedi p. 62)

1.2 Il cyberspazio

Il termine *cyberspace* fu coniato per la prima volta nel 1982 da William Gibson. Il cyber-spazio è un mondo contraddistinto da tre differenti caratteristiche: giovinezza, modernità e autorganizzazione. È giovane poiché solo il 6 agosto 1991 nasce il *World Wide Web*, uno dei più importanti servizi di internet che permette di reperire informazioni tramite un modello di rete definito *Client-Server*. È moderno, poiché si colloca in un mondo in continuo mutamento ed ha la capacità di adattarsi in pochi secondi a qualsiasi cambiamento. È infine autorganizzato, poiché è in grado di rispondere "autonomamente" a tutte le modificazioni cui è soggetto[17]. L'avvento di questo mondo ha portato conseguenze estese sulla vita di chiunque e ciò si esplica altresì nel conferimento di un certo quantitativo di potere dato a singoli individui, organizzazioni e stati che difficilmente si sarebbe potuto immaginare. Vari e plurimi nomi sono stati utilizzati per denominare questa cosiddetta "era digitale": l'età dell'informazione, di internet, del computer, di *Google*. Qualsiasi posto sulla terra è sotto l'influenza del *cyberspace*, pur non rendendosi molto spesso gli individui conto di detto potere che li circonda.

Uno dei poteri più forti è senza alcun dubbio la possibilità di ottenere e fornire informazioni in un brevissimo spazio di tempo tramite l'utilizzo di internet. La forza, potenzialmente distruttiva, dell'informazione non risiede tanto nell'informazione stessa quanto sulla velocità della circolazione. Elemento da non sottovalutare inoltre è, soprattutto, l'incapacità nella maggior parte dei casi di riuscire concretamente a riconoscerne o meno la veridicità. Molto spesso, infatti, gli individui si trovano circondati da questo problema all'apparenza innocuo ma che si sta rivelando di sempre maggior interesse anche da parte degli stati. Difatti, la forza di informazioni non veritiere di difficile interpretazione pone di fronte ciascuno ad una necessaria verificazione delle stesse, cosa che

[17] Harries, D. (2017). Narrative Mapping of Cyberspace. Context and Consequences. In J. Martín Ramírez Luis & A. García-Segura (Cur.), *Cyberspace Risks and Benefits for Society, Security and Development* (pp. 23-40). Berlino: Springer.

nella maggior parte dei casi non avviene. La diffusione di dette *fake news* crea problemi a livello di democraticità e socialità alla stregua di tre elementi: una distorsione della realtà percepita dai cittadini (*Wrongly Informed Citizens*), una permanenza degli stessi in questa situazione irreale (*Echo Chambers: Staying Wrongly Informed*) e una capacità delle notizie stesse, per loro natura solitamente provocatoria, di creare negli individui uno stato di angoscia e frustrazione continua (*Affective Content*)[18].

Il primo punto, che si rifà alla distorsione della realtà percepita dai cittadini, si esplica in minore tutela della democraticità che è alla base della maggior parte degli stati del mondo. La capacità distruttiva di queste mistificazioni della realtà si riverbera in scelte non dettate da logicità e basate su elementi fattuali erronei dei quali sono vittime incoscienti i cittadini stessi.

Il secondo punto "*staying wrongly informerd*" si esplica nella mancata contromisura da attuare contro questo fenomeno che si sta diffondendo sempre con maggior frequenza. L'impossibilità di controllare efficacemente tutte le informazioni che circolano nel *Web*, le difficoltà relative all'adozione di una definizione generale di *fake news* e la conseguente incapacità di adottare un'autonoma normativa che, da un punto di vista legislativo, sia in grado di regolare detto fenomeno, i problemi di attribuzione per la creazione di dette notizie che influenzano inevitabilmente vita e pensieri di molti, sono solo i principali interrogativi che vengono alla luce.

Il terzo punto, infine, si esplica nella situazione di angoscia, frustrazione e rabbia che riescono ad ottenere queste *fake news,* facendo prevalentemente leva sull'esistenza di situazioni problematiche persistenti nel tempo. Queste notizie non vengono difatti scelte casualmente, come non vengono scelti casualmente i soggetti cui sono dirette; sono frutto di un attento studio avente carattere

[18] Bakir, V., & McStay, A. (2018). Fake News and The Economy of Emotions. *Digital Journalism*, 6(2), 154-175. Consultato da https://doi.org/10.1080/21670811.2017.1345645

sociologico e vengono diffuse cercando i terreni più fertili possibile. La forza di dette *fake news* può anche essere riportata e analizzata tramite un recente evento storico – trattato sotto diverse forme nel presente elaborato – ossia l'influenza che la creazione di dette notizie ha portato sull'esito, favorevole al candidato del Partito Repubblicano Americano Donald Trump, delle elezioni americane del 2016. Uno studio effettuato da Alexandre Bovet, ricercatore presso l'università di Oxford, e da Hernan Maske, professore di fisica presso il *Levich Institute*, ha preso in considerazione un quantitativo delineato di notizie diffuse tramite *Twitter* nei cinque mesi antecedenti le elezioni del 2016. Sulla base di un campione elevato di 171 milioni di *tweets*, è stato possibile tracciare una delimitazione pari a 30 milioni degli stessi, condivisi da 2.2 milioni di utenti, i quali contenevano un rimando tramite *link* a varie testate. Sulla base di una classificazione delle varie testate realizzata da *opensource.co*[19], è stato riscontrato che il 25% di detti *tweets* diffondevano *fake news* o notizie fortemente di parte, andando a comportare un'erronea valutazione delle caratteristiche dei due candidati a supporto del candidato repubblicano.[20]

In aggiunta, i problemi che derivano da dette notizie si traducono in effetti dannosi nei confronti del singolo cittadino ma soprattutto in effetti disarmanti per l'economia del paese, quantomeno in uno spazio temporale definito come breve periodo. Come analizzato dall'elaborato di Vincenzo Visco Comandini, docente di economia politica presso l'Università di Tor Vergata (Roma), il fenomeno delle *fake news* può essere studiato alla stregua degli effetti che le stesse hanno nel rapporto classico domanda-offerta. Difatti, il veicolo principale di dette notizie risulta essere, al giorno d'oggi, uno strumento utilizzato dalla quasi totalità della popolazione mondiale: i *social network*. Questo avviene per due ragioni fondamentali: la prima attiene all'assenza di barriere all'entrata, la seconda riguarda la facilità d'accesso a informazioni preconfezionate, all'interno

[19] Opensource. (n.d.). *Official Website.* Consultato da https://opensource.com/

[20] Bovet, A., & Makse, H. A. (2019, 2 gennaio). Influence of fake news in Twitter during the 2016 US presidential election. Nature Communications, 10(7). Da https://doi.org/10.1038/s41467-018-07761-2

di suddetti siti. Per quanto riguarda le barriere all'ingresso, è possibile constatare come le stesse siano quasi nulle, data la facilità e la velocità con cui è possibile creare siti *web* e ricavarne utili tramite le pubblicità. Per quanto invece attiene alla seconda ragione, la facilità di ottenere informazioni preconfezionate è dimostrata dalla totale velocità con cui le stesse sono solite passare sulle schermate, tramite una semplice attività che oggi viene definita "*scrolling*"[21]. Alla stregua di questi due elementi, è possibile vedere come sia relativamente semplice influenzare la volontà dei singoli individui, modificando, sulla base di informazioni erronee, la curva di domanda.[22]

Accanto al problema delle *fake news*, che potrebbe apparire ai più un problema limitato, nuove difficoltà sono sorte a seguito della creazione di questo mondo. Essendo oggi quasi tutto digitalizzato, il problema della difesa dei vari sistemi informatici viene a consolidarsi come uno dei principali argomenti che gli stati si trovano a trattare. È sufficiente pensare a cosa potrebbe succedere se un determinato stato, una determinata organizzazione o ancora un singolo individuo, con capacità informatiche decisamente superiori al normale, riuscisse ad insediarsi in siti istituzionali, riguardanti per esempio l'energia, la gestione del traffico aereo o navale, o ancora siti concernenti l'energia nucleare. Lo scenario che verrebbe a considerarsi esulerebbe totalmente dallo spazio digitale che ha dato il via ad un eventuale processo riguardante l'energia nucleare, andando a causare paure e danni incalcolabili alla popolazione stessa. Sono proprio queste motivazioni che hanno portato non unicamente gli stati ma anche le varie organizzazioni internazionali, in particolare quelle che hanno come obiettivo principale quello della tutela della pace fra i vari stati del mondo, a concentrare le loro forze nella creazione di strumenti e organismi con vari compiti da un punto

[21] Treccani. (2020). *Scrolling.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «In informatica, lo scorrimento in senso orizzontale o verticale di un testo o di un'immagine sullo schermo di un calcolatore in modo tale che questi scompaiano in un lato dello schermo e nuovi dati appaiano dal lato opposto». https://www.treccani.it/enciclopedia/scrolling/

[22] Comandini, V. V. (2018, 25 giugno). Le *fake news* sui social network: un'analisi economica. *Saggi – Fake news, pluralismo informativo e responsabilità di rete*, 183-212. http://www.medialaws.eu/wp-content/uploads/2018/06/Visco-Comandini.pdf

di vista informatico. Come sarà approfondito nel terzo capitolo, le Nazioni Unite si sono dotate dei cosiddetti "*Digital Blue Helmets*", un team composto da esperti qualificati in materia di *cybersecurity*, specializzato nel monitoraggio di eventi, operazioni, test ambientali e *digital forensic*, cioè la scienza forense che si occupa del trattamento di dati digitali di qualsiasi tipo allo scopo di rilevare prove informatiche utili all'attività investigativa.[23] Questi *Digital Blue Helmets*, tuttavia, hanno solo e unicamente il compito di proteggere le informazioni e i siti istituzionali delle Nazioni Unite.

Un ultimo elemento che verrà qui trattato attiene al tema, sempre più pericoloso, del *Dark Web*. Quest'ultimo però deve essere differenziato, cosa che spesso non avviene, dal più generale *Deep Web*. Come analizzato infatti dal giornalista Matt Egan, il mondo di internet è molto più vasto di quello che di solito si è abituati a pensare. Il *Deep Web* si riferisce a tutte le pagine web che i motori di ricerca non riescono a trovare; di conseguenza, si può facilmente constatare come il *dark web* altro non sia se non un sottoinsieme del *deep web*[24]. Come analizzato brillantemente da vari studiosi, i gruppi terroristici sono soliti diffondere le proprie ideologie e le proprie motivazioni in siti che possono essere trovati solo e unicamente nel *dark web.* A tal proposito, sono state evidenziate cinque tipologie di attività tipiche dei gruppi terroristici nel mondo del *dark web* – che verranno spiegate più dettagliatamente nel sottoparagrafo relativo al tema di "*cyber terrorism*" – e vengono catalogate come segue: attività di propaganda, reclutamento e preparazione, richiesta fondi, scambio di informazioni e *targeting*, ovvero attività di identificazione di obiettivi potenzialmente vulnerabili. [25]

[23] United Nations. (n.d.). *Cyber Risk.* Consultato da https://unite.un.org/digitalbluehelmets/cyberrisk

[24] Egan, M. (2019, 25 settembre). *What is the Dark Web, What's on it & How to Access it.* Tech Advisor. https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/ (visitato il 28 ottobre 2020).

[25] Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*, 59(8), 1347–1359. Doi: 10.1002/asi.20838

Il *dark web*, non essendo raggiungibile dai classici motori di ricerca, quali i vari *Google, Bing, Baidu, Qwant* e altri, sovrapponendosi alle normali reti, comporta sempre maggiori difficoltà per l'accesso, aumentando così la possibilità di nascondere materiale commerciale illegale. Infine, il *dark web* viene di conseguenza utilizzato non solo e unicamente da gruppi terroristici; viene utilizzato per lo scambio di merce illegale, per la commissione di crimini informatici, per la condivisione di *file* che vengono solitamente piratati e per il commercio illegale di droghe.

Tutti questi problemi mettono in luce il sentimento di preoccupazione esposto da stati e organizzazioni internazionali relativamente al mondo cibernetico e alla necessità di una tutela uniforme, da un punto di vista giuridico necessaria sia a fini definitori delle varie attività che ogni giorno vengono poste in essere sia per quanto riguarda la necessità di una criminalizzazione omogena delle stesse.

1.3 La guerra cibernetica: i concetti di *Cyber war* e *cyber warfare*

> *Cyberwar*: "*Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the balance of information and knowledge in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended*".[26]
>
> *Cyber warfare: "The warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances".*[27]

[26] Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is coming!*. Santa Monica, CA: RAND Corporation. Consultato da http://www.rand.org/pubs/reprints/RP223.html

[27] Taddeo, M. (2012). An analysis for a just cyber warfare. *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1-10.

Partendo dallo studio di queste due distinte definizioni, è possibile constatare come nel corso della storia lo stesso concetto di guerra si sia evoluto notevolmente. La volontà di ottenere territori sempre più ampi e di sottomettere popolazioni di altri stati, ampliando di conseguenza la propria supremazia ed egemonia, ha portato a scontri che si sono evoluti anche e soprattutto sul piano metodologico. Dalla classica battaglia sul campo di guerra condotta da eserciti schierati fisicamente, l'evoluzione e la diplomazia hanno comportato cambiamenti radicali, a partire dalla creazione di armi di distruzione di massa come le armi nucleari. La paura di dette armi si evolve anche alla stregua della digitalizzazione, se si parte dal presupposto che alla minaccia di utilizzo di armi nucleari da parte dei possidenti delle stesse si è affiancata la minaccia di intrusione da parte di altri stati, gruppi terroristici o singoli individui nei *server* che regolano e gestiscono l'utilizzo delle armi sopra ricordate.

L'evoluzione ha generato, altresì, un concetto di guerra che viene a svilupparsi anche in seno a concezioni distinte; infatti, accanto alle tradizionali armi utilizzate normalmente si sono affiancate armi innovative, che hanno portato a riconsiderare l'elaborazione stessa del concetto di conflitto. Oggigiorno, non trattandosi più di scontri su un campo di battaglia solo fisico e materiale, campo che ormai è stato in maniera concreta ridotto, l'attenzione si è spostata sul campo dell'informatica e su questi nuovi strumenti messi a disposizione di stati o individui per attaccare digitalmente. In questo contesto, come rilevato da plurime fonti, sorge la necessità di ampliare il classico concetto di "*war*", andando ad includere ma soprattutto a differenziare tre elementi distinti: *"cyber attack", "cyber warfare*" e "*cyber war*"[28]. Questi tre concetti, che si contraddistinguono per la difficoltà di fornire una unitaria definizione, sono frutto di studi concreti sviluppati nel corso degli anni. È possibile asserire che la definizione di *cyber*

[28] Robinson, M., Jones, K., & Janicke, H. (2015, marzo). Cyber warfare: Issues and challenges. *Comput. & Secur*. 49(2015), 70–94. DOI: 10.1016/j.cose.2014.11.007

attack, tema che sarà trattato specificatamente nel capitolo, riprende il concetto di operazione cibernetica, offensiva o difensiva, in grado, ragionevolmente, di causare danni come lesioni e addirittura morte di persone o ancora danni e distruzione per diversi oggetti[29]. Il danno preso in considerazione viene ad ottenere una dimensione particolarmente ampia, potendo andare a esplicarsi come danno economico, psicofisico e psicologico. Accanto al danno, un ulteriore elemento, che a breve sarà trattato in maniera più ampia, è quello dell'intenzione. Per *cyber warfare*, invece, si intende l'utilizzo di attacchi cibernetici con intento ostile. Infine, il termine *cyber war* indica quella situazione che si verifica in seguito alla realizzazione di due distinti presupposti: la dichiarazione di guerra da parte di uno stato-nazione (anche se, per il diritto internazionale contemporaneo, non risulta necessario che sia effettuata in forma esplicita[30]) e lo svolgimento, in maniera unicamente cibernetica, di detta guerra. Di conseguenza, la macro-distinzione che può essere tracciata è che la *cyber warfare* è semplicemente un'attività mentre il concetto di *cyber war* è ricollegabile ad uno stato d'essere continuo.

Al fine di fornire un quadro generale corretto, risulta obbligatorio andare ad esaminare uno dei più efficaci metodi utilizzati per riuscire a carpire quando sia necessario parlare di attività cibernetica, metodo che si rifà a due elementi: intento e autore[31]. Per quanto riguarda il primo punto è possibile vedere come, per poter correttamente parlare di *cyber warfare*, sia importante valutare l'intento del soggetto che ha attuato l'attività cibernetica. Un esempio di intento riconducibile al *cyber warfare* è quello di raggiungere obiettivi militari. Il secondo punto fa invece riferimento all'attore che ha realizzato suddetta attività; pur essendo un elemento autonomo, la considerazione sull'attore è rilevante

[29] Schmitt, M. N. (Cur.). (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf. (Vedi p. 106).

[30] Eagleton, C. (1938). *The form and function of the declaration of war*. *Am. J. Int'l L., 32*, 19.

[31] Robinson, *op. cit.*, p. 18. (Vedi pp. 74-75).

anche ai fini della definizione dell'intento che lo stesso ha perseguito. Per spiegare quest'ultimo punto sarà fondamentale rifarsi al caso in cui l'attore considerato sia uno stato oppure sia semplicemente un individuo. Nel primo caso, molto più immediato sarà il nesso con il "*warfare intent*", a differenza di quanto avviene nel secondo caso. Ancora, se l'attribuzione di un *cyber attack* viene a focalizzarsi su un gruppo terroristico, il collegamento al "*warfare intent*" sarà di conseguenza più diretto.

1.4 Diverse tipologie di cyber-activities*: cyber exploitation, cyber espionage* e *cyber attack*

1.4.1 Nozione di *cyber exploitation*

Per spiegare concretamente la natura dell'attività che si esplica nella *cyber exploitation* può risultare utile compararla ad una serie di elementi che la accomunano e la differenziano dal *cyber attack.* Sulla base di questa visione comparatistica, è possibile asserire che l'attività di *cyber exploitation* viene generalmente considerata come un comportamento ostile realizzato contro una rete di computers[32]. Mentre da un lato – come sarà ripreso meglio al termine del paragrafo – un *cyber attack* si concretizza in un attacco diretto contro una rete di computers, avente come risultato quello di causare danni ad oggetti, lesione o morte, dall'altro, l'attività di *cyber exploitation* si esplica nel tentativo di ottenere informazioni residenti o in transito attraverso sistemi o reti di computer avversari. Punto cardine di questa attività risulta essere lo svolgimento di una "semplice" raccolta di informazioni, la quale non va a colpire il corretto funzionamento dell'attività di rete, che invece è l'elemento fondamentale della natura, prevalentemente distruttiva, di un attacco cibernetico. Il punto comune che attiene ad entrambe le attività risiede nell'indispensabile esistenza di una

[32] Wortham, A. (2012). Should cyber exploitation ever constitute demonstration of hostile intent that may violate un charter provisions prohibiting the threat or use of force. *Federal Communications Law Journal, 64(3),* 643-660. https://www.repository.law.indiana.edu/fclj/vol64/iss3/8

vulnerabilità del sistema delle reti, ai fini di un corretto conseguimento dello scopo per cui l'azione è posta in essere. Infine, quello che invece le differenzia ulteriormente è il carattere della segretezza. Difatti, mentre un *cyber attack* necessita di una segretezza inferiore, limitata essenzialmente ai preparativi nell'organizzazione dell'azione per evitare che la parte cui è diretta l'operazione sia in grado di attuare una politica difensiva in grado di neutralizzare l'attacco, nel secondo caso la segretezza si contraddistingue per essere la linfa vitale dell'attività stessa, come spiegato di seguito trattando il tema del *cyber espionage*.

1.4.2 Nozione di *cyber-espionage*

Lo spionaggio tra stati ha subito varie e plurime modificazioni durante il corso della storia, non solo e unicamente in termini di distinte modalità. L'idea principale in termini di spionaggio parte da un concetto relativamente semplice: riuscire a collezionare concretamente un quantitativo di informazioni non disponibili tramite normali ricerche, cercando di raggiungere, grazie alle informazioni stesse, una posizione di vantaggio su uno stato, un gruppo o un singolo soggetto oggetto di spionaggio. L'avvento di Internet, a cui si aggiunge la creazione dei vari *social network*, ha portato ad un ampliamento difficilmente quantificabile di informazioni; dette informazioni, inoltre, sono nella maggior parte dei casi fornite dagli individui stessi. La conoscenza di informazioni "private", dove per private si intende di appartenenza di altri soggetti e non di dominio pubblico, tende a svilupparsi come uno strumento con cui i vari stati hanno la possibilità concreta di cercare di ottenere una situazione di supremazia nel panorama internazionale, oltre a rappresentare uno strumento estremamente efficace nella tutela della sicurezza interna. La forza di questa attività si esplica essenzialmente nel fatto che i vari servizi segreti statali tendono ad attuare queste tipologie di attività per fornire concretamente ai governanti, nel minor tempo possibile, notizie concrete sul comportamento dei propri "avversari", per rendere

gli stessi in grado di rispondere adeguatamente e, in determinati casi, di anticipare le mosse di altri soggetti di diritto internazionale.

L'esempio più romanzato, sia da un punto di vista letterario che cinematografico, si può evincere dall'organo di *intelligence* probabilmente più famoso a livello mondiale: la *Central Intelligence Agency*, comunemente nota con l'acronimo CIA. Pur non essendo mutato nel corso del tempo l'obiettivo delle varie organizzazioni che hanno preceduto la CIA, ovvero la tutela della sicurezza degli Stati Uniti D'America, la nascita di quest'ultima è stata contraddistinta da vari passaggi. In particolare, come riportato dal sito ufficiale della *Central Intelligence Agency*[33], a partire dal 1939 è stata avvertita la necessità da parte del presidente Franklin D. Roosevelt. Solo e unicamente il 18 settembre 1947, in seguito alla fine della Seconda guerra mondiale, con un atto firmato dal presidente Truman (Atto di sicurezza nazionale), venne creata la CIA come conosciuta ai giorni nostri. Quest'atto ha formalmente istituito un'agenzia centrale indipendente, con il compito di svolgere analisi strategiche, aventi come fine il controllo delle attività clandestine per affrontarle e garantire al meglio la sicurezza del paese. Tuttavia, accanto all'organo di controllo più conosciuto per definizione, gli Stati Uniti hanno istituito a partire dal 4 novembre 1952 la "*National Security Agency*[34]"(NSA), un organismo che, insieme alla CIA e all'FBI (*Federal Bureau of Investigation*)[35], si occupa della sicurezza interna ed esterna del paese. La NSA è un'agenzia che si occupa del monitoraggio, della raccolta, di elaborazioni di dati tramite intercettazioni sia di cittadini americani (nel presunto rispetto del quarto emendamento dalla costituzione[36]) la cui

[33] CIA (Central Intelligence Agency). (2020, 6 ottobre). *About CIA: History of the CIA.* Consultato da https://www.cia.gov/about-cia/history-of-the-cia

[34] NSA (National Security Agency). (n.d.). *Understanding the threat.* Consultato da https://www.nsa.gov/what-we-do/understanding-the-threat/

[35] FBI (Federal Bureau of Investigation). (n.d.). *Official Website*. Consultato da https://www.fbi.gov/

[36] Legal Information Institute. (n.d.). *U.S. Constitution, amend. IV*. «*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*». Consultato da https://www.law.cornell.edu/constitution/fourth_amendment

ammissibilità legale è subordinata al rispetto del "*Foreign Intelligence Surveillance Act* (FISA)", il quale, nonostante sia stato più volte emendato in seguito soprattutto agli attacchi terroristici del 11 settembre, prevede la possibilità di effettuare intercettazioni nei confronti dei cittadini americani subordinati ad un'autorizzazione giudiziale, sia nei confronti di cittadini non americani. I problemi che ha portato il rispetto del quarto emendamento e della FISA saranno approfonditi nel paragrafo al *cyber* terrorismo (1.5), con particolare riferimento al caso "*Snowden*".

Di conseguenza, compito fondamentale delle attività di intelligence non è tanto la raccolta della semplice informazione; il punto cardine risulta la sua elaborazione. L'operatore dell'organizzazione di intelligence considerata, oltre ad avere ampie conoscenze dei principali sistemi informatici, deve essere in grado di riuscire a compiere una cernita delle informazioni rilevanti per la sicurezza nazionale, per evitare di perpetrare violazioni di diritti umani. L'operazione si articola di conseguenza in quattro momenti distinti: pianificazione e direzione, raccolta, lavorazione e analisi, diffusione.[37]

Il *cyber* spionaggio presenta varie e molteplici caratteristiche. Al contrario dell'immaginario collettivo, dove la visione distorta porta ad immaginare lo spionaggio come un'attività solo virtuale ed alienata dal soggetto che la realizza, un elemento da considerare è la stessa importanza del soggetto fisico. Difatti, oltre ad avere ottime conoscenze in campo cibernetico, relative al funzionamento dei vari *software e* delle metodologie per effettuare intrusioni nel *cyber* "spazio personale", l'operatore deve essere dotato anche di una forte capacità critica.

Accanto a questo, un ulteriore elemento del *cyber* spionaggio attiene senza dubbio al carattere della sua economicità[38]. Detta economicità si basa sulla basilare necessità di un definito gruppo di *hacker* e di una conoscenza dei vari

[37] Colonna Vilasi, A. (2014). *Storia della CIA*. Sovera Edizioni. (Vedi p. 9).

[38] Teti, A. (2018). *Cyber Espionage e Cyber Counterintelligence: spionaggio e controspionaggio cibernetico.* Rubettino Editore. (Vedi pp. 1-6).

sistemi informatici che permetta concretamente, tramite l'utilizzo di una salda connessione ad Internet, di svolgere una serie di attività dal costo decisamente esiguo. Lo svolgimento da parte dei vari operatori delle attività fino a qui considerate può essere subordinato alla realizzazione di una serie distinta di obiettivi, che meritano di essere approfonditi. Tra questi è possibile annoverare obiettivi militari, politici, terroristici.

In termini prettamente giuridici, il tema dello spionaggio in generale viene affrontato sulla base di una preliminare distinzione che, da un punto di vista storico, è risultata particolarmente interessante: il regime applicabile allo spionaggio svolto in tempo di guerra e quello applicabile in tempo di pace[39]. Infatti, nonostante spesso siano presenti eventi che dovrebbero inevitabilmente avere rilevanza sul piano internazionale, lo spionaggio in tempo di pace è sempre stato visto come una materia di competenza esclusivamente statale. Diversa è la situazione che viene prospettata nel caso in cui si tratti di spionaggio in tempo di guerra, dato che i principi in questo secondo caso sono chiari, univoci e incontestabili; questi principi, infatti, contengono un'indicazione concisa relativa alla tutela di dilemmi che, da un punto di vista giuridico, ma soprattutto etico, possono riguardare i vari diritti umani, il principio di sovranità statale e il tema della sicurezza globale, strettamente correlato al tema della raccolta di informazioni. Uno dei primi tentativi di codificazione e di unificazione delle leggi riguardante il tema della guerra è stato fornito dalla "*Declaration of Brussels Concerning the Laws and Customs of War*"[40]. Si parla di un primordio di accordo internazionale, voluto e richiesto dallo Zar Alexander II di Russia, il quale richiese un incontro, il 27 di luglio 1874, con 15 stati europei volto ad

[39] Demarest, G. B. (1996). Espionage in International Law. *24 Denv. J. Int'l L. & Pol'Y,* 24(2), 321-348. Consultato da https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1657&context=djilp

[40] Project of an International Declaration Concerning the Laws and Customs of War, Adopted by the Conference of Brussels, August 27, 1874. (2017, 4 maggio). *The American Journal of International Law*, 1(2), 96–103. doi:10.2307/2212371 (pubblicato da Cambridge University Press, originale datato aprile 1907).

approvare detto accordo internazionale[41]. L'articolo 19 della Dichiarazione di Bruxelles fornisce un'identificazione del termine spia e sancisce testualmente:

> *«A person can only be considered a spy when acting clandestinely or on false pretenses he obtains or endeavors to obtain information in the districts occupied by the enemy, with the intention of communicating it to the hostile party».*

Nel 1880 a Oxford, inoltre, vengono redatte le "*Laws of War on Land*", le quali, insieme alla Dichiarazione di Bruxelles, fornirono le fondamenta per la redazione delle due Convenzioni dell'Aia sulla guerra e dei Regolamenti ad esse allegati, adottati nel 1899 e 1907[42]. Infine, "*The Geneva Convention of 1949*" ha modificato solo leggermente l'ambito relativo allo spionaggio.

È possibile infine delineare le diverse tipologie di attività di spionaggio, distinzione che risulta particolarmente importante a fini definitori della normativa applicabile, ovvero il caso concreto in cui l'attività di spionaggio rientra all'interno della normativa di competenza di ciascuno stato, oppure il caso in cui l'attività di spionaggio possa comportare una violazione di diritto internazionale. In particolare, pur avendo già appurato che in caso di "tempo di pace" non vi sia un regime internazionale universalmente applicabile, è necessario effettuare una distinzione intercorrente fra le due diverse attività che possono essere eseguite nell'attività di spionaggio: *covert operation* e *intelligence operation*[43]. La prima categoria si contraddistingue per il compimento di operazioni e *cyber* operazioni che uno stato realizza con la finalità di influenzare un altro stato; le attività possono a loro volta essere suddivise in tre tipologie che sono *coercive covert operations, political action* e attività di propaganda. Dall'altra parte le attività di

[41] Schindler, D., & Toman, J. (1988). *The Laws of Armed Conflicts.* Martinus Nijhoff Publishers, 22-34.

[42] International Committee of the Red Cross (ICRC). (n.d.). Treaties, States Parties and Commentaries. *Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874*. Consultato da https://ihl-databases.icrc.org/ihl/INTRO/135

[43] Prochko, V. (2018, 30 marzo). *The International Legal View of Espionage*. E-International Relations. [The University of St, Andrews], 1-10. Consultato da https://www.e-ir.info/pdf/73350

"*covert intelligence*" si suddividono in due tipologie distinte: la collezione di informazioni e l'analisi delle informazioni stesse[44]. Queste due attività sono state oggetto di innumerevoli dibattiti che presentano tuttavia un elemento indiscutibile, ovvero che la raccolta di informazioni è senza dubbio menzionata e disciplinata dal diritto nazionale nell'ambito penale. Da una prospettiva internazionale, lo studioso Rasdan differenzia tre modelli distinti in tema di legalità dell'attività di spionaggio: un modello negativo, un modello positivo e un modello che viene definito "scettico"[45]. Coloro che ritengono che l'attività di intelligence non sia consentita da un punto di vista internazionale partono da una violazione dell'art.2 della Carta delle Nazioni Unite, andandosi a focalizzare sul tema dell'integrità territoriale. Uno dei più accaniti sostenitori di detta teoria, Ingrid Delupis, ritiene che la raccolta di informazioni comporti una violazione dell'integrità territoriale garantita a ciascuno stato nel caso in cui si abbia la presenza di agenti mandati da una forza estera all'interno dello stato oggetto della raccolta di informazioni[46]. Quelli che contrariamente sono favorevoli alla legalità dell'attività di "*covert intelligence*" da un punto di vista internazionale fanno leva sulla mancata presa di posizione letterale della comunità internazionale. Se la comunità internazionale stessa non ha espressamente condannato dette attività, non determinando di conseguenza una violazione dell'integrità territoriale, non esiste ragione per ritenere le stesse illegittime[47]. I sostenitori dell'ultimo modello, definiti scettici, affermano che le attività considerate non sono né legali né illegali da un punto di vista internazionale; questi studiosi ritengono che l'attività di intelligence non costituisca una seria violazione dell'integrità territoriale e rivendicano una posizione neutrale sullo spionaggio in generale.

---

[44] *Ibid.*

[45] Radsan, A. J. (2007). The Unresolved Equation of Espionage and International Law. *Michigan Journal of International Law*, 28(3), 596-623. Consultato da https://repository.law.umich.edu/mjil/vol28/iss3/5

[46] Delupis, I. (1984). Foreign Warships and Immunity for Espionage. *American Journal of International Law, 78*(1), 53-75. doi:10.2307/2202342

[47] Prochko, *op. cit.*, p. 25.

1.4.3. La nozione di *cyber attack*

Sulla falsariga di queste generali definizioni, il tema senza dubbio più rilevante per lo svolgimento del seguente elaborato viene a concretizzarsi nella spiegazione di tutti gli elementi che caratterizzano un attacco cibernetico, la cui prevenzione, tutela ed eventuale tentativo di limitazione dei danni vanno a formare il compito principale di quell'organismo di mantenimento della pace tanto prospettato in seno alle Nazioni Unite e che, al giorno d'oggi, presenta ancora innumerevoli difficoltà derivante da uno stato di cooperazione, da un punto di vista cibernetico, ancora lontano[48]. Per una classificazione iniziale di quest'attività ci si può rifare ad uno studio effettuato nel 2012 ma estremamente attuale, il quale fornisce una definizione che si articola nel seguente modo: "un attacco informatico consiste in un'azione intrapresa per minare le funzioni di una rete di computer a fini di sicurezza politica o nazionale"[49]. Il primo elemento strutturale attiene all'attacco informatico, che è contraddistinto da un'azione attiva, azione che può essere anche di difesa; infatti, come sarà rilevato nel paragrafo 1.5 relativo alla distinzione tra *cyber defense* e *cyber security*, solo e unicamente l'attività di difesa attiva può essere considerata come assimilabile ad un *cyber attack*. L'attacco per essere considerato tale, deve avere un obiettivo primario preciso, ovvero quello di essere in grado di distruggere o limitare il funzionamento di una rete di computer. La scelta di inquadrare un *cyber attack* nell'esistenza di un obiettivo predefinito non è casuale, si evolve anzi alla stregua di due motivi fondamentali: da una parte l'inquadramento dell'obiettivo risulta particolarmente intuitivo, dall'altra estremamente logico. Per chiarire i motivi sopra esposti è possibile rifarsi ad alcuni esempi. In particolare, per spiegare l'intuitività è sufficiente analizzare due situazioni distinte. L'utilizzo di un drone per porre in essere un attacco cinetico non è considerato un *cyber attack* ma

[48] Almutawa, A. (2020). Designing the Organisational Structure of the UN Cyber Peacekeeping Team. *Journal of Conflict and Security Law*, *25*(1), 117-147.

[49] Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review*, *100*(4), 817–885.

viene alla luce come un semplice attacco di guerra con tecnologie avanzate. Contrariamente, far esplodere cavi che sono necessari al trasporto di informazioni fra vari continenti rientra senza dubbio nella definizione di *cyber attack*[50].

Un altro punto da considerare è il tema di distruzione o malfunzionamento di una rete di computer oggetto del *cyber attack*. Detto malfunzionamento può essere causato da "'"*worms"*[51]*, "malware*"[52] o "*Trojan horses*"[53]. L'ultimo elemento, infine, attiene al motivo per cui viene scagliato un *cyber attack*, motivo che rende possibile differenziare quest'ultimo caso dalla più articolata attività che viene comunemente definita *cybercrime.* Infatti, un'azione aggressiva eseguita da un attore statale nel *cyber*-dominio implica necessariamente la sicurezza nazionale ed è quindi un attacco informatico, dal momento che l'azione soddisfa tutti gli altri elementi della definizione precedentemente fornita, sempre che non raggiungerà il livello di *cyber*-guerra. Un crimine cibernetico commesso da un attore non statale per scopi politici o di sicurezza nazionale è un *cyber*-attacco. Dall'altro lato, un *cybercrime* che non viene eseguito per scopi politici o di sicurezza nazionale, come la maggior parte dei casi di frode tramite Internet, di furto di identità o di pirateria intellettuale, non si adatta a questo elemento finale di un "*cyber*-attacco" e viene quindi rilevato alla stregua semplice crimine informatico.

---

[50] *Ibid.*

[51] Treccani. (2020). *Worm*. Enciclopedie on line, Istituto della Enciclopedia Italiana: «Nel linguaggio informatico, virus che si diffonde tramite la rete e la posta elettronica». Consultato da https://www.treccani.it/vocabolario/worm/

[52] Treccani. (2020). *Malware*. Enciclopedie on line, Istituto della Enciclopedia Italiana: «Software scaricato dall'utente sul proprio computer, in modo spesso inconsapevole, che ha la funzione di registrare e segnalare al mittente i siti visitati durante la navigazione in Internet o di far ricevere messaggi pubblicitari indesiderati […]». Co. da https://www.treccani.it/vocabolario/malware_%28Neologismi%29/

[53] Treccani. (2020). *Trojan horse*. Enciclopedie on line, Istituto della Enciclopedia Italiana: «Malware nascosto in un normale programma che danneggia o quantomeno compromette la sicurezza e il funzionamento del computer. Proprio perché nascosto, il t. h. viene spesso installato dall'utente che, ignaro, lo ha scaricato da internet insieme con il programma a cui è interessato (da qui il nome, "Cavallo di Troia"). A differenza dei virus i t. h. non si diffondono in autonomia […]». Consultato da https://www.treccani.it/enciclopedia/trojan-horse/

Accanto allo studio effettuato ed appena analizzato, un'implementazione fondamentale è stata fornita dalla *Rule 30* del *Tallinn Manual*, la quale non si limita solo a fornire una definizione chiara ed unitaria di *cyber attack*, ma evidenzia soprattutto quelli che vanno a concretizzarsi come gli elementi strutturali dello stesso[54]. Sulla base della suddetta regola, un attacco informatico si concretizza in un'operazione cibernetica, sia essa offensiva o difensiva, in grado di causare ragionevolmente la lesione o la morte di persone o ancora danni o distruzione a diversi oggetti[55]. Questa definizione viene applicata nel caso di conflitto armato internazionale e non[56]. Il concetto di attacco risulta particolarmente importante dal momento che una corretta definizione dello stesso rende applicabile la normativa a riguardo come base per un numero definito di limitazioni e proibizioni che attengono al diritto dei conflitti armati. Il termine *attack* risulta ripreso dalla *Rule 32*, la quale afferma l'impossibilità per la popolazione, vista anche come singoli individui, di essere oggetto di attacchi cibernetici[57]. L'art.49 del protocollo addizionale I del *Tallinn Manual* aiuta a chiarire che per attacco si intende un atto di violenza contro un avversario, sia esso un atto offensivo o propriamente difensivo. Per questo motivo, partendo da quest'ultima considerazione, si perviene alla consapevolezza che è l'obiettivo che distingue gli attacchi dalle operazioni militari; di conseguenza le operazioni non violente come quelle relative, per esempio, al cyber spionaggio o come quelle che hanno una natura per lo più "psicologica" ma che non arrivano a causare lesioni viste come sofferenze, non possono essere qualificati come attacchi[58]. Pur avendo accertato la maggiore facilità di riscontro degli attacchi cibernetici nell'esistenza materiale di danni cinetici, il gruppo di esperti ha ritenuto altresì che gli atti di violenza non dovrebbero essere limitati solo al

[54] Schmitt, *op. cit*., p. 19. (Vedi p. 257).

[55] *Ibid*., (p. 92).

[56] Mix, C. (2014). Internet Communication Blackout: Attack Under Non-International Armed Conflict?. *Journal of Law & Cyber Warfare*, *3*(1), 70-102.

[57] Schmitt, *op. cit*., p. 19. (Vedi pag. 96).

[58] Schmitt, *op. cit*., p. 19.

carattere cinetico. Infatti, come è stato evidenziato nel caso Tadic[59], gli attacchi biologici, chimici e radiologici, seppure propriamente privi di un effetto cinetico immediato sul bersaglio individuato, sono universalmente riconosciuti e delineati come attacchi violenti.

Tuttavia, il punto focale della nozione si inserisce stabilmente negli effetti che devono essere causati da dette attività cibernetiche per poter assurgere al rango di attacchi. In particolare, il termine attacco viene determinato non tanto dalla sua natura quanto dalle sue conseguenze; la violenza, infatti, viene contraddistinta dalle sue conseguenze violente e non si limita agli atti violenti[60]. La capacità di causare danni come lesioni o morte è facilmente accertabile mentre la possibilità di causare danni oggetti potrebbe avere una forza interpretativa particolarmente ampia. Tuttavia, tutti i membri del gruppo internazionale di esperti hanno convenuto che il tipo di danno previsto dalla *Rule 30* qualifica una determinata azione cibernetica come *cyber attack* e, accanto a ciò, hanno altresì constatato come non sia al tempo stesso sufficiente la presenza di un minimo danno per poter integrare la qualifica di attacco come sopra definita[61].

Inoltre, la capacità di causare ragionevolmente i danni fino a questo momento prospettati non è sempre automatica, partendo dal presupposto che la parola "*cause*" non si limita agli effetti sul sistema informatico mirato ma si riverbera e si ricollega a qualsiasi prevedibile e consequenziale danno, distruzione, lesione o anche morte[62]. Gli attacchi informatici, pur comportando raramente un'esplicitazione di forza fisica diretta contro il sistema informatico, sono in grado, nella maggior parte dei casi, di causare grandi danni ad individui o oggetti, andando di conseguenza al di fuori del mondo cibernetico ed inserendosi stabilmente nel mondo fisico. La *Rule 30*, sebbene espressamente prevista per

[59] Alvarez, J. E. (1997). Rush to closure: lessons of the Tadic judgment. *Mich. L. Rev.*, 96(7), 2031-2112. doi:10.2307/1290059

[60] Schmitt, *op. cit*., p. 19.

[61] Schmitt, *op. cit*., p. 19. (Vedi p. 92).

[62] Schmitt, *op. cit*., p. 19. (Vedi p. 93).

attacchi che vengono effettuati per causare lesioni a persone o danni ad oggetti, deve considerarsi applicabile anche nel caso in cui l'attacco sia diretto contro dati informatici, partendo dal presupposto che gli stessi non sono considerabili alla stregua delle varie entità fisiche. Infatti, ogni qualvolta che un attacco ai vari dati è strettamente correlato o conduce direttamente alla morte o alla lesione fisica di singoli individui o a danni alle cose, sono gli stessi oggetti o gli stessi individui il target dell'operazione, con conseguente classificazione della stessa come attacco[63]. È stato inoltre constatato dal gruppo internazionale di esperti come la "clausola", contenuta nell'art.49 precedentemente menzionata, relativa all'attacco "contro un avversario" abbia comportato una difficoltà interpretativa evidente. Di fatto, la stessa previsione sembrerebbe causare confusione, potendo arrivare ad asserire che le operazioni distruttive dovrebbero essere dirette al nemico per potersi qualificare come attacchi[64]. Gli esperti sono concordi nel ritenere che questa interpretazione non sarebbe coerente con quelle proibizioni relative agli attacchi su civili ed oggetti. Partendo dunque dalla già citata necessità di tenere in considerazione i danni e le conseguenze, a discapito della natura, nell'ambito definitorio di un attacco, risulta fondamentale annoverare come attacchi gli atti di violenza o che hanno effetti violenti diretti contro civili o oggetti protetti, i quali non sono accomunabili alla classica definizione di nemico[65]. Il gruppo, inoltre, si è confrontato con il problema dell'equiparazione di lesioni fisiche riportate dai singoli individui a lesioni di carattere psicologico che potrebbero portare gli individui vittime di un attacco informatico a malattie gravi o a gravi sofferenze mentali. Essendo, di conseguenza, il terrore instillato in seguito ad un attacco assolutamente in grado di causare sofferenza mentale, risulta indubbia la possibilità di equiparare, tramite analogia, tale sofferenza alla definizione data dalla Rule 30 di attacco cibernetico[66]. Una discussione è stata

[63] *Ibid.*

[64] Schmitt, *op. cit.*, p. 19. (Vedi pag. 94).

[65] *Ibid.*

[66] *Ibid.*

inoltre affrontata relativamente alla possibile inclusione di quelle tipiche operazioni informatiche che non comportano propriamente la realizzazione dei danni sopra descritti ma che si limitano a causare conseguenze negative su larga scala, come per esempio il blocco delle comunicazioni tramite e-mail all'interno di tutto il paese. La maggior parte degli esperti è tuttavia concorde nel ritenere che il diritto dei conflitti armati non riesca ad estendere la propria competenza a quelle operazioni, andando di conseguenza ad ottenere un'impossibilità di equiparazione delle condotte considerate agli attacchi cibernetici di cui alla *Rule 30*[67].

Per concludere il discorso è possibile riportare il caso *Wannacry*, il quale assume particolare rilevanza in tema di *cyber attack* dal momento che è risultato essere l'attacco cibernetico più importante fino ad ora scagliato[68]. La rilevanza del caso preso in considerazione si esplica essenzialmente alla stregua dei caratteri che hanno portato alla classificazione dell'operazione cibernetica come *cyber attack*, partendo, in particolare, dallo studio dei danni concretamente causati dall'operazione. Nel maggio del 2017 un poderoso attacco è stato sferrato tramite la diffusione del *malware* denominato *Wannacry*, ossia un *software* maligno in grado di impedire agli utenti di accedere ai files, tenendo di conseguenza in ostaggio gli stessi o interi dispositivi tramite crittografia; la vittima, soltanto tramite il pagamento di una somma di bitcoin poteva ottenere così una chiave di decrittazione, che consentiva all'utente di accedere ai files o ai sistemi criptati dal programma[69]. Si è parlato di un "*ransomware*", ovvero uno strumento di propagazione del virus in grado di impedire l'utilizzo dei normali computer[70]. Gli

[67] Schmitt, *op. cit*., p. 19.

[68] Mandrioli, D. (2018). Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati. *LA COMUNITÀ INTERNAZIONALE*, (3)2018, 473-492. Consultato da https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=++Mandrioli%2C+D.+%282018%29.+Il+caso+WannaCry%3A+il+fenomeno+dei+cyber+attacks+nel+contesto+della+responsabilit%C3%A0+internazionale+degli+Stati.+Il+caso+WannaCry%3A+il+fenomeno+dei+cyber+attacks+nel+contesto+della+responsabilit%C3%A0+internazionale+degli+Stati%2C+473-492&btnG=

[69] Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5).

[70] *Ibid.*

effetti concretamente causati da questo attacco cibernetico sono stati innumerevoli e hanno riportato conseguenze effettive non solo ed unicamente da un punto di vista prevalentemente economico, dal momento che ha concretamente colpito un'ampia gamma di imprese private, andando a bloccare la possibilità per le stesse di accedere ai server che risultano fondamentali per lo svolgimento di attività di impresa, ma anche e soprattutto ha colpito vari organi statali, con funzioni particolarmente importanti[71]. Come sarà meglio spiegato nel secondo capitolo, sono stati paralizzati per alcuni giorni i sistemi di funzionamento del sistema sanitario del Regno Unito[72].

1.5 La nozione di cyberterrorismo e i pericoli derivanti dall'ISIS

Il concetto di terrorismo si è notevolmente evoluto nel corso del tempo, tanto che non si è mai riusciti a raggiungere una definizione unanime, internazionalmente accettata, del termine. La radice dello stesso, però, aiuta concretamente a fornire uno spunto di riflessione, poiché la parola terrorismo si forma da terrore, ovvero la situazione concreta che alimenta la linfa vitale delle organizzazioni terroristiche. Come riportato da diversi studiosi, l'evoluzione del termine terrorismo si è sviluppata in primis alla stregua dei differenti soggetti che si macchiano del compimento di suddette attività. Non si parla infatti solo di terroristi come concepiti al giorno d'oggi, ovvero organizzazioni terroristiche con epicentro per lo svolgimento della propria attività in stati dell'africa o dell'Asia, che pongono alla base delle loro attività credenze religiose. Attività terroristiche possono essere anche poste in essere da stati o da organizzazioni che distaccano totalmente la loro attività da qualsiasi credenza religiosa; è sufficiente pensare al

[71] Mandrioli, *op. cit.*, p.32. (Vedi p. 476).

[72] *Ibid.*

terrorismo perpetrato da regimi dittatoriali o ancora alle organizzazioni terroristiche di sinistra che sono nate in Italia negli anni 70[73].

Il primo punto, ampliamente ribadito anche e soprattutto da organizzazioni internazionali come le Nazioni Unite, attiene al carattere internazionale proprio del terrorismo[74]. Un elemento particolarmente rilevante si esplica nel fatto che, con lo sviluppo di internet, il quale riesce a garantire non solo connessione rapidissime ma anche livelli di comunicazioni e di coordinamento eccezionalmente funzionanti, tutta l'attività terroristica di propaganda, reclutamento, ricerca dei finanziamenti, allenamento e preparazione per l'attività risulta essere svolta non più unicamente in un singolo stato; molto spesso infatti gli stessi obiettivi possono collocarsi in stati totalmente differenti e distanti, da un punto di vista prettamente geografico, rispetto allo stato in cui l'attività viene pianificata, progettata e architettata nei minimi dettagli. Questa internazionalizzazione e digitalizzazione del fenomeno terroristico non potrebbe efficacemente essere contrastata senza un sistema di leale collaborazione dal punto di vista internazionale che i vari stati sono, molto spesso forzatamente, tenuti a mantenere. Non bisogna scordare infatti che l'obiettivo delle principali agenzie statali è sempre la tutela della sicurezza interna e questa internazionalizzazione del terrorismo comporta, ai fini di una migliore ed efficace tutela, l'istituzione di un sistema di collaborazione. Le Nazioni Unite (ONU), essendo l'organizzazione internazionale che conta il maggior numero di stati membri (193)[75], occupandosi, come statuito dall'art.2 della Carta delle Nazioni Unite, del mantenimento della pace, hanno da sempre avvertito la necessità di andare a fornire una definizione unanime di terrorismo, definizione che risulta essere il punto di partenza per avere la capacità di fornire una risposta

[73] Lamberti, C. (2014). Gli strumenti di contrasto al terrorismo e al cyber-terrorismo nel contesto europeo. *Rivista di Criminologia, Vittimologia e Sicurezza*, 8(2), 138-161. Consultato da http://eprints.bice.rm.cnr.it/9847/1/articolo_lamberti_2014-02.pdf (Vedi p. 139).

[74] Bruce, G. (2013). Definition of terrorism social and political effects. *Journal of Military and Veterans Health, 21*(2), 26. https://jmvh.org/article/definitionof-terrorism-social-and-political-effects/

[75] United Nations. (n.d.). *Official Website.* Consultato da https://www.un.org/en/

adeguata al fenomeno stesso. Uno dei più solidi ma incompiuti tentativi di fornire suddetta definizione è stato espletato dall'ONU in seguito all'attentato terroristico effettuato durante le olimpiadi di Monaco nel 1972, dove un commando dell'organizzazione terroristica palestinese, denominato Settembre Nero, decise di effettuare un'irruzione nel villaggio olimpico negli alloggi in cui si trovavano gli atleti israeliani; suddetto attacco comportò l'uccisione di 9 atleti. Nel 2001 gli stati membri dell'ONU stipularono la Convenzione Internazionale sulla soppressione dei bombardamenti terroristici, senza tuttavia riuscire a fornire una definizione concisa di terrorismo. Tuttavia, venne fornita una lista comprendente una serie di attività, le quali, sulla base di un'analisi dei propri elementi strutturali, lasciano intendere la loro natura terroristica: «attività che comportano o sembrano comportare un'ingente perdita economica, quando l'obiettivo della condotta, per la sua natura o per il suo contesto, è quello di intimidire la popolazione o forzare un organo statale o un'organizzazione internazionale ad adottare o a non porre in essere un determinato atto[76]». Si può dunque da qui constatare la difficoltà di una definizione unanime, con il conseguente obbligo, cui sono sottoposti tutti gli stati, di fornire una interpretazione unilaterale[77]. Partendo da un'incertezza relativa a varie definizioni nel mondo cibernetico, risulta di conseguenza inevitabile l'assenza di una definizione unitaria del *cyber* terrorismo; per questo motivo è utile prendere in considerazione il fenomeno partendo sia da un punto di vista storico che dagli elementi generali che caratterizzano queste tipologie di attività. Come è stato più volte asserito, uno degli elementi da considerare è la potenza incredibile dei media nell'attività terroristica. È sufficiente notare come un ruolo fondamentale nella diffusione del terrore in seguito agli attentanti dell'11 settembre 2001 sia quello fornito indirettamente dai media, i quali si sono rivelati uno dei principali veicoli del terrore nei momenti subito successivi allo schianto aereo contro le due torri. Il riverbero di quegli avvenimenti, tramite la diffusione di immagini e

[76] Bruce, *op. cit*., p. 34. (Vedi p. 26).

[77] Saul, B. (2008). *Defining Terrorism in International Law*. Oxford: Oxford University Press.

notizie, hanno portato a focalizzare il reale obiettivo delle attività terroristiche considerate, ovvero il raggiungimento di quella situazione di timore e paura analizzata precedentemente. In questo modo, i media si sono rivelati ottimi indiretti "alleati" nella gestione dell'informazione per gli attentatori. Difatti, la distruzione delle due torri gemelle non ha semplicemente dimostrato la vulnerabilità della tutela degli spazi aerei americani ma ha altresì dimostrato la potenza distruttiva e difficilmente controllabile dell'utilizzo di internet. In aggiunta, è stato dimostrato come concretamente gli attentatori si siano avvalsi di internet per perseguire i loro obiettivi; infatti, i coordinatori più alti in grado di Al Qaeda, tra i quali il famoso direttore del campo d'addestramento militare di Al Qaeda, chiamato Abu Zubaydah, si sono scambiati migliaia di messaggi criptati tramite il proprio sito internet, contenti informazioni e modalità di attuazione del piano considerato. I messaggi iniziano a partire dal 1° maggio 2001, raggiungono, da un punto di vista quantitativo, l'apice nell'agosto del 2001 e si interrompono il 9 di settembre, a due giorni dall'attentato[78].

Due sono gli elementi che meritano di essere presi in considerazione dal momento che vengono attuate dallo Stato Islamico (ISIS) nel *cyber* spazio: il ruolo fondamentale che oggi svolgono i social media e l'attività di reclutamento e propaganda che viene svolta all'interno del *cyberspace*[79]. Per quanto riguarda il primo punto, è sufficiente riportare alcuni esempi pratici forniti dai maggiori social media come *YouTube* e *Twitter*: il primo conta oggi 2 miliardi di utenti[80] mentre l'analisi del numero di *Tweets* ha portato a constatare come giornalmente gli stessi siano all'incirca 500.000.000.000[81]. Tramite l'utilizzo di plurimi video

[78] Davis, B. R. (2006). *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance.* 15 CommLaw Conspectus 119. Consultato da https://scholarship.law.edu/commlaw/vol15/iss1/7 (Vedi p. 121).

[79] Awan, I. (2017, 15 marzo). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, 54, 138–149. https://doi.org/10.1007/s12115-017-0114-0

[80] YouTube. *YouTube About: Statistics 2020.* Visitato il 9 dicembre 2020. Consultato da https://www.youtube.com/intl/en-GB/about/press/

[81] Twitter. *Twitter Usage Statistic.* Visitato il 9 dicembre 2020. Consultato da https://www.internetlivestats.com/twitter-statistics/

postati su *YouTube* sono state attuate diverse campagne volte a convincere i musulmani, e non solo, a partecipare alla lotta dell'ISIS. Questi video, che sono stati tradotti e inviati a moltissimi e diversi paesi, raggiungendo anche Algeria, Egitto e Libia, sono indirizzati al secondo punto da considerare, ovvero il reclutamento, visto essenzialmente come la chiamata a raccolta contro un nemico comune, che viene sostanzialmente a combaciare con il modello di vita occidentale. Ancora, ci si è spinti addirittura alla creazione di un'applicazione, chiamata "*The Dawn of Glad Tidings*", nella quale venivano inserite le ultime notizie riguardanti l'organizzazione terroristica. Il problema di fondo è che quest'applicazione è stata disponibile tramite il sistema di ricerca *Google*, per sistemi *Android*, fino a quando non è stata individuata e cancellata.

Proprio dall'attentato del 11 settembre 2001 si è sviluppata una sempre maggiore esigenza di effettuare controlli più serrati dei vari sistemi di comunicazione, non solo da parte degli Stati Uniti ma da parte di tutti i paesi del mondo. La tutela della sicurezza interna di un paese è senza dubbio di un'importanza disarmante, a tal punto da essere, in determinati casi, in grado di prevaricare legittimamente una serie di diritti che vengono riconosciuti ai cittadini. Il bilanciamento che deve essere svolto in questo senso è un bilanciamento che si articola nel rapporto essenziale tra diritto alla *privacy* e alla vita privata e l'obbligo di ciascuno stato di combattere il terrorismo. La raccolta di informazioni riguardati cittadini ritenuti "potenzialmente pericolosi" si articola in una serie di attività corrispondenti ad intercettazioni , salvataggio di email , media , messaggi e note audio; tuttavia ciò che è possibile constatare è come concretamente, nell'attività di "*screening*[82]*"*, vengano prese in considerazioni informazioni illimitate, con conseguente immagazzinamento di una serie di informazioni che non hanno

[82] Treccani. (2020). *Screening.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «Termine che in inglese ha vari significati, alcuni in uso anche in Italia, tra cui, in particolare, quello di controllo sanitario eseguito su una popolazione o su singoli gruppi o categorie per consentire la diagnosi precoce di determinate malattie e condizioni morbose; più genericamente, qualsiasi indagine e forma di controllo che, nella vita sociale o nell'attività economica, abbia per scopo di effettuare una selezione […]». Consultato da https://www.treccani.it/vocabolario/screening/

nessuna utilità e che comportano solo una violazione del diritto alla *privacy* del cittadino nei cui confronti sono raccolte. Il diritto alla *privacy* è garantito difatti dalla normativa europea a partire dall'art.8 della Convenzione Europea dei Diritti dell'Uomo, il quale sancisce espressamente che: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza". Dal lato americano, invece, è il quarto emendamento stesso a fornire una garanzia di detto diritto, emendamento che si esprime nel seguente modo:

> *«The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».*

Proprio in questo senso si articola uno dei più famosi e recenti casi relativo all'attività svolta dalla NSA in materia di sicurezza interna volta a reprimere un possibile nuovo 11 settembre, ovvero il caso "*Snowden*". Nel maggio 2017 Edward Snowden (Elizabeth City, 1983), un informatico che lavorava presso la sede nelle Hawaii della NSA, decise di rubare un quantitativo pari a 1.7 milioni di documenti segreti della NSA, che dimostravano l'attività di intercettazione continua che l'organizzazione di sicurezza realizzava sia nei confronti di cittadini americani che nei confronti di tutte le Nazioni tramite l'utilizzo delle più comuni piattaforme online[83]. Questi dati raccoglievano infatti la testimonianza dell'utilizzo di veri e propri programmi per lo svolgimento di suddette attività: tra questi, i programmi *Tempora*, *PRISM*, *eXKeyscore*, nonché la raccolta di moltissime informazioni che coinvolgono i metadati delle intercettazioni

[83] Verble, J. (2014, settembre). The NSA and Edward Snowden: surveillance in the 21st century. *SIGCAS Comput. Soc.*, 44(3), 14-20. Consultato da https://doi.org/10.1145/2684097.2684101

telefoniche negli Stati Uniti e in Europa[84]. Tutto questo lascia intendere come da un lato la lotta al *cyber* terrorismo sia un fenomeno assolutamente da sviluppare e da prendere seriamente in considerazione da parte di tutti gli stati del mondo; dall'altro lascia certamente dubbi e perplessità sugli strumenti da utilizzare concretamente per combatterlo.

1.6 I concetti di *Cyber defense* e *cyber security*

1.6.1 La nozione di cyber security

Il rapido sviluppo di internet e la globalizzazione, in aggiunta alle nuove tecnologie digitali e al commercio elettronico, hanno indotto ad una rappresentazione del *cyberspace* non solo come una delle più importanti piattaforme per lo scambio di informazioni e per l'economia globale, ma anche come uno strumento per la realizzazione di crimini informatici[85]. Sulla base delle differenti definizioni fornite nel presente elaborato relativamente alle principali *cyber activities*, è necessario andare a prendere in considerazione il rapporto intercorrente fra *cyber security* e *cyber defence*, distinzione che viene studiata alla stregua delle diverse attività che contraddistinguono le due tipologie azioni.

Partendo dal primo caso, le difficoltà relative ad una definizione unitaria di *cyber security* anche qui non si sono fatte attendere. Essendo il tema della sicurezza nazionale un elemento di competenza prettamente statale, l'esistenza di una definizione unitaria di *cyber security* risulta particolarmente ostica e, esattamente per questo motivo, è necessario rifarsi ad una serie di documenti statali per cercare di fornire una visione generale del tema. Come è stato rilevato infatti

[84] Herman T. Tavani, T. H., & Grodzinsky, F. S. (2014, settembre). Trust, betrayal, and whistleblowing: reflections on the Edward Snowden case. *SIGCAS Comput. Soc.*, 44(3), 8–13. Consultato da https://doi.org/10.1145/2684097.2684100

[85] Halawi, R. A. S. (2020). Cybercrime and cybersecurity: The need for International Cybersecurity Law. Consultato da Leiden Law Blog https://leidenlawblog.nl/articles/cybercrime-and-cybersecurity-the-need-for-international-cybersecurity-law

dall'Agenzia Europea per la sicurezza delle reti e dell'informazione (ENISA)[86], risulta fondamentale per ciascuno stato dotarsi di una "*National cyber security strategy (NCSS)*", per essere in grado di far fronte a tutti quei pericoli derivanti da attacchi cibernetici che, sulla base della definizione fornita dal *Tallinn Manual* alla *Rule 30*[87], sono in grado concretamente di provocare lesioni e morte a singoli individui o danni a sistemi di particolare interesse per la collettività. Il ruolo svolto da ENISA è fondamentale dal momento che l'agenzia ha cercato di rilevare quelli che sono i caratteri comuni dei vari piani strategici relativi alla *cyber security* per tutti gli stati[88]. L'adozione di strategie per la sicurezza informatica da parte di vari stati si rivela uno strumento assolutamente utile per migliorare la sicurezza e la resilienza delle infrastrutture e dei servizi nazionali[89]; creare infatti un piano strategico per la sicurezza digitale significa stabilire una serie di obiettivi e priorità nazionali che dovrebbero essere raggiunti entro il tempo prefissato e dovrebbero essere in grado di garantire la possibilità al singolo stato di attivare un'attività di *cyber defense* in presenza di eventuali attacchi.

La prima apparizione di un piano di *cyber* sicurezza nazionale risale al 2003 ed è opera degli Stati Uniti d'America, creato e adottato in seguito all'attacco alle torri gemelle[90]. Andando infatti a stabilire i vari settori di particolare rilevanza per la nazione, è stato sottolineato come il *cyberspace* costituisca il sistema nervoso e di controllo degli Stati Uniti. Di conseguenza, un'ampia tutela del *cyber* spazio risulta assolutamente essenziale per il corretto funzionamento dell'economia e per un'efficace tutela della sicurezza del paese. Gli Stati Uniti

[86] ENISA. (2012, 8 maggio). *National Cyber Security Strategies: setting the course for national efforts to strengthen security in cyberspace.* Consultato da https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

[87] Schmitt, *op. cit*., p. 19.

[88] *Ibid.*

[89] *Ibid.*

[90] United Nations CISA. (2003). *National Strategy to Secure Cyberspace*. Consultato da https://www.cisa.gov/national-strategy-secure-cyberspace

hanno inoltre introdotto la "*International strategy for cyber-space*" nel maggio del 2011[91], aggiornato al giorno d'oggi dal "*National cyber strategy of United States Of America*", approvato dal presidente uscente Donald Trump nel settembre 2018[92]. Il piano preso in esame contempla il raggiungimento degli obiettivi prefissati in un termine di 15 anni, obiettivi tra i quali rientrano: la difesa della patria tramite la protezione delle reti, la promozione della prosperità americana tramite l'alimentazione di un'economia digitale più sicura e fiorente ma soprattutto il mantenimento della pace e della sicurezza rafforzando, in concerto con alleati e partner internazionali, la capacità statale di scoraggiare e, in determinati casi, punire coloro che utilizzano strumenti informatici per scopi illeciti[93].

Accanto agli Stati Uniti, molti paesi europei hanno iniziato a adottare atti concernenti la *cyber* sicurezza nazionale, come per esempio la Germania, prima nel 2005 con l'adozione del "*National Plan for Information infrastructure protection*"[94] e in seguito nel 2016 tramite l'adozione del "*Cyber security strategy for Germany*"[95]. Sulla base di detto piano la Germania ha deciso di fondare la propria attività in tema di *cyber security* sulla base di quattro livelli distinti i quali sono così classificabili:

---

[91] National Security Council (U.S.), & United States. Executive Office of the President. (2011). *International strategy for cyberspace: Prosperity, security, and openness in a networked world*. [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[92] National Security Council (U.S.), & United States. Executive Office of the President. (2018). *National Cyber Strategy of the United States of America.* [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council. Consultato da https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[93] *Ibid.*

[94] Federal Ministry of the Interior. (2005). *National Plan for Information Infrastructure Protection*. Consultato da https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/EN/BSI/Kritis/National_Plan_for_Information_Infrastructure_Protection.pdf?__blob=publicationFile

[95] ENISA. (2016). *German National Cyber Security Strategy*. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

1) Mantenimento della sicurezza e dell'autonomia tedesca all'interno del mondo digitale

2) Implementazione della collaborazione tra il governo tedesco ed il settore privato

3) Creazione di un'architettura forte e sostenibile per la sicurezza informatica su tutti i livelli di governo

4) Amplificazione del ruolo attivo della Germania nella politica europea ed internazionale in tema di sicurezza informatica

L'Estonia, inoltre, ha rappresentato il primo paese europeo ad adottare un'ampia strategia per il mantenimento della sicurezza informatica prima nel 2008[96] e in seguito nel 2019[97], la quale ha come punti cardine il riconoscimento e la protezione dei diritti e delle libertà fondamentali tanto nel mondo fisico quanto nel *cyberspace* e una necessità di ottenere una relazione tra sicurezza ed innovazione, dove la tutela dell'una presuppone l'implementazione dell'altra, accanto alla promozione della cooperazione internazionale con lo scopo di rafforzare la sicurezza cibernetica globale già introdotta a partire dal 2008. A partire dal 2008 quasi tutti gli stati europei si sono impegnati ad adottare strategie di tutela della sicurezza informatica, avendo constatato la necessità di tutelare un mondo contraddistinto da tante possibilità ma altrettanti pericoli[98]. Dal un punto di vista italiano, l'impellenza di un piano per la tutela della sicurezza informatica è stata avvertita già tramite l'adozione del "*National strategic framework for*

[96] Ministry of Defence. (2008). *National Cyber Security Strategy: Cyber Security Strategy Committee of Estonia*. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

[97] Ministry of Economic Affairs and Communications. (2019). Cybersecurity Strategy 2019-2022: Republic of Estonia. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

[98] Gli stati europei che hanno adottato dette strategie aggiornate sono : Regno Unito (2016), Francia (2015), Finlandia (2013), Polonia (2017), Svezia (2017), Lettonia (2014), Lituania (2018), Danimarca (2018), Cecoslovacchia (2015), Romania (2013), Bulgaria (2016), Grecia (2017), Ungheria (2018), Austria (2013), Spagna (2019), Portogallo (2019), Irlanda (2015), Belgio (2012).

cyberspace security" nel 2013[99] e poi successivamente tramite l'adozione del "*Italian cybersecurity action plan*" del 2017[100]. Quest'ultimo presenta una serie di obiettivi che si esplicano nel seguente modo: il rafforzamento di infrastrutture critiche nazionali e della loro capacità di difesa, il miglioramento delle capacità tecnologiche operative dei *cyber actors*, il consolidamento della capacità di controazione nei confronti delle attività criminali ed infine l'implementazione di una migliore cooperazione internazionale in materia di sicurezza informatica. Al di fuori dall'Unione Europea, una menzione particolare merita il piano in tema di sicurezza cibernetica adottato dal Canada[101], il quale presenta tre livelli operativi. Il primo comporta un rafforzamento della sicurezza e resilienza dei sistemi canadesi; tramite una forte cooperazione internazionale con i vari *partners*, il Canada si impegna a rispondere al meglio delle sue possibilità alla criminalità informatica e ad eventuali attacchi, rispondendo alle minacce in evoluzione e cercando di proteggere i sistemi privati, oltre a quelli pubblici. Il secondo punto trova la sua forza nella ricerca avanzata che porterà a sviluppare competenze e conoscenze informatiche. Con il terzo, infine, il governo federale canadese si impegnerà a promuovere la sicurezza informatica ed a collaborare con gli alleati per modellare al meglio il tema della sicurezza cibernetica internazionale[102].

In conclusione, mancando una definizione unitaria di cyber security sia a livello europeo che a livello internazionale, la comprensione del tema della sicurezza cibernetica e dei vari elementi chiave varia da stato a stato ma è possibile andare ad enucleare una serie di elementi comuni a tutte le varie strategie fino ad ora

[99] Presidency of the Council of Ministers. (2013). *National Strategic Framework for Cyberspace Security.* Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

[100] Presidency of The Council of Ministers. *(2017). The Italian Cybersecurity Action Plan*. Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

[101] Government of Canada, Public Safety Canada. (2020). *National Cyber Security Action Plan (2019-2024).* Consultato da https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx#a02

[102] *Ibid*.

adottate[103]. Queste ultime servono per definire un quadro di *governance* per la sicurezza informatica, per delineare le misure politiche e regolamentari necessarie per definire chiaramente gli obiettivi in tema di sicurezza, per migliorare o creare effettivi piani di risposta e di ripresa per le infrastrutture critiche di un paese che è vittima di un *cyber* attacco ed infine per amplificare la cooperazione con gli stati membri dell'Unione Europea e non. Di conseguenza, la cooperazione tra stati, non solo a livello europeo, è necessaria tanto per prepararsi efficacemente quanto per rispondere congiuntamente ad attacchi informatici; per questo, le strategie nazionali di sicurezza informatica rappresentano solo il primo passo in questa direzione.

Un ultimo punto da considerare su questo tema attiene alla distinzione di due termini che molto spesso vengono erroneamente assimilati e che presentano elementi distintivi da non sottovalutare: *information security* e *cybersecurity*. Infatti, mentre il primo si specifica esplicitamente nella costante e continua protezione delle informazioni, viste come un bene comune, da possibili danni derivanti da varie minacce e vulnerabilità, la *cybersecurity* d'altro canto, non si sviluppa solo e unicamente nella necessità di protezione del ciberspazio stesso, ma si articola anche nella protezione di coloro che operano nel ciberspazio e di tutte le loro risorse raggiungibili attraverso il ciberspazio[104].

1.6.2 La nozione di *cyber defence*

Tema decisamente più delicato è quello della *cyber defence*, soprattutto prendendo in considerazione, come sarà fatto più approfonditamente nei prossimi capitoli, i limiti che vengono imposti agli attori di detta attività. Basandosi su una visione di attività difensiva aerea sviluppata dalla dottrina militare americana, è possibile suddividere l'attività di difesa in due tipologie distinte: *active cyber*

[103] ENISA, op. cit., p. 41.

[104] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

defense e *passive cyber defense*[105]. Il primo elemento si concretizza in tutte quelle azioni cibernetiche difensive volte a distruggere, annullare oppure semplicemente ridurre l'efficacia delle minacce informatiche contro le forze amiche e contro i vari sistemi. Il secondo invece si concretizza nell'adozione di tutte quelle misure che non rientrano in quelle precedentemente menzionate e che si articolano nel tentativo di minimizzazione dell'efficacia delle minacce cibernetiche contro le forze e le risorse alleate[106]. Mentre le attività di difesa attiva sono rivolte a minacce specifiche, quelle di difesa passiva sono utili per aumentare la resistenza dei sistemi contro eventuali attacchi. Le prime possono inoltre riguardare operazioni dirette contro sistemi utilizzati da colui che effettua un *cyber attack*, nell'ottica pratica paragonabile ad un contrattacco. Le seconde includono ancora attività che comportano l'utilizzo di crittografia e steganografia[107], il monitoraggio e la gestione delle varie e distinte configurazioni, un controllo statistico delle vulnerabilità e la valutazione dei rischi, il *backup*[108] e recupero dei dati persi, istruzione e formazione degli utenti.

Quello che maggiormente rileva in tema di *cyber defense* è che quest'attività sottostà ad una serie di principi che devono essere rispettati[109], come il principio autorità, immunità di terzi, necessità, proporzionalità, coinvolgimento umano e

---

[105] Denning, D. E. (2013). Framework and Principles for Active Cyber Defense. *Computers & security*, 40. DOI: 10.1016/j.cose.2013.11.004. (Vedi pp. 109-110).

[106] *Ibid*., (pp. 109-110).

[107] Treccani. (2020). *Steganografia.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «tecnica, spesso inclusa nella → crittografia, che ha per obiettivo quello di nascondere un messaggio in modo che non possa essere letto da nessun altro all'infuori del destinatario. Al contrario delle tecniche propriamente crittografiche, la steganografia non si basa sulla trasformazione del testo, ma sull'occultamento fisico del messaggio. Nell'antica Grecia (da cui il nome) una comune tecnica steganografica era la ricopertura con argilla della tavoletta incisa con il messaggio segreto; un esempio di tecniche più moderne è quella dei *microdots* (micropunti), in cui il messaggio viene miniaturizzato, separato in diverse parti e infine inserito all'interno dei puntini delle lettere *i* che fanno parte delle parole di un documento con contenuti generalmente irrilevanti». https://www.treccani.it/enciclopedia/steganografia_%28Enciclopedia-della-Matematica%29/

[108] Treccani. (2020). *Backup.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «La procedura per la registrazione e memorizzazione delle operazioni, attuata al fine di disporre di informazioni sufficienti a ricostruire quanto è andato perso, nel caso in cui le operazioni non vadano a buon fine o si distruggano parte dei dati». Consultato da https://www.treccani.it/enciclopedia/backup/

[109] Denning, *op. cit*., p. 44. (Vedi pp. 111-112).

libertà civili. Il principio di autorità si caratterizza per il fatto che l'attività di difesa può essere adottata solo da autorità che sono effettivamente legittimate. Particolari problematiche di legittimità non risultano quando si tratta di attività di difesa prettamente interna, cosa che invece non avviene qualora si tratti di attività di difesa esterna. Il secondo principio, quello dell'immunità di terzi, presuppone che l'attività di *cyber defense* non può in nessun caso andare a causare un danno ingiusto ad un eventuale terzo. Il principio di necessità, strettamente correlato a quello di immunità di terzi, presuppone che qualsiasi attività di difesa, soprattutto quelle che potrebbero, sulla base di un'effettiva valutazione del rischio, comportare un danno ingiusto per parti terze, si esplica alla stregua del fatto che l'attività stessa deve essere impellente. Il quarto principio, quello di proporzionalità, presuppone che le difese informatiche attive non dovrebbero essere utilizzate a meno che il danno subito o potenziale non sia proporzionato ai benefici ottenuti. Il quinto principio presuppone l'insostituibile necessità di utilizzare lo strumento umano nel processo di difesa, in grado sia di razionalizzare efficacemente la situazione che di fornire un parere non cibernetico all'attività stessa. L'ultimo punto, infine, fa riferimento al principio stante il quale le difese informatiche attive dovrebbero rispettare le libertà civili di tutte le persone interessate, compresi i diritti alla *privacy*, alla libertà di parola e di associazione. Questo principio si applica agli utenti della rete di difesa, nonché a terzi e sospetti.

In conclusione, alla stregua delle difficoltà di definizione ravvisate, la distinzione tra attività di *cyber security* e *cyber defense* risulta lieve ma distinta. Infatti, mentre la prima è una tipologia di attività che si articola nella predisposizione di un piano avente la funzione di prevenire concretamente possibili attacchi, il quale comporta miglioramenti dei propri sistemi digitali e concreta collaborazione e scambio di informazioni tra i vari stati, l'attività di *cyber defense*, quella attiva quantomeno, presuppone l'esistenza di un attacco e la necessità di contrastarlo. Quello che rileva, ai fini del seguente elaborato è come concretamente,

nonostante gli innumerevoli passi avanti effettuati in tema di cooperazione e coordinazione sia dagli stati che dalle varie organizzazioni internazionali, ci si trovi ancora in una situazione che non prevede la creazione, per ora solo ipotetica e più volte prospettata, di un organo collettivo in grado di svolgere operazioni per riportare, costruire o prevenire la pace minata da un ipotetico attacco cibernetico[110], attività che viene normalmente svolta dall'ONU tramite le "*peacekeeping operations*", le quali sono operazioni militari che prevedono la possibilità di utilizzare la forza per il mantenimento della pace in seguito ad una minaccia o ad un'aggressione[111] . Proprio per questo motivo, anziché agire in maniera singola, è stata più volte auspicata la creazione di un organo in grado di svolgere operazioni di mantenimento della pace in seguito ad attacchi cibernetici volti ad indebolire o distruggere la difesa e la sicurezza cibernetica dei vari stati, i quali, sulla base dei requisiti fino a qui analizzati, sono in grado di minare la pace e la sicurezza internazionale.

1.7 I sistemi di difesa statali nel *cyber* spazio: Italia, Spagna, Russia e Cina.

Accanto ai sistemi di tutela contro l'attività cibernetica di varie organizzazioni internazionali, tema che verrà trattato nel terzo capitolo, potrebbe risultare utile avere una visione generale e sommaria dei sistemi di difesa all'interno del *cyber* spazio che sono stati concretamente istituiti nei singoli sistemi nazionali. Avendo già ampiamente trattato il sistema di una delle più grandi ed avanzate superpotenze nel mondo cibernetico come gli Stati Uniti, la trattazione riguarderà quattro paesi che, oltre all'Italia, meritano di essere quantomeno menzionati per vicinanza o forza.

[110] Almutawa, *op. cit*., p. 27.

[111] Conforti, B., & Focarelli, C. (2017). *Le Nazioni Unite* (11. ed.). CEDAM.

Partendo da un discorso prettamente nazionale, è possibile constatate come il contesto di tutela e di sicurezza del *cyberspace* sia stato notevolmente modificato tramite il Decreto del Presidente del Consiglio[112] Gentiloni, il quale ha riorganizzato totalmente l'architettura nazionale[113], cui è seguito il Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica. Tramite questo decreto è stato infatti stabilito che organo cardine nell'attività di cybersecurity italiana debba essere senza dubbio il Dipartimento delle Informazioni per la Sicurezza (DIS)[114], organo fondamentale subordinato alle direttive del Presidente del Consiglio dei ministri e con il compito fondamentale di garantire unitarietà nella ricerca informativa e nell'attività dell'Agenzia Informazioni e Sicurezza Interna (AISI) e dell'Agenzia Informazioni e Sicurezza Esterna (AISE). La prima ha il compito di "ricercare ed elaborare tutte le informazioni utili per difendere la sicurezza interna della Repubblica e le istituzioni democratiche da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica"[115]. Dunque, l'AISI si occupa di tutte le attività che vengono svolte sul territorio italiano e di contrastare le attività di spionaggio che vengono realizzate sia per danneggiare l'Italia sia per danneggiare gli interessi nazionali. L'AISE, d'altra parte, "ha il compito di ricercare ed elaborare tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica dalle minacce provenienti dall'estero[116]"; di conseguenza si occupa di tutte le attività che vengono svolte al di fuori del territorio italiano, attività che hanno come obiettivo interessi politici, economici e militari.

---

[112] D.P.C.M. 87/2017.

[113] Dominioni, S. (2019, 2 dicembre). *Cybersecurity: l'architettura della difesa italiana*. Istituto per gli studi di politica internazionale. Consultato da https://www.ispionline.it/it/pubblicazione/cybersecurity-larchitettura-della-difesa-italiana-24546

[114] Sistema di informazione per la sicurezza della Repubblica. (n.d.). *DIS: Chi siamo.* Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html

[115] Sistema di informazione per la sicurezza della Repubblica. (n.d.). *AISI: Chi siamo*. Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aisi.html

[116] Sistema di informazione per la sicurezza della Repubblica. (n.d.). *AISE: Chi siamo.* Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html

Per quanto concerne invece la Spagna, è possibile constatare come nel 2006 sia stato istituito lo "*Instituto Nacional de Ciberseguridad"* (INCIBE)[117]. Il suddetto organo statale, con sede a Leòn, svolge un ruolo primario nel rinforzo della cyber sicurezza e nella tutela dell'informazione e della *privacy* soprattutto per quelle infrastrutture che da un punto cibernetico assumono una particolare rilevanza dal punto di vista statale. Essendo sottoposta alla normativa prevista dal "*Real Decreto 3/2010, de 8 de enero*", INCIBE opera sulla base di 4 pilastri fondamentali: fornitura di servizi, investigazione, formazione di informatici e coordinamento[118]. Accanto a suddetto organo, con la legge 11/2002 (testo modificato l'ultima volta il 18 marzo 2020)[119] , è stato istituito il centro nazionale di Intelligenza che viene definito dall'art.1 della legge stessa il quale sancisce che l'attività fondamentale per cui è stato creato si riverbera nella formazione di raccolte di dati, studi e proposte che siano in grado di prevenire ed individuare eventuali pericoli che avranno rilevanza da un punto di vista informatico in grado di creare danni all'indipendenza e all'integrità territoriale spagnola[120]. L'operato svolto suddetto organo, dunque, si articola in spionaggio e controspionaggio, con anche funzioni di coordinamento.

La Russia si è dimostrata nel corso del tempo l'antagonista per eccellenza degli Stati Uniti, soprattutto in tema di spionaggio, controspionaggio e tutela delle informazioni interne che riguardano lo stato stesso. A partire dalla guerra fredda, dunque, il tema dell'attività di *intelligence* si è andato a sviluppare dentro e soprattutto il mondo cibernetico. Il 12 aprile 1995 è stato istituito il "*Federal Security Service of the Russian Federation",* la principale agenzia di intelligence e sicurezza russa. Suddetto organismo, che risponde direttamente al presidente

[117] INCIBE. (n.d.). *Cómo trabajamos.* Consultato da https://www.incibe.es/que-es-incibe/como-trabajamos

[118] INCIBE. (n.d.). *Qué hacemos*. Consultato da https://www.incibe.es/que-es-incibe/que-hacemos#actividad

[119] BOE. Jefatura del Estado. (2002, 7 maggio). *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.* https://www.boe.es/eli/es/l/2002/05/06/11/con

[120] BOE. Legislación Consolidada. (2002, 7 maggio). *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.* https://www.boe.es/buscar/pdf/2002/BOE-A-2002-8628-consolidado.pdf

Putin, svolge attività di spionaggio e controspionaggio per garantire non solo la sicurezza del paese ma anche la collezione di informazioni riguardanti altri stati[121].

Ultima ma non meno importante, è l'agenzia di *intelligence* e di sicurezza cinese che svolge un ruolo preliminare all'interno del cyber spazio. In particolare, nel 2014 è stata istituita il *Cyberspace Administration of China* (CAC)[122], con sede operativa a Pechino, che è l'organo centrale di regolamentazione, censura, sorveglianza e controllo di Internet per la Repubblica popolare cinese. È proprio la sorveglianza uno dei punti fondamentali dell'attività della CAC. La Cina detiene il numero più alto di utenti collegati ad internet; una stima approssimativa, effettuata nel 2015, conta ben 641 milioni di users[123]. Proprio il quantitativo di persone che utilizzano questo sistema ha portato una necessità concreta di adottare politiche di sorveglianza sempre più stringenti. Da quando il presidente Xi Jinping ha ottenuto il potere nel 2012, internet è stato visto come un campo di battaglia per il controllo ideologico. Detto regime stringente può essere efficacemente riassunto con una semplice direttiva del 14 luglio 2015, la quale stabilisce espressamente che:

> *«All websites must, without exception, use as the standard official and authoritative media reports with regards to the detention of trouble-making lawyers by the relevant departments. Personnel must take care to find and delete harmful information; do not repost news from non-standard sources».*

---

[121] Wikipedia. (2020). *Federal Security Service.* Consultato da https://en.wikipedia.org/wiki/Federal_Security_Service

[122] Miao, Weishan, M., & Lei, W. (2016). Policy review: The Cyberspace Administration of China. *Global Media and Communication,* 12(3), 337-340. 10.1177/1742766516680879

[123] CECC (Congressional-Executive Commission on China). (2015, 18 settembre). *Urging China's President Xi Jinping to Stop State-Sponsored Human Rights Abuses.* Statement by Xiao Qiang. https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Human%20Rights%20Abuses%20-%2018Sept15%20-%20Xiao%20Qiang.pdf

Questa la direttiva fornita subito dopo l'arresto di 200 persone, tra avvocati ed attivisti, ritenuti semplicemente cospiratori sulla base di attività di libera informazione e libero servizio svolte avvalendosi dello strumento di internet.

Alla luce di quanto descritto in questo capitolo, nel quale sono stati presentati i punti cardine della tematica, risultano evidenti la nebulosità e la complessità che ancora avvolgono e caratterizzano lo studio del mondo cibernetico. Trattare questo argomento, difatti, è un compito ambizioso vista la sua ampiezza e la sua costante evoluzione. Gli aspetti da considerare sono molteplici, come le situazioni che ne derivano e gli utenti coinvolti. Tuttavia, la prerogativa di questo elaborato consiste nell'analisi e nella spiegazione teorica dei concetti più importanti relativi a questo ambito, al fine di fornire molteplici implicazioni concrete che possano essere interpretate in chiave giuridica. Partendo da questo presupposto, nei capitoli successivi, l'attenzione si concentrerà sull'importante possibilità di creazione di organi internazionali che, in virtù della cooperazione internazionale, possano garantire e preservare quei fondamentali principi spesso a rischio, soprattutto nel mondo del cyberspazio, quali la sicurezza, la tutela delle informazioni e il rispetto della privacy, lavorando in termini di *cyber security* e *cyber defence.* Accanto a questo, obiettivo dell'elaborato sarà cercare di spiegare come gli stati si sono rapportati con il mondo cibernetico da un punto di vista prettamente giuridico, tramite le varie dichiarazioni statali, relative prevalentemente all'applicabilità della normativa internazionale in materia. Infine, accanto al tema della creazione di un organo quale un *cyber peacekeeping team* in seno alle Nazioni Unite, si cercherà di analizzare, a grandi linee, il regime di responsabilità statale per le operazioni compiute nel *cyberspace*.

Capitolo 2

LE FONTI NORMATIVE INTERNAZIONALI APPLICABILI AL *CYBERSPACE*

SOMMARIO:

2.1. Cenni storici - 2.2. Il ruolo del diritto internazionale pattizio - 2.3 Il ruolo del diritto consuetudinario – 2.3.1 Principi e norme di diritto internazionale applicabili nel *cyberspace*: il principio di sovranità territoriale - 2.4 Il Tallinn Manual del 2013 e il Tallinn Manual 2.0 — 2.5. Il ruolo delle dichiarazioni statali relative al diritto internazionale applicabile al cyberspace– 2.6. *Segue*: diritti umani e *cyberspace* - 2.7. *Segue*: operazioni cibernetiche ed uso della forza – 2.7.1. Operazioni cibernetiche e minaccia dell'uso della forza – 2.7.2. *Segue*: operazioni cibernetiche e legittima difesa

2.1 Cenni storici

La mancanza di un'unità di visione relativa al regime legislativo da applicare concretamente all'interno del *cyberspace,* derivante da un altrettanto grave mancanza di uniformità in termini definitori, ha portato numerosi problemi a cui diversi studiosi hanno cercato di dare, senza univoco successo, risposta. Partendo da un discorso generale, quello che può essere constatato attiene alla visione, distinta da qualsiasi altra realtà comunemente conosciuta, che viene affidata al mondo cibernetico. Analizzando di conseguenza da un punto di vista prettamente geografico il tema, quello che viene alla luce riguarda una nuova concezione di dimensione del *cyberspace*, relazionata ad un argomento di particolare importanza, ovvero quello del conflitto fra vari stati. Come infatti brillantemente analizzato dal dr. Luigi Martino, esistono quattro diverse dimensioni relative alla conflittualità che sono rispettivamente: terra, mare, aria e spazio extra-atmosferico. A queste quattro dimensioni si è aggiunto l'ultimo dominio, dominio che, per la natura stessa da cui è composto, si differenzia notevolmente dagli altri quattro: il dominio cibernetico.[124] La caratteristica principale del dominio cibernetico è che, contrariamente agli altri, i quali presentano una natura

[124] Martino, L. (2013). La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace ei rischi di guerra cibernetica. *Centro Interdipartimentale di Studi Strategici Internazionali e Imprenditoriali (CSSII), Florence*.

fisica totalmente univoca, possiede una natura ibrida, cioè contraddistinta tanto da elementi fisici e materiali (un cyber attacco che comporta l'intrusione in un sistema missilistico di un altro stato, cui segue il lancio non autorizzato di un attacco cinetico, inevitabilmente viene osservato come un elemento che crea danni fisici e materiali) quanto da elementi propriamente virtuali (come la semplice creazione di un archivio digitale). La natura ibrida di questo mondo, apparentemente lontano da quello reale, può essere fornita, come spiega accortamente Martin C. Libicki, professore alla *Frederick S. Pardee RAND Graduate School* di Santa Monica in California, andando ad analizzare la presenza simultanea di tre livelli distinti: livello fisico, livello sintattico e livello semantico[125]. Il primo livello si esplica nel fatto che qualsiasi sistema di informazione si basa su uno strato fisico costituito da scatole e nella maggior parte dei casi, fili. Se si rimuove lo strato fisico tecnicamente anche il sistema "scompare"; è dunque certamente possibile attaccare un sistema informativo attraverso mezzi cinetici. Il livello sintattico invece contiene tutte le istruzioni che i progettisti e gli utenti forniscono alla macchina stessa ed ai protocolli, tramite i quali le macchine interagiscono l'una con l'altra: riconoscimento, inquadramento dei pacchetti, *routing* o più comunemente instradamento[126], formattazione di documenti[127], manipolazione di *database*… L'ultimo livello, infine, è il livello semantico, il quale ha il compito fondamentale di rielaborare i dati contenuti dentro alle varie macchine. Di conseguenza, la natura ibrida del *cyberspace*, le difficoltà relative ad una definizione unitaria, i problemi propri delle delimitazioni territoriali e le difficoltà nell'ottica applicativa del principio di sovranità, sono solo alcuni punti che hanno portato, al giorno d'oggi, alla

[125] Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND *Corporation*.

[126] Treccani. (2020). *Instradamento*. Enciclopedie on line, Istituto della Enciclopedia Italiana: «In telematica, e in particolare nella tecnologia Internet, operazione con la quale i messaggi sono inviati verso l'indirizzo del destinatario, per mezzo della tecnica della commutazione di pacchetto […]». Consultato da https://www.treccani.it/enciclopedia/instradamento/

[127] Treccani. (2020). *Formattazione.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «In informatica, trasformazione di dati e/o informazioni in un formato predefinito; in particolare, la preparazione di un disco magnetico o ottico in modo che sia pronto a ricevere le informazioni da memorizzare». Consultato da https://www.treccani.it/enciclopedia/formattazione/

difficoltà di creare una normativa unitaria. Come precedentemente spiegato, per quelle attività il cui svolgimento ed i cui effetti non si riscontrano solo in un singolo paese, è necessaria l'applicazione di una normativa internazionale. Attualmente, la normativa prevalente applicabile in caso di *cyber activity* è contenuta essenzialmente, come verrà specificatamente discusso nei paragrafi successivi del capito, all'interno dei trattati e delle norme consuetudinarie. Accanto agli attori statali, i quali svolgono singolarmente un ruolo importantissimo nella definizione e creazione di una particolare disciplina in tema di *cyber activities*, un ruolo fondamentale è oggi svolto da varie organizzazioni internazionali, le quali sono state in grado di adattarsi alle nuove tecnologie e hanno apportato interpretazioni più ampie in grado di estendere, sempre nei limiti della legittimità, i propri compiti.

Come precedentemente rilevato, uno degli elementi principali che contraddistinguono le difficoltà normative si riverbera nel tema dei confini territoriali. L'applicabilità di diritti e leggi statali, al giorno d'oggi, risulta subordinata in prima istanza ai confini geografici; in altre parole, i confini territoriali determinano quali norme si andranno ad applicare in seguito ad eventi verificati dentro i confini dei territori stessi[128]. Gli stessi non sono tracciati arbitrariamente ma sono frutto di eventi storici che si sono di anno in anno susseguiti; quest'ultimo elemento può essere constatato sulla base di tre punti distinti ovvero potere, effetti e legittimità. Per quanto riguarda il potere, l'applicabilità di una norma si esplica essenzialmente anche alla stregua della capacità di far rispettare la stessa. La possibilità di legiferare richiede un certo meccanismo per l'applicazione della legge stessa, il quale a sua volta dipende dalla possibilità di eseguire un controllo fisico e di applicare misure coercitive. Il secondo tema, che riguarda gli effetti prodotti, si esplica anch'esso su una necessaria conciliazione tra confini territoriali e normativa applicabile all'interno degli stessi. Il terzo ed ultimo riguarda, invece, la legittimità: sulla base dei

[128] Johnson, D., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367-1402. doi:10.2307/1229390

confini territoriali, compito dello stato è garantire l'applicazione della normativa relativa ai fatti considerati. Il problema fondamentale che rileva in tema di attività cibernetica è senza dubbio l'assenza radicale di confini e delimitazioni geografiche nel *cyberspace.* Conseguentemente, il sistema di internet ha totalmente ribaltato il classico sistema di applicazione delle leggi basato semplicemente sulla delimitazione di confini territoriali; quelli che normalmente vengono definiti "*physical borders*" vanno ad assumere una rilevanza assolutamente inferiore in tema di definizione della normativa applicabile. Infatti, il *cyber* spazio non ha confini territoriali e "distrugge" la localizzazione fisica in tre differenti direzioni[129]. La prima si articola nel fatto che le attività che vengono svolte nel *cyberspace* avvengono ovunque e, di conseguenza, in nessun luogo; queste attività difatti ignorano totalmente l'esistenza di confini fisici. Il costo e la velocità dei messaggi risultano indipendenti da qualsiasi distanza, non esistono barriere che impediscano in alcun modo di raggiungere i posti geograficamente più remoti. In secondo luogo, l'attività considerata spesso non è ricollegabile ad un soggetto localizzabile geograficamente; ci sono infatti attività che non hanno alcun legame con luoghi fisici ma che hanno luogo unicamente dentro la rete stessa, la quale ovviamente non è localizzabile. In terzo luogo, infine, la rete consente connessioni simultanee tra plurime persone le quali non conoscono o non possono essere in grado di conoscere l'ubicazione fisica delle altre parti. Si può dunque parlare di "luogo" di eventi e transizioni ma soltanto in relazione ad uno spazio virtuale semplicemente costituito dagli "indirizzi" delle macchine ai quali vengono indirizzati messaggi ed informazioni; tuttavia, il sistema di indirizzamento macchina è molto spesso indipendente dall'indirizzo fisico e dall'ubicazione di tali macchine[130].

L'ultimo punto che verrà analizzato attiene all'ipotesi che vede il *cyberspace* come una *law free-zone,* ovvero una dimensione della realtà, seppur virtuale, in

[129] Post, D. G. (1996). Governing cyberspace. *Wayne Law Review, 43(1),* 155-172.

[130] Burk, D. L. (1995). Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermark. *Law School Journal,* 1(1). Consultato da https://scholarship.richmond.edu/jolt/vol1/iss1/4/

cui tutti possono condurre qualunque attività, tenendo anche comportamenti definiti ostili al di sopra delle leggi e di restrizioni. Per spiegare l'inesattezza di questa teoria, è necessario rifarsi a quanto storicamente avvenuto al diritto internazionale nel corso del tempo. In particolare, non è di certo la prima volta in cui si ha un cambiamento radicale della tecnologia; il diritto internazionale di volta in volta ha avuto l'obbligo di adattarsi ai tempi correnti e di rapportarsi con i cambiamenti[131]. Partendo quindi dal presupposto che gli strumenti con cui condurre le guerre si sono evoluti e si evolveranno all'infinito, compito degli studiosi di diritto internazionale sarà interpretare la normativa esistente per poterla applicare a tale innovazione. L'elaborato seguente andrà a spiegare come concretamente i trattati internazionali e le norme consuetudinarie siano interpretabili anche in tema di attività cibernetiche, andandosi poi a focalizzare sul problema di sovranità statale all'interno del *cyberspace*. In terzo luogo, sarà esaminato il Manuale di Tallinn 2.0, facendo anche riferimento al Manuale che l'ha preceduto nel 2013, cercando di spiegare la sua valenza da un punto di visto legislativo, passando poi all'esame generico della normativa prevista nel caso di conflitto armato. Infine, il discorso si incentrerà sui diritti umani riconosciuti all'interno del cyberspazio e sui loro metodi di tutela.

2.2 Il ruolo del diritto internazionale pattizio

Quando si parla del regime giuridico che regola l'attività cibernetica da un punto di vista internazionale, è necessario fare riferimento alla distinzione intercorrente fra norme di diritto internazionale generale e norme di diritto internazionale particolare: tra le prime annoveriamo le norme consuetudinarie e i principi generali di diritto internazionale applicabili a tutti gli stati, tra le seconde gli

[131] Koh, H. (2012). Remarks as Prepared for Delivery By Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, Sept 18, 2012. *Harvard International Law Journal (Online)*, *54*, 1-12.

accordi e le fonti previste dagli accordi[132]. Un ruolo particolare è infine lasciato alle decisioni giudiziali e alla dottrina degli autori più autorevoli delle varie nazioni. Queste fonti sono espressamente riconosciute dall'articolo 38 dello "*Statute of the international Court of Justice"* (ICJ), il quale sancisce letteralmente quali saranno le fonti normative che verranno prese in considerazione dalla Corte di Giustizia Internazionale. [133]

L'articolo 2 della *Convenzione di Vienna* fornisce una concreta definizione di trattato internazionale, visto come un accordo che viene concluso tra due o più stati per iscritto, regolato dal diritto internazionale, costituito da uno o più strumenti connessi[134]. La Convenzione stessa, oltre a fornirne la definizione, determina anche le regole che sottostanno alla creazione, interpretazione, termine ed invalidità dei trattati stessi[135]. Dall'altra parte le norme consuetudinarie sono norme non scritte che si sono sviluppate nel corso del tempo sulla base del comportamento, ripetuto nello stesso modo più volte nel panorama internazionale, che ha portato a seguirle e che sono vincolanti per qualsiasi stato.

Un ulteriore punto è stato inoltre più volte dibattuto nel corso del tempo, chiedendosi gli studiosi[136] se le norme internazionali, nate storicamente per regolare i rapporti tra i vari e diversi stati, fossero applicabili anche ai singoli individui. Sebbene il diritto internazionale continui a governare in primo luogo le relazioni internazionali tra gli stati, nell'ultimo secolo si è occupato di affrontare i comportamenti individuali. Esempi classici sono le norme giuridiche internazionali che consentono la giurisdizione universale su determinati atti come i crimini di guerra. Tuttavia, per corrispondere al diritto internazionale, tutte

---

[132] Gioia, A. (2013). *Diritto internazionale: manuale breve*. Giuffrè Editore. (Vedi p.10).

[133] Stato. (2015, 24 febbraio). Traduzione de *Convenzione di Vienna sul diritto dei trattati (1969).* Consultato da https://www.admin.ch/opc/it/classifiedcompilation/19450070/201201250000/0.193.501.pdf

[134] *Ibid.*

[135] Roscini, *op. cit.*, p. 6. (Vedi p. 20).

[136] Schmitt, M. N. & Vihul, Liis. (2014, 1 dicembre). The Nature of International Law Cyber Norms. *Tallinn Papers No. 5 (NATO Cooperative Cyber Defence Centre of Excellence, Dec. 2014)*. Consultato da SSRN: https://ssrn.com/abstract=2543520

queste norme devono essere concordate da più Stati, attraverso trattati o lo sviluppo del diritto consuetudinario[137].

Il tema assume una particolare rilevanza nel momento stesso in cui si cerca di ricomprendere, nella normativa corrente, le varie attività cibernetiche considerate. Come fatto notare antecedentemente, non esiste al giorno d'oggi un vero e proprio trattato o alcun accordo internazionale che vada singolarmente a disciplinare il mondo del *cyberspace*, causando di conseguenza un'apparente lacuna normativa. Detta lacuna non si verifica, tuttavia, alla stregua dell'interpretazione evolutiva che viene fornita del diritto internazionale esistente. La nozione di interpretazione evolutiva non risulta ampiamente dibattuta come elemento prioritario nelle varie analisi effettuate dagli studiosi[138]; tuttavia, quello che si può rilevare è come, molto spesso, sia stata individuata come un'interpretazione semplicemente aggiornata ai tempi che corrono[139].

Nonostante vari e plurimi trattati siano stati stipulati comprendendo negli stessi le materie più disparate, le *cyber operations* che raggiungono la valenza di uso della forza o, comunque sia, di atto di ostilità dovrebbero senza dubbio rientrare all'interno di quell'area del diritto internazionale che regola l'utilizzo della forza da parte degli stati (*jus ad bellum*) e di quel ramo di diritto internazionale che regola la legittimità di operazioni che possono essere attuate una volta che il conflitto armato già è esploso (*jus in bello*, più comunemente la legge sul conflitto armato o quello che viene definito *international humanitarian law*)[140]. Mancando un trattato ad hoc, la domanda che sorge spontanea è la seguente: quando le *cyber operations* possono essere paragonabili, e di conseguenza disciplinate nello stesso modo, ai normali atti di uso della forza?

---

[137] *Ibid.*

[138] Turrini, P. (2012). *L'interpretazione evolutiva nella giurisprudenza internazionale*. [Tesi di dottorato, Università degli Studi di Firenze]. Consultato da https://flore.unifi.it/retrieve/handle/2158/826147/27268/Tesi%20completa%20%28Paolo%20Turrini%29%20-%2014-01-2013.pdf

[139] Cannizzaro, E. (2012). *Diritto internazionale*. Giappichelli: Torino. (Vedi pp. 170-173).

[140] Roscini, *op. cit.*, p. 6.

Le fondamenta della normativa propria dello *jus ad bellum* e *jus in bello* sono riscontrabili in trattati come la *Carta delle Nazioni Unite* del 1945, le convenzioni dell'Aia nel 1899 e nel 1907, le quattro *Convenzioni di Ginevra* relative alla protezione delle vittime di guerra e i corrispettivi protocolli aggiuntivi del 1977. Ovviamente, per ragioni prettamente storiche, nessuno dei seguenti trattati rimanda espressamente ad alcun tipo di attività cibernetica, non esistendo al tempo la possibilità di sferrare gli attacchi fino ad ora analizzati, sulla base di una mancanza effettiva della materia prima, ovvero una rete in grado di connettere tutti i portali del mondo. Il concetto di interpretazione evolutiva, alla stregua del quale risulta possibile assimilare dette attività cibernetiche alle attività che raggiungono il livello di atti comprendenti l'uso della forza, viene garantito tramite un articolo particolare della *Convenzione di Vienna*, ovvero l'art. 31, il quale fornisce, a tutti gli effetti, regole interpretative determinate e predefinite, le quali partono da un concetto di interpretazione seguendo i principi di buona fede. Il punto cardine dell'articolo, per la parte cui si rivolge il seguente elaborato, è il numero 3 paragrafo b, il quale esplica che la prassi sorta in seguito ad elementi innovativi sarà osservata nell'interpretazione evolutiva degli strumenti del trattato stesso[141]. La teoria stante la quale le attività cibernetiche sarebbero accomunabili ai normali atti previsti espressamente dai trattati che concernono lo *jus ad bellum* e lo *jus in bello* trova solido fondamento nel fatto che moltissimi stati hanno affermato l'applicazione delle leggi esistenti alle *cyber operations*, andando di conseguenza ad includere anche la *Carta delle Nazioni Unite* e il diritto sui conflitti armati, molto spesso neanche differenziando espressamente trattati e norme consuetudinarie. Potenze internazionali come gli Stati Uniti hanno dichiarato che tutte le attività cibernetiche che assumono un determinato rilievo equivalgono (e sono di conseguenza regolate allo stesso modo) alle normali attività che usualmente vengono considerate come uso della forza[142]. Anche se le singole dichiarazioni

[141] *Ibid.*

[142] Guymon, C. D. (ed). (2012). *Digest of United States Practice in International Law.* (Vedi p. 594).

statali verranno analizzate in un paragrafo apposito, altri stati come Italia[143], Russia[144] o organizzazioni internazionali regionali, tra le quali la stessa Unione Europea[145], hanno confermato suddetta visione. Inoltre, nel 2013 è stato constatato in seguito al report fornito dal *Group of Governamental Experts*[146] (GGE), come il diritto internazionale, con particolare riguardo alla Carta stessa delle Nazioni Unite, sia applicabile nel *cyberspace* ed è essenziale per mantenere la pace e stabilità anche attraverso la promozione di una ICT (*Information and Communication Technologies*) aperta, libera e sicura[147].

Accanto al tema appena esposto, è possibile constatare come, da un punto di vista pratico, l'estensione interpretativa dei trattati di diritto umanitario internazionale ha portato, come esposto anche dal protocollo I addizionale della Convenzione di Ginevra in termini relativi all'art.36 della stessa, ad includere nella tutela fornita dai trattati stessi l'utilizzo di armi innovative quali quelle cibernetiche che, al tempo della ratifica, non erano neanche lontanamente immaginate[148].

Infine, è possibile constatare come il cyberspazio non abbia acquisito uno status giuridico speciale all'interno del diritto internazionale, ma, al contrario, le categorie giuridiche ed i vari principii esistenti sono stati applicati al mondo cibernetico[149]. Tuttavia, dato che il *cyber* spazio è un dominio che offre ampie possibilità ma contiene al tempo stesso molti rischi e pericoli il più delle volte, è

---

[143] Governo italiano. (2012, 17 settembre). *La posizione italiana sui principi fondamentali di Internet*. (Vedi p 5).

[144] The Russian Ministry of Defense. (2011, settembre). *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*. (Vedi p. 6).

[145] European Commission. (2013, 7 febbraio). *EU Cyber security strategy: An Open, Safe and Secure Cyberspace.* (Vedi pp 15–16).

[146] United Nations. (n. d.). *Group of Governmental Experts*. Definizione: «Gruppo istituito dalla General Assembly delle Nazioni Unite, con risoluzione 73/266, con compiti di sorvegliare l'attività dei vari stati membri all'interno del cyberspace per tutelare la sicurezza internazionale». Consultato da https://www.un.org/disarmament/group-of-governmental-experts/

[147] United Nations General Assembly. (2013, 24 giugno). *Doc A/68/98. Developments in the field of information and telecommunications in the context of international security*. (Vedi p. 8).

[148] Roscini, *op. cit.*, p. 6.

[149] Tsagourias, N., & Buchan, R. (Cur.). (2015). *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

stata ipotizzata un'implementazione della cooperazione che possa portare ad un trattato vero e proprio, avente carattere globale e negoziato a livello mondiale, in grado di stabilire forti ed efficaci regole di condotta, prevedendo soprattutto regole definitive relative ai vari conflitti di giurisdizione[150].

Si può altresì constatare come, dal punto di vista del diritto internazionale pattizio, infine, la creazione di un testo normativo generale in grado di creare, per i vari stati ratificanti, una *governance* di internet è, fino a questo momento, risultato impossibile. Vari e plurimi tentativi sono stati effettuati ma senza dubbio il più importante tra questi è rappresentato dal fallimento della Convenzione generale del "*World Summit on Information Society (WSIS)*"[151], proposta dall'Assemblea Generale delle Nazioni Unite il 21 dicembre 2001 con la risoluzione 56/183[152]. Mentre la prima fase della Convenzione aveva ad oggetto il tentativo di accordare gli stati relativamente alla necessità di dotarsi di diverse regole comuni per disciplinare la società dell'informazione[153], la seconda fase aveva mire assolutamente più ampie e, di conseguenza, di più complicata realizzazione; l'obiettivo considerato era quello di riuscire a creare un vero e proprio "accordo quadro" relativamente alla regolamentazione del mondo cibernetico. Come rilevato nel corso dell'elaborato, l'unico trattato ad oggi contenente norme generali è rappresentato dalla Convenzione del Consiglio d'Europa sulla cybercriminalità, adottata a Budapest nel 2001[154]. Il compito di questa convenzione si riverbera nel tentativo di fornire un quadro normativo

[150] Kamal, A. (2005). *The Law of Cyber-Space: An invitation to the table of negotiations*. United Nations Institute of Training and Research.

[151] Ruotolo, G. M. (2014). Internet (Diritto Internazionale)(Internet (International Law)). *RUOTOLO GM*, in *Enciclopedia del diritto–Annali, Milano*, *2104*, 545.

[152] United Nations General Assembly. (2002, 31 gennaio). *A/RES/56/183. Resolution 56/183 World Summit on the Information Society*. Consultato da https://undocs.org/pdf?symbol=en/A/RES/56/183

[153] Ruotolo, *op. cit*., p. 61.

[154] Il Consiglio federale. Il portale del Governo svizzero. (2020, 14 settembre). *Convenzione sulla cibercriminalità*. Consultato da https://www.admin.ch/opc/it/classified-compilation/20100537/index.html

comune per permettere agli stati di armonizzare il diritto nazionale penale in materia di reati commessi tramite internet[155].

2.3 Il ruolo del diritto internazionale consuetudinario

La seconda fonte del diritto internazionale risulta essere il diritto consuetudinario, da sempre consolidato nel tempo e che è stato oggetto di numerosi e plurimi dibattiti relativamente alla natura di cui è composto e ai margini possibili di incertezza che lo contraddistinguono. La specialità della consuetudine è che la stessa è una norma non scritta; si crea nel corso del tempo e, a differenza di quanto avviene nel caso dei trattati, risulta applicabile a qualsiasi stato, con sole poche eccezioni che saranno brevemente menzionate nel corso della trattazione. Il diritto consuetudinario si crea e si cristallizza qualora siano presenti due requisiti determinati: un elemento oggettivo, la "*diuturnitas"*, che comporta la pratica ripetuta dello stesso comportamento da parte di più stati, ed un elemento soggettivo, ovvero *l'opinio juris sive necessitatis*, cioè la convinzione concreta per lo stato che la esamina relativa all'obbligatorietà ed alla necessità del comportamento stesso[156]. Una volta che la norma consuetudinaria è effettivamente emersa, diventa applicabile a tutti gli stati, anche a quelli che non hanno partecipato effettivamente alla cristallizzazione della stessa[157].

Più complicato, rispetto a quanto avviene per i trattati, è l'estensione della consuetudine al tema delle *cyber operations*. La ragione di detta difficoltà si riverbera in primis nella natura stessa delle *cyber operations*, circondate, nella maggior parte dei casi, da elementi di segretezza o che comunque gli stati si dimostrano restii a divulgare. Quello che avviene all'interno del *cyberspace* risulta essenzialmente più complicato da percepire chiaramente. Inoltre, gli stati

[155] Ruotolo, *op. cit.*, p. 61.

[156] Conforti, B., & Iovane, M. (1997). *Diritto internazionale*. Editoriale scientifica. (Vedi p. 220).

[157] Schmitt, *op. cit.*, p. 19. (Vedi pp. 24-25).

malvolentieri forniscono opinioni riguardanti la legalità delle operazioni nello spazio cibernetico e la mancanza di uniformità di comportamenti e definizioni impedisce molto spesso l'applicazione della consuetudine, soprattutto sulla base dell'impossibilità di avere quella "*diuturnitas",* ovvero quel ripetuto e unanime comportamento attuato dagli stati. Di conseguenza, questi fattori impediscono la cristallizzazione di nuove norme consuetudinarie, contraddistinte in realtà da una forte elasticità che sarebbe in grado adattarsi ai tempi moderni. Pertanto, l'impatto normativo del diritto consuetudinario è più facile avvenga sulla base di interpretazione delle norme consuetudinarie esistenti, piuttosto che sulla creazione di nuove. Questo ultimo elemento fa quindi sorgere ulteriori problemi per due motivi: le norme consuetudinarie non sono, come i trattati, espressamente articolati e non ci sono regole uniformi relative alla loro interpretazione, come invece avviene nel caso della Convenzione di Vienna[158]. Al giorno d'oggi non risulta univoca la determinazione di norme di diritto consuetudinario che siano in grado di limitare la sovranità statale nel mondo di internet applicabili al *cyberspace*, sulla base del moderno sviluppo del diritto internazionale[159]. Tuttavia, il ruolo lasciato al diritto consuetudinario in tema di operazioni informatiche è duplice. Da una parte, le norme consuetudinarie dello *jus ad bellum* e *jus in bello* si estendono alle *cyber operations* che raggiungono il livello di utilizzo della forza o di atti di ostilità, nello stesso modo di quanto avviene con i trattati. Dall'altra parte, non è possibile escludere a priori che le norme consuetudinarie specifiche per la guerra cibernetica possano essere oggetto di un processo di formazione e cristallizzazione nel corso del tempo.[160] Le difficoltà relative all'applicabilità delle norme di diritto consuetudinario in materia cibernetica sono state riscontrate da alcuni commentatori, i quali hanno asserito che risulta impossibile che si sia sviluppato un diritto consuetudinario nuovo in

[158] Prochko, *op. cit.,* p.25.

[159] Ruotolo, *op. cit.,* p. 61.

[160] Roscini, *op. cit.,* p. 6. (Vedi p. 25).

materia dato che il fenomeno risulta troppo recente[161]. La visione rilevata invece dagli esperti nel Manuale di Tallinn si riverbera nella constatazione che «le pratiche cibernetiche dei vari stati e le dichiarazioni disponibili di *opinio juris* sono particolarmente scarse», per questo motivo risulta molto spesso difficile concludere per l'esistenza di una specifica normativa consuetudinaria in materia cibernetica[162]. Per poter verificare la sussistenza di queste affermazioni, è necessario andare a verificare che cosa si intende per "*diuturnitas"*, ovvero la pratica ripetuta nel tempo dello stesso comportamento. Nel momento in cui non risulta possibile attribuire un'operazione cibernetica ad uno stato, la determinazione dell'*usus* considerato come elemento della consuetudine comprende atti non solo fisici ma anche verbali di stati, come, per esempio, le dichiarazioni politiche o diplomatiche, i comunicati stampa, i manuali ufficiali che sono applicabili all'ambito militare, o ancora i commenti governativi sui progetti dei trattati o infine le dichiarazioni adottate tramite le risoluzioni degli organi delle organizzazioni internazionali[163]. Quest'ultimo punto è risultato particolarmente rilevante dal momento che anche le opinioni fornite dai "*legal advisers"* assumono importanza come esempi di atti verbali; su questo punto un caso degno di nota risulta essere il discorso sul diritto internazionale applicabile nel *cyber* spazio tenuto dall'allora consulente legale del dipartimento americano della CYBERCOM, Harold Koh, che verrà evidenziato nel paragrafo relativo alle dichiarazioni statali[164]. Infine, come rilevato dall'ICJ, il passaggio di un breve

[161] Schmitt, N. M. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 37, 1-41, pag 921. Consultato da https://apps.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf

[162] Schmitt, M. N. (Cur.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press. (Vedi p. 5).

[163] Committee On Formation Of Customary (General) International Law. (2000). *Statement of Principles Applicable to the Formation of General Customary International Law*, in International Law Association (ILA), Report of the Sixty-Ninth Conference, pp. 1-66. London Conference. Consultato da http://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ILA%20Report%20on%20Formation%20of%20Customary%20International%20Law.pdf (Vedi p. 725).

[164] Hongju Koh, H. (2012). International Law in Cyberspace. *Harvard International Law Journal*, 54, 1-12. Consul. da https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

periodo di tempo non è necessariamente un ostacolo alla formazione di una nuova norma internazionale di diritto consuetudinario[165].

2.3.1 Principi e norme di diritto internazionale applicabili nel *cyberspace*: il principio di sovranità territoriale

La Corte Internazionale di Giustizia (ICJ), chiamata a decidere relativamente al *"case concerning military and paramilitary activities in and against Nicaragua"*[166], ha constatato la presenza di una consuetudine in capo agli stati che impedisce agli stessi di intervenire negli affari interni o esterni degli altri stati, la quale risulta essere un corollario del principio di sovranità territoriale[167]. Il principio di sovranità territoriale sancisce espressamente che lo stato considerato conserva un'esclusiva e piena autorità all'interno del proprio territorio. La stessa Corte ha enfatizzato la necessità del rispetto del principio di sovranità territoriale, partendo dal presupposto che lo stesso assume un'importanza fondamentale nelle relazioni internazionali[168]. Il diritto ad un'esclusiva e piena autorità all'interno del proprio territorio garantisce, allo stato che fa leva sul principio, quattro macro-tipologie di diritti che assumono particolare rilevanza e che circondano il principio stesso: il principio di giurisdizione territoriale, di non intervento, di controllo sui propri confini ed infine il diritto di utilizzare le proprie risorse[169]. Il tema della giurisdizione territoriale, contraddistinto dalla possibilità di legiferare, sancisce altresì il diritto di far rispettare, anche e soprattutto in maniera coercitiva, quanto normativamente previsto relativamente all'attività di quei soggetti che si trovano

[165] Roscini, *op. cit.*, p. 6.

[166] International Court of Justice (ICJ). (1984, 26 novembre). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984.* (Vedi p. 392). Consultato da https://www.icj-cij.org/en/case/70/judgments

[167] Mandrioli, *op. cit.*, p. 32.

[168] International Court of Justice (ICJ). (1949, 9 aprile). *Corfu Channel (U.K. v. Alb.). Judgment of 9 April 1949*, 6, 35. Consultato da https://www.icj-cij.org/en/case/1

[169] Stilz, A. (2019). *Territorial sovereignty: A philosophical exploration*. Oxford University Press.

geograficamente e fisicamente sul territorio che si trova sotto la giurisdizione dello stato medesimo. Il principio di non intervento si esplica nell'esclusività del diritto di governare e regolare le attività dei soggetti sopra considerati, senza l'interferenza di alcuno stato estero, di individui o ancora di gruppi. Il terzo principio stabilisce la possibilità di regolare e controllare i movimenti di persone e beni che avvengono tramite i confini del territorio stesso, principio subordinato molto spesso a limitazioni provenienti dal diritto internazionale regionale, come avviene in caso dell'Unione Europea. Il quarto ed ultimo principio si articola alla stregua di un esempio concreto: ciascuno stato ha il diritto di regolare autonomamente l'utilizzo e l'estrazione di minerali, petrolio e altre risorse naturali che si collocano geograficamente all'interno del territorio considerato. Tuttavia, accanto ai quattro diritti che vengono riconosciuti, sugli stati gravano pure una serie di obblighi come, per esempio, l'obbligo di proteggere all'interno del proprio territorio i diritti riconosciuti agli altri stati, il diritto di integrità ed inviolabilità in tempo di pace e di guerra, o altresì la tutela di quei diritti che stati esteri avanzano sulla base della presenza di propri nazionali all'interno del territorio stesso[170].

Una specifica rilevanza su questo tema viene assunta, invece, nel momento in cui viene preso in considerazione l'elemento del *cyberspace.* Sulla base, infatti, delle definizioni dello stesso precedentemente considerate, il *cyberspace* viene definito il quinto dominio, sulla base delle caratteristiche di ubiquità e anonimato[171]. Il punto principale che qui rileva è che potrebbe sembrare che il mondo cibernetico sia totalmente esente dall'applicazione del principio di sovranità territoriale, mancando uno spazio "esclusivo" in cui gli stati possano esercitare la loro giurisdizione. Quest'ultima, difatti, è una delle due teorie che rileva in tema di

[170] Heintschel von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. *International Law Studies, 89*(1), 17.

[171] Herrera, G. L. (2006). Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In M. D. Cavelty, & V. Mauer (Cur.), *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace* (Cap. 4).

sovranità territoriale e *cyberspace*[172]: la prima, di conseguenza, vede una totale impossibilità di ritenere il cyberspace immune dalla sovranità statale, la seconda invece vede il *cyberspace* come uno spazio regolato nella stessa maniera di quanto avviene per il mare aperto, per lo spazio aereo internazionale o comunque sia uno spazio che viene identificato come una *res communis omnium.*

Per quanto riguarda la prima teoria, è possibile annoverare cinque elementi chiave che sintetizzano l'obbligo di ritenere corretta l'interpretazione relativa all'applicazione del principio di sovranità statale anche nel *cyberspace*[173]. Il primo elemento da analizzare è la fondamentale esistenza di un'entità in grado di controllare le attività che vengono svolte all'interno di questo spazio, necessaria inoltre per garantire la vita e la prosecuzione dello stesso. Infatti, quest'ultimo ha bisogno di una struttura fisica, dal momento che, senza la stessa, verrebbe impedito l'accesso agli utenti. Essendo questa una struttura materiale, inevitabilmente si troverà dentro il territorio di uno stato e di conseguenza dovrà sottostare, in parte, alla sovranità dello stesso come antecedentemente analizzato. Il secondo punto è che le relazioni economiche nel *cyberspace* necessitano obbligatoriamente di leggi che governino le transazioni e le parti stesse[174]. Se, come nella teoria suddetta, il mondo cibernetico fosse immune dalla giurisdizione territoriale, mancando leggi atte a disciplinare le varie relazioni economiche, le transazioni sarebbero circondate da un ampio grado di incertezza e comporterebbero pericoli per entrambe le parti. Il terzo motivo per il quale il *cyberspace* rientra, almeno in parte, all'interno delle competenze derivanti dalla sovranità statale è che il contenuto concretamente inviato tramite il sistema di rete produce effetti nel "mondo reale". Se infatti, da un lato, il cyberspazio idealmente permette il libero flusso di informazioni, dall'altro non vi è alcuna esenzione in grado di proteggere le stesse informazioni da validi interessi dello

[172] Franzese, P. W. (2009). Sovereignty in cyberspace: Can it exist? *Air Force Law Review, 64(1),* 1-42.

[173] *Ibid*.

[174] O'Sullivan, M., Goldsmith, J., & Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. *NUCB journal of language culture and communication*, *8*(1), 143-144.

stato dove queste informazioni sono inviate, ricevute ed immagazzinate. Il quarto motivo riguarda il fatto che gli stati sono sempre più portati ad affermare la propria presenza, giorno dopo giorno, nel *cyberspace* poiché lo stesso ha cominciato ad assumere una rilevanza specifica in tema di sicurezza nazionale. Avendo, come già analizzato, digitalizzato la maggior parte delle infrastrutture pubbliche che hanno particolare rilevanza per il funzionamento e per il benessere della collettività dello stato stesso, la paura e la possibilità concreta di subire danni ha portato i vari stati ad un impellente tentativo di controllo sul mondo digitale ai fini di proteggere eventuali vulnerabilità. Il quinto ed ultimo punto, invece, si articola sulla base di due visioni distinte del mondo cibernetico: mentre da una parte l'evoluzione tecnologica può comportare un assoluto miglioramento nella vita degli individui, dall'altra parte la volontà potrebbe essere quella di creare caos, sfruttare individui con competenze tecnologiche inferiori per ottenere illegittimamente un vantaggio su un concorrente o ancora per diffondere messaggi di odio o violenza. Per tutti questi motivi, a fini regolatori, sanzionatori e di controllo, al giorno d'oggi non è possibile ammettere un'esclusione totale del principio di sovranità territoriale nel mondo cibernetico[175].

La seconda teoria, invece, vede il cyber spazio alla stregua dei vari beni comuni globali[176]. Per spiegare questa teoria occorre partire da uno studio preliminare del termine "*global commons*". Non essendo stata fornita una definizione univoca ed unitaria, quello che può essere asserito è che questi beni si contraddistinguono per cinque caratteristiche che saranno di seguito analizzate[177]. La prima caratteristica è che, per essere definito tale, un *global common* deve essere circoscritto, regolato e tutelato da un trattato internazionale. La seconda peculiarità è che il trattato considerato deve prevedere i metodi di utilizzo e d'uso, nonché le varie proibizioni che riguardano il bene considerato. Per terzo, i

[175] Franzese, *op. cit.*, p. 66. (Vedi pp. 11-14).

[176] *Ibid*., (pp.14-15).

[177] *Ibid.*, (p. 16).

global commons sono contraddistinti da confini e limiti geografici predeterminati o, in ogni caso, facilmente identificabili. Come quarto punto, tutti gli stati devono, espressamente o tacitamente, aver rinunciato a qualsiasi rivendicazione esclusiva su ogni porzione del bene comune globale. La quinta ed ultima caratteristica si materializza nell'incapacità assoluta, da parte di un qualsiasi stato, di effettuare un controllo sulle zone considerate. Per concludere dunque, un bene comune globale non viene visto come un bene su cui manca una singola sovranità statale, quanto come un bene su cui grava una sovranità statale condivisa[178]. Di conseguenza, categorizzare il *cyberspace* all'interno del mondo dei *global commons*, con relativa applicabilità normativa in materia, risulta non corretto poiché i cinque requisiti analizzati non vengono rispettati.

In aggiunta a ciò, per chiarire ogni dubbio, il Manuale di Tallinn 2.0 redatto nel 2017, ha constatato, come prima regola, che anche nel mondo del *cyberspace* dovrebbe essere applicato il principio di sovranità[179]. Agli stati viene infatti riconosciuta la possibilità di godere del principio di sovranità sulle strutture in cui vengono svolte attività cibernetiche all'interno del proprio territorio. Il gruppo internazionale di esperti ha riconosciuto, tuttavia, l'impossibilità per ciascuno stato di invocare una sovranità *per sé* nel cyberspazio. La caratteristica più importante, riportata esplicitamente alle regole 2 e 3, attiene alla distinzione intercorrente tra sovranità interna ed esterna.

La *Rule 2*, relativa alla sovranità interna, afferma che: «*a State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations*». La sovranità dello stato su infrastrutture e attività informatiche si può rinvenire alla stregua di due conseguenze giuridiche internazionali. In primo luogo, le infrastrutture sono soggette alla legislazione nazionale e ad un controllo regolamentare da parte dello stato; difatti, quest'ultimo ha la possibilità di far

[178] *Ibid.*, (p. 17).

[179] Schmitt, *op. cit.*, p. 64.

rispettare le leggi e i regolamenti nazionali che li riguardano. In secondo luogo, la sovranità dello stato sul territorio conferisce un obbligo per lo stato stesso di proteggere le infrastrutture informatiche e le attività che ivi vengono svolte[180]. Di conseguenza, ciascuno stato può regolare le *cyber activities* che vengono svolte all'interno del proprio territorio; ha dunque la possibilità di criminalizzare varie attività come quelle che comportano il caricamento di materiali pornografici, o di materiali che incitano alla violenza, censura che deve essere effettuata sempre e comunque proteggendo i diritti umani tutelati negli ambiti suddetti. Inoltre, il diritto consuetudinario internazionale e i trattati stessi hanno la possibilità di limitare i diritti di ciascuno stato in materia di sovranità nazionale.

La regola numero tre, che riguarda il tema della sovranità esterna, si esplica nel seguente modo: «a *State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it*». Questo principio sancisce espressamente che ciascuno stato è indipendente nelle relazioni esterne con altri stati, potendo inoltre condurre attività cibernetiche oltre il proprio territorio, attività che in ogni caso non possono violare nessuna normativa internazionale. Inoltre, come stabilito dalla regola n.4 del Manuale, non vi è la possibilità di condurre attività cibernetiche che siano in grado di violare la sovranità di altri stati[181]. Tutte quelle tipologie di attività cibernetiche che precludono il legittimo esercizio della sovranità di uno stato nel proprio territorio sono da considerare illegittime e per questo motivo come una violazione del diritto internazionale. Il gruppo internazionale di esperti ha inoltre ritenuto che quanto appena descritto sia applicabile solo agli stati e tra gli stessi, non applicandosi di conseguenza nei confronti di attori non statali, a meno che le azioni condotte da questi ultimi non siano riconducibili ad indicazioni dello stato stesso. Avendo il gruppo stabilito che una violazione fisica del principio di sovranità avviene quando uno o più soggetti di uno stato materialmente entrano

[180] Jensen, E. (2017). The Tallinn manual 2.0: Highlights and insights. *Georgetown Journal of International Law*, 48(3), 735-778.

[181] Schmitt, *op. cit.*, p. 64.

all'interno del territorio o dello spazio aereo di un altro senza consenso o qualche altra giustificazione, da un punto di vista cibernetico la violazione del principio di sovranità si verifica nel momento in cui un organo di uno stato o direttamente i soggetti inviati dallo stato si trovano nel territorio straniero conducono operazioni cibernetiche dentro lo stato suddetto. Un esempio che può essere riportato è il caso in cui un agente inviato dallo stato A utilizza una chiavetta *usb* per introdurre un *trojan horse* all'interno di un sistema informatico dello stato B mentre si trova fisicamente nel territorio di quest'ultimo.

2.4 Tallinn Manual (2013) e Tallinn Manual 2.0 (2017)

Sulla scorta di quanto affermato nel paragrafo precedente, è necessario sia fornire una visione generale del processo che ha portato alla redazione dei due manuali più importanti redatti in tema di *cyber activities* sia soprattutto delineare la valenza che, da un punto di vista internazionale, possiedono gli stessi. Nel 2009 la *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*[182] ha messo insieme un gruppo internazionale di esperti con il compito fondamentale di individuare ed esaminare la normativa internazionale in tema di regolazione delle attività cibernetiche[183]. Il gruppo era composto in tutto da 20 studiosi e luminari del diritto internazionale di vari paesi, nonché dagli alti ufficiali militari responsabili della consulenza legale sulle operazioni informatiche. Tre organizzazioni internazionali hanno inoltre fornito osservatori al processo di formazione tra cui: il comitato internazionale della Croce Rossa, la *NATO's Allied Command Transformation*[184] ed infine il Comando Cibernetico degli Stati

[182] The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Official Website*. Consultato da https://ccdcoe.org/

[183] Liivoja, R., & McCormack, T. (2014). Law in the Virtual Battlespace: The Tallinn Manual and the *Jus in Bello*. In: Gill T., Geiß R., Heinsch R., McCormack T., Paulussen C., & Dorsey J. (Cur.), *Yearbook of International Humanitarian Law Volume 15* (2012). T.M.C. Asser Press, The Hague. Consultato da https://doi.org/10.1007/978-90-6704-924-5_3

[184] NATO. Supreme Allied Commander Transformation (NATO's ACT). (n.d.). *Official site.* Consultato da https://www.act.nato.int/

Uniti[185]. Il processo di formazione comportò tre anni e mezzo di lavoro, portando nel 2013 alla pubblicazione del "*Tallinn Manual on the International Law Applicable to Cyber Warfare".* La linfa vitale del manuale qui considerato comprendeva, senza dubbio, la regolazione delle attività cibernetiche che assumevano il rango di uso della forza e di quelle che venivano assunte in un conflitto armato[186]. A distanza di poco tempo, tuttavia, partendo dal presupposto che la redazione del manuale non era stata osservata ed effettuata da studiosi provenienti da ogni stato ma solo da alcuni, il CCDCOE ha deciso di lanciare una nuova iniziativa volta ad ampliare il campo di applicazione del manuale, col fine di includere al suo interno anche il diritto internazionale pubblico che invece disciplina le operazioni informatiche in tempo di pace. Per questo motivo venne creato un nuovo gruppo di esperti di diritto internazionale, con particolare specializzazione di coloro in possesso di maggiori competenze in tema di attività informatiche nel periodo considerato. Nel 2017 di conseguenza venne adottato il *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* il quale ha inglobato il primo, modificandone gli aspetti ritenuti rilevanti.

Il punto cardine da sottolineare quando parliamo dei suddetti Manuali attiene alla valenza che, da un punto di vista normativo, possiedono. La natura dei manuali, nonché le modalità con cui si è concretamente realizzato il processo di formazione, porta ad annoverare gli stessi come il prodotto ottenuto da due semplici tentativi di individuazione della normativa esistente, eseguiti da un gruppo di esperti indipendenti. Infatti, la visione espressa nel Manuale non coincide con la visione ufficiale del CCDCOE, della NATO stessa e degli stati membri. Quindi la vincolatività del manuale in sé e per sé non risulta in nessun modo, ma deve essere concepito esclusivamente come il tentativo di raccolta della normativa esistente da un punto di vista internazionale in tema di *cyber operations* e come un insieme di opinioni fornite e messe per iscritto dal gruppo

[185] U.S. CYBER COMMAND. (n.d.). *Official site.* Consultato da https://www.cybercom.mil/

[186] Schmitt, *op. cit.*, p. 64.

internazionale di esperti[187]. Le regole e i commenti che esplicitamente costituiscono il manuale possono essere suddivisi in due macro-temi: lo *jus ad bellum* e lo *jus in bello.* Il manuale inoltre non è comprensivo di tutte le normative in tema di *cyber operations*: manca infatti qualsiasi riferimento al diritto penale internazionale, al diritto internazionale commerciale oppure alla proprietà intellettuale. Le "*Rules*" del manuale sono state rilevate basandosi sul principio del consenso tra gli esperti; i commenti che vengono eseguiti sulle stesse riguardano l'interpretazione, la spiegazione dei contenuti normativi, fornendo inoltre le differenti visioni che alle stesse possono essere date. Quando infatti sono presenti due visioni distinte esposte dal gruppo di esperti, entrambe vengono riportate, analizzando all'interno dei commenti i motivi sui quali il gruppo era diviso e anche le teorie singole. Quello che invece deve essere sottolineato è l'importanza dei manuali internazionali: in mancanza di un trattato internazionale che regola la materia presa in considerazione, il manuale si limita a registrare quella che, secondo il parere non vincolante degli esperti, è l'eventuale consuetudine applicabile nella fattispecie concreta[188].

L'elaborato seguente si focalizza sul tema dell'uso della forza e dell'equiparazione delle attività cibernetiche alle attività che raggiungono quell'intensità. Sulla base di ciò, come verrà analizzato meglio nel capitolo relativo allo studio delle varie organizzazioni internazionali, la proibizione fornita dall'art.2 e 51 della Carta delle Nazioni Unite trova fondamento anche nel caso di attività cibernetiche come esplicitamente sottolineato dalla rule 68, la quale sancisce che: «*a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful*». Il divieto dell'uso della forza e i principi che sottostanno alla legittima difesa in determinati casi propri del mondo cibernetico si esplicano partendo dal

[187] Schmitt, *op. cit.,* p. 64.

[188] Liivoja, *op. cit.,* p. 71.

parere consultivo sulla *Legalità della minaccia e uso delle armi nucleari*, in cui viene chiaramente spiegato che qualsiasi tipologia di arma in grado di assurgere a detto grado sarà considerata come proibita[189]. Da qui la possibilità di far rientrare nelle definizioni fornite dagli articoli appena nominati le attività cibernetiche.

Un ultimo elemento del Manuale di Tallinn 2.0 che merita particolare attenzione è il tema della *due diligence*. Quest'ultimo risulta strettamente correlato al tema della responsabilità statale (tema che verrà meglio analizzato nel quarto capitolo e di cui in questa sezione si vuole solo dare una visione generale), dal momento che dal mancano rispetto degli obblighi di *due diligence* potrebbe sorgere una responsabilità internazionale; sugli stati sembrerebbe gravare infatti un'obbligazione tale da imporre agli stessi di utilizzare una normale diligenza al fine di evitare che attività illegittime vengano compiute all'interno del proprio territorio[190]. Il Manuale di Tallinn parla di *due diligence* relativamente alle attività cibernetiche statuendo alla *Rule* 6 che:

> *«A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States».*

Partendo da una visione di sovranità, gli esperti del gruppo sono concordi a ritenere che il principio di due diligence valga anche in relazione alle attività cibernetiche, come espresso dallo stesso gruppo nel report del 2013[191]. La regola considerata presuppone il coinvolgimento di tre parti: lo stato che subisce l'operazione informatica, lo stato territoriale che è soggetto della regola ed infine l'autore della *cyber operation*. In aggiunta, si applica allo stesso modo a parti

[189] International Court of Justice (ICJ). (n.d.). *Legality of the Threat or Use of Nuclear Weapons*. Consultato da https://www.icj-cij.org/en/case/95

[190] Barnidge, R. (2006). The Due Diligence Principle Under International Law. *International Community Law Review, 8*(1), 81-121. doi: https://doi.org/10.1163/187197306779173194

[191] United Nations General Assembly. GGE. (2013). *Report A/68/98*: para. 20.

terze eventualmente presenti nel processo, indipendentemente dal fatto che siano persone private, società o stati.

2.5. Il ruolo delle dichiarazioni statali relative al diritto internazionale applicabile al *cyberspace*

Come rilevato precedentemente, non essendo presente un trattato uniforme o deliberazioni comuni che prevedono l'applicazione del diritto internazionale nel *cyberspace*, è necessario analizzare le dichiarazioni di alcuni stati che hanno confermato suddetta applicabilità.

Dichiarazioni statali che hanno assunto una particolare rilevanza in questi termini sono riportate dalla Francia, la quale il 9 settembre 2019 ha adottato il documento intitolato *"Droit International appliqué aux opérations dans lecyberspace"*[192]. Questo documento rappresenta la posizione francese in tema di applicabilità della normativa internazionale nel *cyber* spazio e risulta essenzialmente suddivisa in due parti distinte: la prima si concentra sulle operazioni cibernetiche che vengono svolte contro la Francia in tempo di pace, mentre la seconda si focalizza sull'applicabilità delle norme di diritto internazionale nel *cyber* spazio in tempo di guerra[193]. La parte iniziale del documento riprende i lavori svolti dal "*Group of Governamental experts*" (GGE), il gruppo di esperti istituito in seguito alla risoluzione 73/266[194] dell'Assemblea Generale dell'ONU, con il compito di promuovere la realizzazione di comportamenti responsabili dei vari stati nel contesto della tutela della sicurezza

[192] Ministère Des Armes. (2019, 9 settembre). *Droit International Appliqué Aux Opérations Dans Le Cyberespace*. Consultato da https://www.google.com/search?client=firefox-b-d&q=Droit+International+appliqu%C3%A9+aux+op%C3%A9rations+dans+lecyberspace

[193] *Ibid.*

[194] United Nations General Assembly. (2019, 2 gennaio). *A/RES/73/266 Resolution adopted by the General Assembly on 22 December 2018: Advancing responsible State behaviour in cyberspace in the context of international security*. Consultato da https://undocs.org/A/RES/73/266

internazionale[195]. Il risultato più importante raggiunto dal gruppo preso in considerazione è stato quello di aver suggerito l'obbligo per gli stati, all'interno del *cyberspace*, di rispettare il diritto internazionale ed in particolare la Carta delle Nazioni Unite, andando a comprendere di conseguenza i principi che la contraddistinguono come l'obbligo di risoluzione pacifica delle controversie o l'astensione dal ricorso o dalla minaccia dell'uso della forza[196]. Partendo quindi da quanto appena affermato, la Francia si è esposta predisponendo che:

> *«Qualsiasi attacco informatico contro i sistemi digitali francesi o qualsiasi produzione di effetti sul territorio francese tramite mezzi digitali da parte di un organo statale, una persona o un'entità che esercita prerogative di poteri pubblici o da una persona o da persone che agiscono su istruzioni o direttive o sotto il controllo di uno Stato costituisce una violazione di sovranità»*[197].

La seconda parte invece si focalizza sul punto che vede l'applicazione del diritto internazionale umanitario alle azioni offensive nel dominio cibernetico. Per questo motivo tutte le condotte offensive cibernetiche devono essere effettuate rispettando i principi che disciplinano la condotta dei conflitti[198].

Oltre alla Francia, anche la Cina, seppur con alcune problematiche, è arrivata ad esprimere la necessità di vedere applicati al regime cibernetico i principi fondanti del diritto internazionale[199]. In particolare, il governo cinese è arrivato ad affermare che intende, a tal fine, lavorare insieme alla comunità internazionale per promuovere la costruzione di un cyberspazio pacifico, sicuro, disciplinato,

---

[195] United Nations Official site. (n.d.). *Group of Governmental Experts*. Consultato da https://www.un.org/disarmament/group-of-governmental-experts/

[196] Sarti, E. (2019, 1 ottobre). *La visione francese sul diritto internazionale nel cyberspace. Center for Cyber Security and International Relations Studies.* Consultato da https://www.cssii.unifi.it/upload/sub/Francia_DirInt_Cyberspace.pdf

[197] *Ibid.*

[198] *Ibid.*

[199] Hsu, K., & Murray, C. (2014). *China and international law in cyberspace*. US-China Economic and Security Review Commission.

aperto e cooperativo. Quello che tuttavia deve essere constatato è come la Cina abbia supportato con particolare forza e particolare vigore l'applicabilità del diritto internazionale nel *cyberspace*, con riferimento prevalentemente all'obbligo del rispetto del principio di sovranità e del principio di non intervento negli affari dei singoli stati[200]; la Cina infatti ritiene, come avviene nel mondo fisico, che sia necessario rispettare preliminarmente il principio di sovranità statale anche nel *cyberspace*[201]. Questo principio particolare è stato evidenziato tramite la spiegazione di due corollari importanti. Il primo di questi prevede che gli stati debbano essere in grado di affermare la propria sovranità nel cyberspazio, sia nei confronti dei propri cittadini sia nei confronti di organizzazioni straniere che operano nei propri confini; proprio su questo aspetto, la Cina si differenzia notevolmente dagli Stati Uniti, che prevedono, sulla carta, un regime altamente protettivo della libertà individuale e che vede gli sforzi eccessivi dello stato per controllare i contenuti *online* come "inappropriati"[202]. Il secondo, invece, è un'esplicazione del principio di non intervento, nel senso che prevede che gli stati dovrebbero astenersi dall'utilizzo di proprie risorse e di infrastrutture critiche per minare il diritto di altri paesi di esercitare la sovranità all'interno dei propri confini[203].

Un ulteriore stato che, recentemente, ha confermato, sulla base dei lavori effettuati dal già citato UN GGE report del 2013, l'applicabilità del diritto internazionale nel *cyberspace* è la Finlandia[204]. Sulla base di ciò, la Finlandia ha

---

[200] *Ibid.*

[201] Delegation to UN General Assembly (PRC). (2013, ottobre). *Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA*. (New York: United Nations).

[202] Painter, C. (2014, 4 marzo). *Remarks at Georgetown University Institute for Law Science and Global Security's 2014 International Engagement on Cyber Conference*. (Washington, DC). Consultato da http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm.

[203] Jian, S. (2014). An International Code of Conduct for Information Security: China's perspective on building a peaceful, secure, open and cooperative cyberspace'. In *Cyber Stability Seminar*.

[204] Finnish Government, Ministry of Foreign Affairs. (2020, 15 ottobre). *Finland published its positions on public international law in cyberspace*. Consultato da https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace

affermato come consideri il rispetto del diritto internazionale un quadro essenziale per un comportamento responsabile nel cyberspazio. Ammettendo la possibilità di avere l'applicazione delle norme e dei principi internazionali nel *cyberspace*, la Finlandia ha altresì evidenziato come, per rispettare alcune specifiche previsioni, sia necessario un incremento della cooperazione tra stati, favorita tramite un costante scambio di opinioni su particolari questioni che riguardano il modo in cui le stesse devono essere applicate[205]. In aggiunta a ciò, ha riportato, tramite commenti, una serie di questioni che sono state sollevate. Le questioni riguardano la necessità di una visione unitaria relativa all'applicabilità del principio di sovranità, del principio di non intervento, del danno tra stati, della responsabilità statale, del diritto internazionale umanitario ed infine del regime dei diritti umani. Da un punto di vista della responsabilità statale, tema che verrà approfondito dettagliatamente nel capitolo conclusivo dell'elaborato, la Finlandia ha rilevato come l'applicabilità del diritto internazionale in materia debba essere necessariamente approfondita ed ampliata, per permettere di delineare, con efficienza, le possibili contromisure che potrebbero essere adottate da uno stato da un punto di vista cibernetico. Essendo queste ultime assolutamente innovative, per poter applicare il regime di responsabilità statale, sarà necessario delineare con precisione quelle che possono essere adottate[206].

Anche l'Olanda ha reso pubblica la propria posizione dettagliata sull'applicabilità del diritto internazionale alle operazioni condotte nel *cyberspace*, delineata tramite una lettera del ministro degli Affari esteri dei Paesi Bassi diretta al presidente della camera dei rappresentanti[207]. Secondo la lettera, viene compreso il concetto di sovranità nel *cyberspace*, si includono inoltre le operazioni informatiche nel regime delle attività sottoposte alla proibizione della

[205] *Ibid.*

[206] *Ibid.*

[207] Government of Netherlands. (2019, 5 luglio). *Letter to the parliament on the international legal order in cyberspac*e. Consultato da https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

minaccia o dell'uso della forza; inoltre, viene esteso il principio di *due diligence* nel panorama informatico. Viene ribadito come il diritto umanitario internazionale e la disciplina della neutralità debbano essere applicati anche alle condotte informatiche durante i conflitti armati[208]. Accanto a ciò, anche le norme sui diritti umani vengono garantite, pur ammettendo, anche nel mondo cibernetico, la possibilità di limitazione di alcuni per garantire la tutela di diritti ritenuti più importanti. Infine, la lettera chiarisce la posizione dell'Olanda in merito alla tanto contestata autodifesa: la risposta, così come le contromisure informatiche e non, devono essere ammesse. L'eccezione della necessità si riverbera quando ci sono conseguenze che possono essere, potenzialmente, molto gravi in seguito ad attacchi cibernetici alle infrastrutture critiche[209].

Da un punto di vista degli Stati Uniti invece, come già rilevato antecedentemente nel capitolo, l'applicabilità delle norme internazionali nel *cyberspace* è stata sottolineata tramite un discorso particolare, tenuto da Harold Koh, consigliere legale dell'*US State Department*, nel 2012; la tesi fondamentale espressa da quest'ultimo prevedeva l'erroneità della concezione del *cyberspace* come una "*law-free zone*"[210]. A distanza di quattro anni, il nuovo consigliere legale dell'*US State Department*, Brian Egan, ha tenuto un importante discorso alla *Berkeley law school*, relativamente al rapporto tra il diritto internazionale e operazioni cibernetiche[211]. In particolare, è stato sottolineato come gli esistenti principi di diritto internazionale vadano a formare la pietra miliare dello "S*trategic Framework of International Cyber Stability during peacetime and during armed conflict*"[212] americano. Vengono individuati inoltre tre pilastri, ognuno dei quali in grado di contribuire notevolmente alla sicurezza cibernetica. Il primo prevede

[208] *Ibid*

[209] *Ibid.*

[210] Hongju, *op. cit*., p. 64.

[211] Schmitt, M. (Cur.). (2016, 15 novembre). *US Transparency regarding International Law in Cyberspace.* Consultato da Just Security https://www.justsecurity.org/34465/transparency-international-law-cyberspace/

[212] Egan, B. J. (2017). International Law and Stability in Cybershpace. *Berkeley J. Int'l L., 35*, 169.

l'affermazione globale dell'applicabilità del diritto internazionale esistente nel *cyberspace*, sia in tempo di pace che durante i conflitti armati. Il secondo prevede lo sviluppo di un consenso internazionale su alcune norme aggiuntive volontarie e non vincolanti per un comportamento responsabile degli stati. Il terzo infine prevede lo sviluppo e l'attuazione di misure pratiche di rafforzamento della fiducia, che siano in grado di garanti un miglior livello di cooperazione per il mantenimento della pace e della sicurezza internazionale[213].

Quelli riportati fino ad ora sono solo alcuni degli innumerevoli esempi che potevano essere riportati in tema di dichiarazioni statali. Tuttavia, quello che importa il seguente elaborato è dimostrare come gli stati non possano esimersi da fornire proprie valutazioni su argomenti che stanno diventando sempre più impellenti.

2.6 Diritti umani e *cyberspace*

Lo sviluppo e l'evoluzione costante della tecnologia, coadiuvato dalla creazione di Internet, ha portato ad una valutazione ulteriore del mondo virtuale. Internet è diventato uno strumento essenziale per raggiungere gli obiettivi che chiunque si propone e, attualmente, anche i tradizionalisti più solidi sono portati a scontrarsi con questo mondo per ottenere determinati vantaggi. Il punto focale che interessa il seguente elaborato si contraddistingue per l'equiparazione dei due mondi, mondo "*online"* e mondo "*offline*"[214], sul tema dei diritti umani. Questi diritti sono senza dubbio garantiti da un punto di vista internazionale a chiunque, indipendentemente dal luogo di nascita o dai limiti territoriali che molto spesso impediscono l'applicazione della generalità delle normative. Essendo oggi riconosciuti da un punto di vista materiale, gli studiosi si sono più volte chiesti se

[213] *Ibid.*

[214] Dobrzeniecki, K. (2005). How should we deal with human rights in cyberspace? Some remarks. *International Review of Law, Computers & Technology*, 19:3, 253-258 Consultato da https://doi.org/10.1080/13600860500348036

gli stessi siano da considerare tutelabili anche all'interno di un mondo privo (almeno apparentemente) di materialità e contraddistinto da una vera e propria mancanza di delimitazione[215]. In altri termini, ci si è chiesti quali diritti e quali limitazioni possano essere ammessi nel cyberspazio e come gli stessi, che per natura storicamente sono stati solitamente ammessi in altri ambiti, siano riconosciuti dentro questo mondo innovativo.

La maggior parte degli esperti dei diritti umani sono concordi nel ritenere che queste tipologie di diritti derivino dalla dignità intrinseca della persona umana; ogni persona possiede questi diritti per il semplice fatto di essere umano, alla stregua di presupposti di diritto naturale[216]. Di conseguenza, sulla base di questo approccio, la legge non crea ma semplicemente riconosce i diritti stessi ed è questa la posizione dominante nei trattati relativamente ai diritti umani, nonché all'interno della dottrina. Inoltre, in una dottrina consolidata, questi diritti vengono definiti come possibilità dell'essere umano, possibilità che sono naturali, indispensabili, eguali, inalienabili ed universali[217]. Tuttavia, le tesi che fanno leva sul diritto naturale come legittimazione e fondamento giuridico della tutela internazionale dei diritti umani non sono prive di contraddizioni, derivanti prevalentemente dal fatto che possiedono un fondamento debole e che prevede il ricollegamento a nozioni e concetti particolarmente vaghi[218]. Altre tesi inoltre sono state fornite, come quella relative al consenso, che si basa sulla concezione adottata da una collettività di soggetti che ritiene, in un determinato momento storico, di dover riconoscere una serie di diritti umani[219]. Tuttavia, quello che è possibile asserire in tema di legittimazione dei diritti umani fa riferimento da un lato alla necessità di avere regole giuridiche ed un sistema di protezione

[215] *Ibid.*

[216] Pustorino, P. (2019). *Lezioni di tutela internazionale dei diritti umani* (pp. 1-232). Cacucci Editore.

[217] Mik, C., & Człowieka, Z. P. (1992). *Collective Human Rights*. Wydawnictwo UMK, Torun. (Vedi p. 7).

[218] Pustorino, *op. cit*., p. 81.

[219] *Ibid.*

adeguato, in grado di tutelare i diritti stessi, e dall'altro ad un richiamo al diritto naturale, il quale può servire ad implementare la protezione dei diritti umani considerati nonché a stimolare l'attività del legislatore[220].

Anche se il gruppo internazionale di esperti ha riscontrato come sia i trattati che il diritto consuetudinario in materia dei diritti umani dovrebbero essere applicati anche nel caso di attività cibernetiche, ha altresì avvertito l'esigenza di sottolineare come siano presenti una serie di diritti umani, previsti dai trattati, la cui cristallizzazione nel diritto consuetudinario risulta dubbia; detti dubbi sorgono soprattutto alla stregua di una mancata uniformità di definizione relativa alle diverse attività cibernetiche, mancanza che presuppone una differente interpretazione da parte degli stati o degli enti regionali. Inoltre, tramite la *rule* 37, come verrà spiegato a fine paragrafo, il gruppo ha osservato che gli stati hanno la possibilità di limitare l'esercizio, subordinato a determinate circostanze, e il godimento di alcuni diritti in conformità al diritto internazionale sul tema dei diritti umani[221].

Lo studio fino a qui effettuato vede, all'art.30, la definizione concreta di *cyber attack,* il quale prevede determinate tipologie di danni che vanno a riverberarsi non solo ed unicamente nei confronti dello stato cui è rivolto l'attacco cibernetici ma anche e soprattutto contro gli stessi individui [222]. In particolare, analizzare quali e quanti diritti umani vengono concretamente riconosciuti nel *cyberspace* permette di districarsi più agevolmente nello studio dei danni causati da un *cyber attack* e nella classificazione dello stesso come tale[223]. Come riportato all'interno dell'elaborato relativamente al *cyber attack* effettuato nel maggio 2017, corrispondente al caso *Wannacry* (ad oggi riconosciuto come il maggiore attacco

[220] *Ibid.,* (p. 11).

[221] Schmitt, *op. cit.,* p. 64. Art 37: «*The obligations to respect and protect international human rights, with the exception of absolute rights, remain subject to certain limitations that are necessary to achieve a legitimate purpose, nondiscriminatory, and authorized by law*».

[222] Schmitt, *op. cit*., p. 19. (Vedi p. 257).

[223] Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2014, July). A cyber attack evaluation methodology. In *Proc. of the 13th European Conference on Cyber Warfare and Security.*

cibernetico mai avvenuto[224]), gli attacchi cibernetici hanno la possibilità di colpire una serie di diritti umani dei cittadini che sono, da un punto di vista internazionale, riconosciuti[225]; accanto infatti al "semplice" diritto alla vita, ricollegabile agli attacchi cibernetici nel momento in cui gli stessi possono comportare la morte dei soggetti, se ne aggiungono molti altri. Tra questi, un esempio pratico può essere visto da corollari del diritto alla vita stesso come il diritto alla salute o il diritto ottenere i servizi sanitari essenziali[226] ; sotto quest'ultimo punto di vista, il cyber attacco all'interno del caso *Wannacry* non ha solo ed unicamente causato violazioni dei diritti umani da un punto di vista economico, andando a danneggiare economicamente una serie innumerevole di imprese degli stati in cui lo stesso si è diffuso, ma ha avuto anche la forza di causare danni comprendenti violazioni più ampie dei diritti umani[227]. Infatti, l'attacco considerato ha portato ad una serie gravissima di conseguenze al sistema di funzionamento sanitario del Regno Unite[228]; nel discorso tenuto dal presidente dell'ufficio legale della *Microsoft*, Brad Smith, è stato evidenziato come l'attacco abbia forzato il servizio sanitario nazionale inglese a deviare ambulanze o a cancellare più di 19000 appuntamenti per visite mediche o per ottenere un intervento chirurgico[229].

Le infrastrutture che permettono una condivisione di informazioni di massa, oltre alla possibilità in millesimi di secondo di esprimere la propria opinione attraverso il mondo cibernetico, hanno causato cambiamenti fondamentali nella vita di chiunque. Questa interazione sempre più invasiva, variegata e continuamente in evoluzione ha portato a rapportarsi con quesiti legali ed etici, soprattutto per

[224] Chen, Q., & Bridges, R. A. (2017, December). Automated behavioral analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 454-460). IEEE.

[225] Mandrioli, *op. cit*., p. 32

[226] Pustorino, *op. cit*., p. 81. (Vedi p. 109).

[227] Mandrioli, *op. cit*., p. 32.

[228] Brandom, R. (2017). UK hospitals hit with massive ransomware attack. *The Verge*, *12*.

[229] *Ibid.*

quanto riguarda la protezione e la promozione dell'importantissimo diritto di espressione. Le innovazioni tecnologiche hanno portato a cambiamenti e notevoli opportunità per le modalità di ottenimento e lo scambio di informazioni. Una delle sfide più interessanti al giorno d'oggi è quella di fornire un'interpretazione legittima da un punto di vista legale della libertà di pensiero e d'espressione nel *cyberspace*[230]. L'assemblea generale delle Nazioni Unite e degli stati e il *UN human Rights Council* hanno più volte ribadito la necessità di una tutela dei diritti umani nel *cyberspace* identica a quella fornita nel mondo reale[231]. Per questo non ci sono motivi per ritenere che la protezione dei diritti umani dovrebbe essere limitata nel cyber spazio. Nel momento in cui da un punto di vista internazionale sono stati riconosciuti i vari diritti umani, è stato esplicitato che questi principi si sarebbero estesi a tutti i media, indipendentemente dai progressi tecnologici. Altresì, la Dichiarazione Universale dei Diritti Umani sancisce all'art.19 che chiunque ha il diritto alla libertà d'espressione e di opinione. Questo diritto inoltre include la facoltà di esprimersi senza interferenze e di cercare, ricevere e trasmettere opinioni tramite qualsiasi mezzo ed indipendentemente dalle frontiere[232]. Gli stati sono obbligati a rispettare i diritti umani sulla rete, non possono violare quelli che un soggetto sta esercitando all'interno del cyberspazio e non possono servirsi di quest'ultimo come uno strumento con cui violare i diritti degli individui. Le leggi sui diritti umani richiedono che gli stati rispettino, proteggano e garantiscano gli stessi[233]; alle varie nazioni viene inoltre richiesto di adottare tutte le misure appropriate

[230] Lucchi, N. (2014). Internet content governance and human rights. *Vanderbilt Journal of Entertainment and Technology Law*, 16(4), 809-856.

[231] United Nations General Assembly. (2012, 29 giugno). *Doc. A/HRC/20/L.13: The promotion, protection and enjoyment of human rights on the Internet.* Consultato da https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

[232] United Nations. (n.d.). *The Universal Declaration of Human Rights*. Consultato da https://www.un.org/en/universal-declaration-human-rights/ Art. 19: «*Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers*».

[233] United Nations Human Rights Committee (HRC). (2004, 26 maggio). *General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13.* Consultato da https://www.refworld.org/docid/478b26ae2.html

(educative, giudiziarie, ed amministrative) volte a adempiere gli obblighi imposti[234], includendo la protezione dei diritti individuali nei confronti di arbitrarie interferenze legislative poste in essere da eventuali terze parti.

Come rilevato da David Kay, osservatore speciale delle Nazioni Unite con compiti di sorveglianza sulla promozione e protezione del diritto di libertà di opinione ed espressione da agosto 2014 a luglio 2020[235], il mondo cibernetico garantisce una capacità mai vista prima d'ora agli stati di interferire ed interagire illegittimamente coi vari diritti umani riconosciuti[236]. Gli individui di tutto il mondo, consci dell'esistente censura *online,* della sorveglianza di massa mirata alla raccolta di dati per una necessaria tutela della sicurezza, dei continui attacchi alla società che avvengono online e delle restrizioni che derivano in seguito all'utilizzo di espressioni "pericolose" nel web, sono obbligati a cercare in ogni momento una maggiore sicurezza per diffondere le proprie opinioni senza interferenze di nessun tipo. Detta ricerca avviene tramite gli strumenti della crittografia, dello "*scrambling*"[237] di dati per fare in modo che solo e unicamente i destinatari abbiano la possibilità di accedervi e di visionare il contenuto; altri ancora cercano un rispetto del loro diritto alla *privacy* nell'anonimato, utilizzando tecnologie sofisticate ed avanzate per riuscire a mascherare la propria identità e la propria impronta digitale. Crittografia ed anonimato sono dunque i principali veicoli per la sicurezza online e per permettere agli individui di leggere, navigare, sviluppare e condividere opinioni nel rispetto della loro privacy e dei loro diritti di libertà ed espressione.

---

[234] United Nations Human Rights Committee (HRC). General comment, supra note 9, 7: *Art. 2 requires that States Parties adopt legislative, judicial, administrative, educative and other appropriate measures in order to fulfill their legal obligations.").*

[235] OHCHR. (n.d.). *Mr. David Kay, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Consultato da https://www.ohchr.org/en/issues/freedomopinion/pages/davidkaye.aspx

[236] Human Rights Council. (2015, 22 maggio). *U.N. Doc. A/HRC/29/3*: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye.*

[237] Treccani. (2020). *Scrambling.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «Sistema crittografico, tecnica di alterazione del contenuto digitale, reso fruibile solo da chi è in possesso della chiave di decrittazione necessaria […]».
Consultato da https://www.treccani.it/vocabolario/scrambling_%28Neologismi%29/

Esistono una serie di diritti umani, accanto a quello relativo alla libertà di espressione che verrà analizzato nello specifico alla fine del paragrafo, che hanno assunto una dimensione particolarmente importante nello spazio cibernetico e che si sono contraddistinti per un'interpretazione totalmente differente da quella che originariamente veniva loro data: il diritto alla *privacy*, il diritto alla protezione dei dati personali ed il diritto all'oblio. Il diritto alla *privacy*[238] e alla libertà di espressione[239] sono oggi riconosciuti e codificati in strumenti regionali ed universali in materia di diritti dell'uomo, interpretati di conseguenza dagli organi dei trattati e dai sistemi di corti regionali, interpretazioni valutate a loro volta dal consiglio per i diritti umani tramite revisioni periodiche annuali e universali. Gli *standard* universalmente riconosciuti relativamente a *privacy* e libertà di espressione sono contenuti nel "*Covenant on Civil e Political Rights" (ICCPR)*, adottano nel 1966 ed entrato in vigore il 23 marzo 1976, che è stato ratificato da 168 stati. Per quei pochi stati che hanno deciso di non adottarlo, il patto presenta uno standard minimo che deve essere comunque garantito e che spesso si riverbera in un vincolo consuetudinario. Per quanto riguarda il diritto alla privacy, l'art.8 della *European Convention of Human Rights* sancisce che:

"1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria 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 del paese, alla difesa dell'ordine e alla

[238] *Diritto alla privacy* contenuto in: Articolo 12 della Dichiarazione Universale dei diritti dell'uomo (UCHR), Art.17 della Convenzione su diritti civili e politici (ICCPR), Articolo 16 della Convenzione sui diritti dei bambini (CRC), Art.22 della Convenzione sui diritti delle persone affetti da disabilità (CRPD), Art.14 della Convenzione sulla protezione dei diritti dei migranti lavoratori e dei membri delle loro famiglie (CRMW), art.8 della Convenzione Europea dei diritti umani (ECHR), art.11 della Convenzione americana dei diritti dell'uomo (ACHR).

[239] *Diritto di espressione* contenuto in: Articolo 19 della Dichiarazione Universale dei diritti dell'uomo (UCHR) e della Convenzione internazionale sui diritti civili e politici (ICCPR), Articolo 9 della Carta Africana sui diritti degli uomini e delle persone (ACHPR), Articolo 13 della Convenzione americana sui diritti dell'uomo (ACHR), Articolo 10 della Convenzione europea sui diritti dell'uomo (ECHR).

prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui".[240]

Si può concretamente constatare come il diritto alla vita privata e familiare sia una sorta di "contenitore"; questa macro insieme contiene al suo interno una serie di ulteriori diritti ed interpretazioni distinte che sono sorte soprattutto in seguito all'invenzione delle nuove tecnologie. Il contenitore qui considerato impone due diversi obblighi per i vari stati: in primis obblighi di *non facere* e secondariamente obblighi positivi. Per quanto riguarda il primo caso, si tratta ovviamente di impossibilità per lo stato di agire limitando o violando illegittimamente la vita privata e familiare; il secondo invece si esplica in obblighi positivi, concernenti molto spesso l'obbligo di adottare varie misure legislative con il compito di colmare eventuali lacune. Si parla difatti normalmente di un'applicazione "verticale" di dette norme, essendo nella maggior parte dei casi violazioni effettuate contro privati da organi statali. Dall'altra parte, premesso che si abbiano violazioni particolarmente gravi, nella maggior parte dei casi si parla di un'applicazione "orizzontale" che obbliga gli stati a reprimere condotte aventi carattere interindividuale[241]. Questo diritto tuttavia può essere soggetto a limitazioni subordinate alla realizzazione di tre condizioni distinte: le stesse devono essere previste dalla legge, devono essere giustificate da un interesse generale oppure da un interesse individuale (ad esempio, una restrizione concernente una violazione della vita privata e familiare che ha ad oggetto un'intercettazione di messaggi tra possibili attentatori per tutelare la sicurezza e la vita di altri individui) ed infine il necessario rispetto del principio di proporzionalità. Il rispetto del principio di proporzionalità deve essere tutelato sia a priori, per riuscire a comprendere se una determinata attività sia strettamente necessaria al raggiungimento dell'obiettivo e se detto obiettivo non può essere raggiunto in altro modo, sia ex post, in relazione alla vicenda

[240] Council of Europe. European Court of Human Rights. (2010). *Convenzione Europea dei diritti dell'uomo.* Consultato da https://www.echr.coe.int/documents/convention_ita.pdf

[241] Pustorino, *op. cit*., p. 81.

concreta. La nozione di vita privata è stata più volte dibattuta: quello che è possibile affermare al giorno d'oggi è che detto diritto copre la tutela di beni, luoghi e documenti che sono collegati alla sfera personale. Di conseguenza non si tratta di *privacy* solo della vita privata vista come luogo di abitazione o come luogo in cui viene svolta l'attività commerciale, ma anche e soprattutto deve essere garantita una corretta protezione della corrispondenza, sia essa effettuata in maniera postale o telematica.[242]

Un elemento del tutto particolare, già rilevato in parte durante il presente elaborato, è il diritto a non subire intercettazioni o controlli ingiustificati su comunicazioni che vengono effettuate tramite telefoni o strumenti digitali e satellitari. Queste intercettazioni possono avere una duplice natura: individuale o collettiva. Obbligo dello stato non è evitare qualsiasi tipologia di intercettazione in quanto potenzialmente lesiva del diritto fino a qui analizzato, ma è quello di dotarsi di una delimitazione legislativa che esplichi in maniera chiara e coincisa quali siano casi, limiti e durata che circondano le attività stesse. Inoltre, lo stesso concetto di "famiglia" è stato più volte dibattuto anche se oggi si è arrivati ad una soluzione comunemente accettata che comprende, oltre alla classica concezione di famiglia ritenuta come quella sorta in seguito ad un matrimonio, la famiglia nata tramite una relazione di fatto intercorrente fra genitori e figli naturali o adottivi.[243]

Negli Stati Uniti il diritto alla *privacy* risulta riconosciuto dalla *US Supreme Court* a partire dal caso *Griswold vs. Connecticut*[244]. Nel 1879 nel Connecticut fu approvata una legge che impediva qualsiasi tipologia di droga, dispositivo medico o qualsiasi altro strumento per promuove la contraccezione. Lee Buxton, ginecologo presso la *Yale School of Medicine,* in collaborazione con una donna di nome Estelle Griswold, uno dei maggiori sostenitori della genitorialità

[242] *Ibid.,* (p.156-157).

[243] *Ibid.,* (pp.158-159).

[244] Oyez. LII Supreme Court Resources. (n.d.). *Griswold v. Connecticut*. Consultato da https://www.oyez.org/cases/1964/496

programmata, decise di aprire una clinica di controllo delle nascite, violando così lo statuto vigente. Lo scopo era quello di far valutare lo statuto considerato incostituzionale per violazione del diritto alla *privacy*. La Corte Suprema, il 7 giugno 1965, con sette pareri favorevoli e due contrari, riconobbe per la prima volta un diritto alla *privacy* riconosciuto costituzionalmente, nonostante la costituzione stessa non fornisca un riferimento esplicito al diritto stesso. Di conseguenza, sulla base di un'analisi accurata del primo, terzo, quarto e nono emendamento, veniva ottenuto il diritto alla *privacy* all'interno delle relazioni coniugali. Inoltre, il diritto alla *privacy* si estende fino a comprendere il diritto a non subire perquisizioni o sequestri illegali ai sensi del rispetto del quarto emendamento della Costituzione Americana, alla luce di quanto espresso sempre dalla Corte Suprema nel caso Katz. Vs United States[245], a cui si aggiunse la chiarificazione dalla parte del giudice Potter Steward che rilevò come il quarto emendamento ha il compito di proteggere le persone, non i luoghi.

Accanto al diritto alla *privacy*, viene riconosciuto il diritto alla protezione dei dati personali. Nonostante molto spesso questi due diritti vengano presi in considerazione simultaneamente, non sono identici. Infatti, mentre il primo riguarda eventuali intrusioni nella vita privata dei soggetti, il secondo riguarda il processo materiale di collezioni di dati personali[246]. Il commento generale n.16 proposto dalla *Human Rights Committee* chiarifica un punto fondamentale relativo alla protezione dei dati personali nel paragrafo 10 del documento stesso, in cui si esplica che la raccolta e la detenzione di dati personali all'interno di computer, banche dati o altri dispositivi, siano essi pubblici o privati, devono essere regolati dalla legge. Ancora, gli stati sono tenuti a adottare le misure necessarie per garantire che tutte le informazioni che riguardino la vita privata di una persona non giungano nelle mani di persone che per legge non sono

[245] Oyez. LII Supreme Court Resources. (n.d.). *Katz v. United States*. Consultato da https://www.oyez.org/cases/1967/35

[246] Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Rev. 25*, 307, 308–309.

autorizzati e adibiti a riceverle, ad elaborarle o, più in generale, ad utilizzarle. Per avere una maggiore protezione, a ciascun individuo dovrebbe essere garantito inoltre il diritto di sapere se ci sono e, in caso affermativo, quali sono i dati personali che sono stati memorizzati, dove, da chi e con quale scopo. Se gli stessi *file* hanno ad oggetto dati personali errati o ancora sono stati raccolti in violazione di disposizioni di legge, ad ogni individuo dovrebbe essere garantito il diritto di ottenere la rettifica o addirittura l'eliminazione.[247] Le legislazioni variano in modo molto significativo a partire dalla definizione degli elementi fondamentali che riguardano il regime della protezione dei dati personali, partendo anche da una differente considerazione del tema della *privacy*. Per esempio, da un punto di vista prettamente regionale, nel territorio sudamericano sono presenti tre approcci totalmente differenti l'uno dall'altro: un'assenza totale di leggi (come avviene ad esempio a El Salvador), una regolazione estensiva basata sul concetto del "*habeas data*" (come avviene ad esempio in Costa Rica) ed infine una legislazione basata sul modello europeo (come avviene ad esempio in Brasile)[248]. L'unico accordo internazionale multilaterale, comprendente un numero ragguardevole di stati firmatari, è la Convenzione del 28 gennaio 1981, elaborata dal Consiglio d'Europa, sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, entrata in vigore a partire dal 1° ottobre 1985. La convenzione predispone che i dati della persona possano essere acquisiti solo ed unicamente con il consenso preventivo dell'interessato o in forza di quanto stabilito dalla normativa vigente, contraddistinta tuttavia da requisiti di chiarezza e prevedibilità. Lo svolgimento del processo del trattamento deve inoltre prendere in considerazione il tipo di dati trattati[249]. Inoltre, l'articolo 6 della Convenzione suddetta sancisce che è necessario che gli stati si

[247] United Nations Human Rights Committee (HRC). (1988, 8 aprile). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. Consultato da https://www.refworld.org/docid/453883f922.html

[248] Kittichaisaree, K. (2017). *Public international law of cyberspace (Vol. 32)*. Cham: Springer. (Vedi p..87)

[249] Pustorino, *op. cit.*, p. 81. (Vedi pp.160-161).

preoccupino con maggior interesse di quelli che vengono definiti come "*special categories of data*", ovvero la collezione di dati personali che riguardano o rivelano la razza, opinioni politiche e religiose o altre credenze, quelle ancora relative all'orientamento sessuale. Lo svolgimento del processo di trattamento dei questi dati, definiti sensibili, non deve essere eseguito automaticamente a meno che non ci siano, da un punto di vista legislativo, adeguate tutele[250]. La convenzione stessa, inoltre, all'articolo 11 ribadisce che viene fornito uno standard minimo di tutela che deve sempre e comunque essere riconosciuto e che può essere modificato solo se lo stato considerato è in grado di fornire standard di tutela superiori a quanto espressamente stabilito. Accanto al diritto alla protezione dei dati personali, viene riconosciuto da un punto di vista internazionale il diritto all'oblio. Questo diritto riguarda la prerogativa del soggetto nei cui confronti sono stati raccolti dati personali a vedere eliminati, soprattutto dal *web*, i dati stessi che riguardano la persona ma attengono a fatti risalenti nel tempo. Oltre, dunque, al diritto di veder cancellate e rimosse informazioni sullo stesso raccolte o che sono immagazzinate e che non possiedono più alcuna rilevanza, il diritto all'oblio difficilmente riesce ad essere rispettato sempre dagli stati, dal momento in cui lo stesso presenta contorni poco definiti. Quello che è certo è che, innanzitutto, questo diritto non impedisce allo stato di raggruppare e memorizzare i dati personali i quali, seppur risalenti nel tempo, hanno ad oggetto condotte criminose del soggetto stesso. In aggiunta, il principio da utilizzare per gli stati necessario per il rispetto del diritto all'oblio è il principio di *due diligence*, con cui lo stato è tenuto a adottare tutte le misure preventive per ottenere una tutela dell'oblio stesso[251].

[250] Council of Europe. (2020). *Lista completa dei trattati del Consiglio d'Europa.* Art. 6: «*Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions*». Consultato da https://www.coe.int/it/web/conventions/full-list/-/conventions/rms/0900001680078b37 art.6

[251] Vedi nota 183.

L'ultimo diritto che merita di essere analizzato è il diritto relativo alla libertà d'espressione. Questo diritto viene infatti riconosciuto tramite vari e plurimi strumenti internazionali, la cui interpretazione evolutiva ha permesso di modificare il concetto stesso di espressione, andando di conseguenza a ricomprendere non solo concetti espressi in maniera orale o scritta, limitata al materiale per lo più cartaceo, ma anche ad inglobare, nella tutela stessa, la libertà di espressione anche dentro al mondo virtuale. L'articolo 19 della ICCPR ricalca di pari passo l'articolo 19 della UCHR, stabilendo inoltre che le limitazioni allo stesso sono ammesse solo se prescritte dalla legge e solo se necessarie alla stregua di due motivi: per proteggere i diritti e la reputazione degli altri e per proteggere la sicurezza nazionale, l'ordine pubblico, la salute o la moralità[252]. Da un punto di internazionale, il diritto alla libertà d'espressione possiede un limite particolare, che viene essenzialmente definito "esterno": detto limite si esplica nella impossibilità di esporre qualsiasi opinione che sia anche solo lontanamente riconducibile a odio, incitamento alla violenza e alla discriminazione razziale. Come infine rilevato tramite il Tallinn Manual 2.0, nei commenti esplicativi della *Rule 35* relativa ai diritti degli individui all'interno del cyberspazio, viene presa in considerazione la distinzione intercorrente fra diritto di espressione e diritto di opinione[253]. La differenza si riverbera soprattutto nel tema delle restrizioni: mentre infatti il diritto di opinione non può in nessun modo subire restrizione il diritto d'espressione, come ampiamente sottolineato, è soggetto alle stesse.

2.7 Operazioni cibernetiche ed uso della forza

L'ultimo paragrafo del seguente capitolo ha come fine il tentativo di spiegare se ed in quali occasioni gli attacchi cibernetici possano essere equiparati ad attacchi dinamici che comportano l'uso della forza, i quali sono disciplinati nella Carta delle Nazioni Unite.

[252] Kittichaisaree, *op. cit.,* p. 90. (Vedi p. 113).

[253] Schmitt, *op. cit.,* p. 64. (Vedi pp.187-190).

Compito fondamentale delle Nazioni Unite è quello di evitare qualsiasi evento che sia in grado di minacciare la pace e la sicurezza internazionale. Questo obiettivo viene perseguito tramite una serie di prescrizioni contenute nella Carta delle Nazioni Unite, con precisione agli articoli 2, 39, 41, 42. Tuttavia, è necessario effettuare una distinzione preliminare ma di vitale importanza, relativa a due termini che molto spesso, ma non sempre, vengono a coincidere: "*use of force*" e "*armed attack*"[254]. La prima distinzione da prendere in considerazione attiene al differente regime che si riscontra nell'esistenza di due diversi articoli per entrambi i termini; il primo rientra appieno all'interno della definizione fornita all'art.2, mentre il secondo è tutelato dall'art.51 della Carta. Accanto a ciò, l'uso della forza ammette l'adozione da parte del Consiglio di Sicurezza di una serie di contromisure, aventi carattere politico o soprattutto economico, ma non giustifica mai un vero e proprio contrattacco, seppur proporzionale all'uso della forza stesso[255]. È stato, inoltre, generalmente accettato che non tutti i tipi di pressioni, comprese quelle politiche ed economiche, siano in grado di costituire un uso illecito della forza[256]. Dall'altra parte, partendo dallo studio delle Convenzioni di Ginevra relativamente al tema dello *jus in bello*, è possibile fornire una definizione generale, tuttavia non condivisa in maniera unitaria, di *armed attack* come quell'attività che comporta atti di violenza tra varie forze armate, che colpiscono almeno una persona, indipendentemente dall'entità dei danni o dalle sofferenze inflitte[257]. Nonostante le Nazioni Unite non abbiano fornito una definizione unitaria, si può analizzare una serie di casi in cui l'organizzazione ha stabilito che ci si trova di fronte ad una vera e propria

[254] Dev, P. R. (2015). Use of force and armed attack thresholds in cyber conflict: The looming definitional gaps and the growing need for formal U.N. response. *Texas International Law Journal, 50(2-3),* 381-402. Consultato da https://texashistory.unt.edu/ark:/67531/metapth838918/

[255] NATO CCDCOE Group of Experts. (Schmitt, M. N., cur). *Tallinn Manual on the International Law Applicable to cyber Warfare*. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf *Rule 9*. (Vedi p. 36).

[256] *Ibid.*

[257] Todd, G. H. (2009). Armed attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition. *Air Force Law Review, 64(1),* 65-102. Consultato da https://www.afjag.af.mil/Portals/77/documents/AFD-091026-024.pdf

aggressione. Tramite la risoluzione n.3314/1974 l'Assemblea generale ha definito il termine aggressione nel seguente modo, fornendo inoltre una serie non esaustiva di esempi:

> *«use of armed force by a State against the sovereignty, territorial integrity, or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations*[258]*»*.

Di conseguenza, il riscontro dell'aggressione, anziché di un vero e proprio attacco armato, viene preso (infelicemente) in considerazione sulla base di circostanze rilevanti, presupponendo nel primo caso una mancanza di quella "*sufficient gravity*" in grado di far coincidere l'attività come un "*armed attack*"[259].

L'art.2 al paragrafo 4 sancisce una proibizione fondamentale per tutte quelle attività che prevedono l'uso della forza, imponendo agli stati l'obbligo di trattenersi, all'interno delle loro relazioni internazionali, da qualsiasi minaccia o dall'utilizzo concreto della forza attuato nei confronti dell'indipendenza e dell'integrità territoriale e politica di altri stati, o in qualsiasi altra maniera che risulta incompatibile con i fini per i quali le Nazioni Unite sono state istituite[260]. Sono presenti due eccezioni alla proibizione dell'utilizzo della forza, eccezioni inserite all'interno della carta stessa. La prima è contenuta nell'art.39[261], il quale sancisce che il Consiglio di sicurezza può decidere, una volta accertata una minaccia alla pace, una violazione della pace o un atto di aggressione, di adottare o una raccomandazione (la quale tuttavia non ha efficacia vincolante nei confronti del destinatario) oppure decidere quali misure adottare tra quelle legittime stanti gli articoli 41 e 42, col fine di mantenere o ristabilire la pace. Il

---

[258] United Nations General Assembly. (1974). *Res. 3314, U.N. GAOR, 29th Sess., art. 1 (Dec. 14, 1974)*. Consultato da https://research.un.org/en/docs/ga/quick/regular/29

[259] Todd, *op. cit*., p. 94.

[260] United Nations. (2020). *Charter of the United Nations. Chapter I: Purposes and Principles.* Consultato da https://www.un.org/en/sections/un-charter/chapter-i/index.html

[261] *Ibid.*

secondo caso che ammette, pur essendo subordinato a notevoli ed evidenti limitazioni, l'uso della forza è contenuto nel art.51, il quale rende lecita la legittima difesa. Sulla base di queste previsioni, nessuno stato ha la possibilità di utilizzare la forza nei confronti di un'altra nazione a meno che non venga fornita un'autorizzazione da parte del Consiglio di sicurezza, o nel caso di legittima difesa.

L'evoluzione di queste previsioni ha portato le Nazioni Unite ad includere all'interno delle stesse l'equiparazione dei *cyber attacks* agli attacchi dinamici. Partendo dal presupposto che gli articoli sopra menzionati in nessun modo fanno riferimento ad armi o a categorie di armi particolari, la Corte Internazionale di Giustizia, tramite un suo *advisory opinion* del 1996 relativo alla legalità della minaccia di armi nucleari, ha rilevato come le previsioni sull'uso della forza siano totalmente indipendenti dall'arma utilizzata, includendo di conseguenza come possibili minacce per la pace anche le armi cibernetiche[262]. Inoltre, sulla base del fatto che la normativa contenuta nella Carta delle Nazioni Unite all'art.2(4) riflette una norma di diritto consuetudinario e, per quanto riguarda il suo "nucleo", anche di *jus cogens*[263], è stata più volte affermata l'applicabilità della normativa sull'uso della forza nel contesto di operazioni cibernetiche sulla base, in primis, di dichiarazioni statali rilevanti in materia e successivamente anche tramite il riscontro all'interno del report del 2013 realizzato dal gruppo di esperti di detta applicabilità[264]. Le dichiarazioni statali, come analizzato antecedentemente, relative all'applicabilità della normativa prevista dalla Carta alle operazioni cibernetiche, sono state fornite da paesi come Italia, Cuba, Mali, Iran, Olanda, Qatar, Stati Uniti, ma anche da organizzazioni internazionali regionali come per esempio l'Unione Europea[265]. Dall'altra parte, il report del

[262] International Court of Justice (ICJ), Official Website. (2020). *Legality of the Threat of Nuclear Weapons, Advisory Opinion,* (1996, 8 luglio). 22, 39. Consultato da https://www.icj-cij.org/en/case/95

[263] Tsagourias, *op. cit*., p. 61. (Vedi p. 233).

[264] *Ibid*.

[265] *Ibid*.

2013 ha inoltre riscontrato come le previsioni contenute nella Carta delle Nazioni Unite siano applicabili anche alle operazioni cibernetiche non solo per mantenere la pace e la stabilità ma anche per promuovere un ambiente informatico sicuro e contraddistinto da una leale cooperazione fra gli stati[266]. Le problematiche maggiori tuttavia riguardano, da una parte, le caratteristiche generali che un *cyber attack* deve possedere per rientrare nelle previsioni relative all'uso della forza e dall'altra, basandosi sulle stesse caratteristiche, sotto quale specifico articolo far rientrare l'attività[267] .

Sulla base dell'art.2, viene dato al *Security Council* il ruolo di organo principale per determinare quando è lecito utilizzare la forza, essendo anche riconosciuta, allo stesso, la possibilità di avere una forza militare "propria", con il diritto di agire servendosi della forza per mantenere la pace e la sicurezza internazionale[268]. L'articolo 2, accanto al vero e proprio uso della forza, sancisce l'impossibilità per gli stati di comportarsi con le altre nazioni con attività che assurgono al livello di minaccia dell'uso della forza stessa. Il termine "*threat*" è ancora molto vago, mancandone una definizione unitaria. Quello che può essere asserito fa riferimento ad una vera e propria dinamicità del termine stesso, con conseguente ampliamento, anche sulla base delle innovazioni tecnologiche, dei casi in cui è riscontrabile una minaccia per la pace. Come analizzato dal Professor Wingfield, ci sono una serie di minacce che possono essere ricondotte a quelle coperte dall'art.2 della Carta: tra queste ci sono le minacce verbali, i movimenti iniziali delle truppe, movimenti preliminari di missili balistici, il raggruppamento e movimento di truppe lungo il confine o anche le interferenze

[266] *Ibid*.

[267] Weissbrodt, D. (2013). *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage.* University of Minnesota Law School, 347-387. Consultato da https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles

[268] Miller, A. (1993). Universal Soldiers: U.N. Standing Armies and the Legal Alternatives, *81 GEO. L.J.*, 773, 779-83. Consultato da https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles

con i sistemi di allerta di comando e controllo dei vari stati[269]. Il fatto che manchi, di conseguenza, una lista esaustiva delle minacce lascia presagire la possibilità di includere nelle stesse quelle derivanti da un *cyber attack.* Nonostante la mancanza, inoltre, di una definizione unitaria di uso della forza, l'inclusione all'interno della stessa dell'attività cibernetica, fino ad ora considerata, si concretizza partendo dall'esistenza di diversi parametri che accomunano le varie attività. Preliminarmente, due visioni sono state proposte per determinare se è stata effettuata un'attività comprendente l'uso della forza non legittima sulla base dell'art.2[270]. La prima è quella avanzata dallo studioso Michael Schmitt, il quale vede nella presenza di 7 fattori la possibilità di far rientrare un'azione dello stato o all'interno del regime di forza armata proibita stante l'art.2 oppure all'interno di quella categoria che comprende l'esercizio non di una forza armata ma di una forza economico o politica, la quale deve essere considerata al di fuori delle attività illegittime regolate dall'art.2[271]. Questi 7 parametri considerati attengono ai temi della serietà, istantaneità, immediatezza, efficacia, misurabilità dell'attacco, possibile legittimità ed infine il regime di responsabilità applicabile.

Mentre le azioni che comportano un danno materiale a persone o cose, se assumono un certo livello, sono senz'altro da considerare come atti che comportano l'uso della forza da parte di uno stato, dall'altra parte le *Computer network operations* (CNO), le quali sono state definite dallo Stato Maggiore Congiunto degli Stati Uniti come quelle attività cibernetiche utilizzate per attaccare, ingannare, interrompere, degradare, negare o sfruttare informazioni ed infrastrutture elettroniche[272], possono avere addirittura un impatto sulla

[269] National Research Council. (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press. Consultato da https://www.nap.edu/read/12651/chapter/1

[270] Weissbrodt, *op. cit.*, p. 96.

[271] Schmitt, M. N. (2011). Cyber Operations and the Jud Ad Bellum Revisited. *Vill. L. Rev.*, *56(3)*, 569-606. Consult. da https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1019&context=vlr

[272] Ghosh, S., & Turrini, E. (Cur.). (2010). *Cybercrimes: a multidisciplinary analysis*. Springer Science & Business Media.

popolazione maggiore. Infatti, queste attività hanno un impatto su interessi critici a livello nazionale ed hanno maggiori probabilità di assurgere al rango di attività rientrante nell'uso della forza; inoltre, la portata ma soprattutto la durata degli effetti saranno utilizzati per determinare la gravità dell'attacco[273]. Viene inoltre valutata la velocità con cui gli effetti si propagano in seguito ad un CNO e l'esistenza di una connessione tra i danni analizzati e quest'ultimo. La presunta legittimità va verificata sulla base del principio che tutte quelle attività che non sono illegali sono di conseguenza legittime. Tramite questi parametri, di conseguenza, è possibile determinare se l'azione considerata assurge al rango di uso della forza vietato dall'art.2 oppure se è meglio non farlo rientrare all'interno di quel contesto[274].

Il secondo approccio, sempre analizzato da Schmitt, si concretizza nella realizzazione di un'ampia analisi, partendo dai risultati, in grado di esaminare l'impatto che hanno avuto le *Computer network operations,* sulla base della gravità dell'azione. Secondo lo studioso, analizzare solo il risultato o la gravità delle conseguenze non risulta sufficiente ai fini della distinzione tra un attacco armato ed una coercizione economica e politica[275]. Infatti, sulla base di questo approccio solamente legato agli effetti, una forza di tipo economico per i danni prodotti sarebbe in grado di assurgere al livello di forza armata, proprio per la forza del suo impatto[276]. L'approccio considerato, basato sui risultati, pertanto contrasta con l'attuale interpretazione, stante la quale l'uso della forza non comprende la forza economica.

Per essere in grado di interpretare le operazioni cibernetiche alla stregua dell'art.2(4) della Carta, tre condizioni distinte devono sussistere: la prima fa

---

[273] *Ibid.*

[274] Hoisington, M. (2009). Cyberwarfare and the use of force giving rise to the right of self-defense. *BC Int'l & Comp. L. Rev., 32*, 439. Consultato da https://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16/

[275] Schmitt, *op. cit.*, p. 97. (Vedi pp. 917-919).

[276] Barkham, J. (2001). Information warfare and international law on the use of force. *NYUJ Int'l L. & Pol., 34*, 57.

riferimento alla riconducibilità dell'attività cibernetica ad uno stato, la seconda prevede che l'operazione assurga ad un livello di minaccia della pace o ad un uso della forza ed infine la terza prevede che la minaccia o l'uso della forza siano subordinate ad attività cibernetiche adottate nel contesto di relazioni internazionali.[277] Per quanto riguarda il primo punto, è possibile constatare come i maggiori problemi derivino essenzialmente dalle difficoltà di attribuire con assoluta certezza un'operazione cibernetica ad uno stato. Il secondo punto viene preso in considerazione alla stregua delle differenti operazioni cibernetiche considerate, mentre il terzo prevede l'applicabilità della normativa solo quando l'attività sia posta in essere da uno stato contro un altro stato: di conseguenza uno stato ha la possibilità di ricorrere alla minaccia o all'utilizzo della forza tramite operazioni informatiche nei confronti di attori non statali all'interno del proprio territorio[278].

Il secondo punto preso in considerazione merita infine una particolare analisi, dal momento che non tutte le operazioni cibernetiche assumono la rilevanza di attacco cibernetico, così come definito dalla *Rule 30* del Tallinn Manual, cui potrebbe essere applicabile l'art.2(4) della Carta. In particolare, il mancato utilizzo nell'operazione informatica di una "*weapon*" è in grado di contraddistinguere l'attività di *cyber exploitation* da quella di *cyber attack*[279]. È previsto che se un attacco informatico causa o è in grado di causare danni fisici alla proprietà, perdita di vite o lesioni personali, in un modo assolutamente equivalente ad un attacco dinamico, tramite la cancellazione o la distruzione di software e di dati, lo stesso porterà ad una violazione di cui all'art.2(4) della Carta[280]. Questo tema viene inoltre analizzato in relazione alla *Rule 11* del Tallinn Manual, la quale chiarisce come un'operazione cibernetica costituisca un'attività comprendente l'uso della forza quando la sua portata ed i suoi effetti

[277] Tsagourias, *op. cit.*, p. 61.

[278] *Ibid.*

[279] *Ibid*., (p. 240).

[280] *Ibid*., (p. 242).

siano paragonabili alle operazioni non cibernetiche che assurgono ad operazioni comprendenti l'uso della forza[281]. All'interno del suo discorso tenuto di fronte al CYBERCOM, Harold Koh cita alcuni esempi materiali di *cyber* operazioni che sono in grado di assurgere al rango di atti comprendenti l'uso della forza: le operazioni cibernetiche che, tramite un'intrusione, fanno scattare una fusione all'interno di una centrale nucleare di un altro stato, le operazioni che comportano l'apertura dei sistemi di sicurezza di una diga, andando di conseguenza a causare morte e devastazione nell'area popolata antistante o ancora operazioni che disabilitano il controllo aereo sul territorio di uno stato causando una confusione che porta alla collisione di più aerei[282].

Mentre da un lato vi è una comunità di visione relativamente all'applicabilità della normativa contenuta nell'art.2(4) per le operazioni appena menzionate, una maggiore incertezza si ha nel momento in cui si cerca di ricomprendere quelle operazioni che vengono definite "dirompenti": tra queste, per esempio, quelle che hanno come obiettivo quello di rendere inefficaci ed inutilizzabili determinate infrastrutture senza causare effettivi danni alle stesse[283]. È possibile di conseguenza asserire come, anche sulla base delle caratteristiche di interpretazione evolutiva che sono state precedentemente analizzate, l'attività cibernetica che ha un'intensità tale da colpire la sicurezza statale rientri senz'altro tra quelle attività che comportano una violazione della proibizione dell'uso della forza contenuta all'art.2(4)[284]. Come sottolineato inoltre dalla direttiva presidenziale americana n.20/2012, si dovrebbero includere anche attività cibernetiche che colpiscono le infrastrutture di sicurezza pubblica ed

[281] Schmitt, *op. cit*., p. 64.

[282] Koh, H. (2018). *International law in cyberspace*. (Discorso tenuto presso *the USCYBERCOM Inter-Agency Legal Conference*, 18 settembre 2012) in Carrie Lyn D. Guymon (Cur.), Digest of United States Practice in International Law (United States Department of State 2012) 593, 594–595.

[283] Tsagourias, *op. cit*., p. 61.

[284] *Ibid.*

economica che risultano essere fondamentali per lo stato[285]. Queste attività cibernetiche che rendono impossibile usufruire di servizi essenziali dello stato, pur non causando effettivi danni fisici al sistema, possono causare ritardi nelle attività di emergenza o di soccorso, o ancora nella fornitura di energia, nella tutela della sanità pubblica, andando di seguito a causare probabilmente danni materiali agli individui[286].

Infine, attacchi cibernetici che non causano, o non sono ragionevolmente in grado di causare, un danno materiale agli oggetti, perdite di vite umani o lesioni personali, o ancora gravi perturbazioni dei servizi essenziali, non rientrano nelle previsioni relative all'uso della forza, non andando a costituire di conseguenza una violazione dell'art.2 della Carta[287]. Tuttavia, se gli stessi vengono realizzati da uno stato, possono integrare una violazione del principio di non intervento all'interno degli affari interni di un altro stato[288].

È possibile, di conseguenza, concludere asserendo che le previsioni relative all'uso della forza contenute nella Carta delle Nazioni Unite possono essere applicate anche alle operazioni cibernetiche: la mancanza di disposizioni speciali sul tema non presuppone la possibilità per i vari stati di effettuare operazioni informatiche contro altri stati senza restrizioni. La necessità di utilizzo di un "arma" come sopra delineata nel compimento dell'operazione informatica ed il carattere coercitivo dell'attività sono gli elementi fondamentali per poter individuare un'operazione cibernetica come l'uso di forza armata. Non solo, dunque, la normativa sarà applicata nel caso di perdita di vite umane o lesioni, ma anche nel caso di attività che rendono inutilizzabili una serie di strutture critiche per lo stato, anche se non si configurano come danni materiali.

---

[285] US Presidential Policy Directive/PPD–20. (2012, ottobre). *US Cyber Operations Policy*. Consultato il 14 gennaio 2021 da https://fas.org/irp/offdocs/ppd/ppd-20.pdf

[286] Tsagourias, *op. cit.*, p. 61.

[287] *Ibid.*

[288] Schmitt, *op. cit.*, p. 64 (*Rule 10)*.

Inoltre, è stato analizzato ed evidenziato dal gruppo di esperti che ha dato vita al Tallinn Manual il tema della minaccia o dell'uso della forza, a cui è dedicato interamente il capitolo 14. In particolare, il gruppo ha sottolineato, tramite la *Rule 68*, come una cyber operazione che ottiene, nel mondo cibernetico, la qualifica di minaccia o uso della forza contro l'integrità territoriale o l'indipendenza politica di uno stato o, che risulta in qualsiasi altra maniera inconsistente con le previsioni della Carta, costituisca una violazione dell'art.2[289]. Come già spiegato nel corso dell'elaborato, anche per qualificare un'operazione cibernetica come uso della forza non è necessario che la stessa sia intrapresa dalle forze armate di uno stato. Infatti, accanto al normale di caso di uso della forza tramite l'utilizzo di forze armate, una condotta cibernetica si qualificherebbe come tale anche se intrapresa da attività di intelligence o dai cosiddetti contractors[290], quando la condotta sia attribuibile alla volontà dello stato[291]. Sulla base della *Rule 69* viene inoltre definita come cyber operation che assurge al rango di uso della forza quella che, studiando gli effetti considerati, è in grado di essere comparata alle operazioni dinamiche che includono l'uso della forza stessa[292].

Lo scopo del seguente elaborato, come verrà analizzato specificatamente nel capitolo quarto, parte dall'assimilazione di attacchi cibernetici agli attacchi dinamici, i quali sono a tutti gli effetti in grado di compromettere la pace internazionale. Mentre sono a stabilite una serie di contromisure adottabili per il mantenimento della pace da un punto di vista dinamico, tramite anche le cosiddette operazioni di *peacekeeping* che hanno la funzione prevenire conflitti o cercare di "stabilizzare" la pace nei paesi in cui la stessa non è garantita, da un

[289] *Ibid.*, (p. 329).

[290] Lovato, G. (2017). *Private Military and Security contractors Origini, problematiche e continuità con il passato*. [Tesi, Università Ca'Foscari Venezia]. Il termine inglese "*contractors*" si riferisce generalmente ad imprese che forniscono consulenze o determinati servizi aventi natura militare. Hanno la possibilità anche di fornire personale.

[291] Schmitt, *op. cit.*, p. 19. (Vedi p. 330).

[292] *Ibid.*

punto di vista cibernetico l'attività delle organizzazioni internazionali risulta particolarmente carente[293]. Partendo dunque da un'equiparazione degli attacchi cibernetici a quelli dinamici, con conseguente applicabilità della stessa normativa, la cooperazione internazionale ed il mantenimento della pace potrebbe essere coadiuvata dal fenomeno, per ora solo ipotetico, di un *cyber peacekeeping team* in grado di attuare una serie di cyber *peacekeeping operations*, le quali sarebbero in grado di garantire una situazione di stabilità all'interno del mondo cibernetico, così come avviene nel mondo dinamico[294].

2.7.1 *Segue*: Minaccia dell'uso della forza

Accanto alla proibizione dell'uso della forza, la seconda clausola da esaminare si riferisce al termine inglese "*threat*", il quale può essere "banalmente" definito come minaccia dell'uso della forza. Su questo tema possono essere fornite chiarificazioni tramite quanto analizzato nella *Rule 70* del Tallinn Manual, la quale cerca di fornirne una definizione: un'operazione informatica o un'operazione informatica minacciata, costituisce un illegale minaccia dell'uso della forza quando l'azione minacciata, se effettuata, sarebbe considerato come un atto che comporta l'uso della forza[295]. Questa regola dovrebbe essere applicabile in due situazioni: qualora un'operazione informatica venga utilizzata per comunicare una minaccia dell'uso della forza (sia essa cinetica o dinamica) e nel caso in cui la minaccia stessa sia trasmessa con qualsiasi mezzo (come, per esempio, le dichiarazioni pubbliche) per portare operazioni informatiche qualificabili come uso della forza[296]. Risulta comunemente riconosciuto che le minacce da parte degli stati e degli ufficiali che ricoprono le posizioni più alte siano assolutamente illegittime, sempre che l'azione minacciata sia illegittima.

[293] Almutawa, *op. cit*., p. 27.

[294] *Ibid*.

[295] Schmitt (2017), *op. cit*., p. 64.

[296] *Ibid.*

Un esempio, riportato dal gruppo di esperti, che spiega questa situazione può essere analizzato: uno stato, nei cui confronti è stato scagliato un attacco cibernetico armato ha la possibilità di minacciare l'aggressore. Inoltre, minacciare di intraprendere azioni che non sono proibite dal diritto internazionale risulta giuridicamente legittimo. Anche se solitamente la minaccia dovrebbe essere intesa come coercitiva, non è richiesto, per la qualificazione della stessa come tale, che essa sia accompagnata da alcuna richiesta[297].

La natura della minaccia ha una matrice comunicativa e deve avere, come caratteristica, la capacità di essere trasportata fino allo stato di destinazione, il che ammette la possibilità che sia espressa o veicolata implicitamente. Inoltre, la reale capacità e forza cibernetica di uno stato non è uno degli elementi che servono a valutare la veridicità e la gravità di una minaccia, dal momento che la capacità cibernetica di uno stato non viene valutata alla stregua di parametri come la grandezza, la popolazione o la forza economico militare. Allo stesso modo non è stato raggiunto un consenso relativamente ad uno stato che possiede la capacità di realizzare la minaccia professata ma che chiaramente non intende farlo. Un esempio pratico è rappresentato da uno stato che possiede una capacità informatica offensiva e il cui leader esprime minacce contro gli altri stati solo ed unicamente per motivi puramente politici.

2.7.2. *Segue*: operazioni cibernetiche e legittima difesa

L'art.51 della Carta delle Nazioni Unite pone le basi del concetto di legittimità di autodifesa individuale o collettiva[298]. L'articolo è stato fortemente voluto,

[297] *Ibid*.

[298] Goodrich, L. M., Simons, A. P., & Hambro, E. I. (1969). *Charter of the United Nations: Commentary and Documents. 3d and rev. ed*. Columbia University Press.

durante la Conferenza di San Francisco, dagli stati latino-americani[299]. L'art. 51 recita nel seguente modo:

> «*Nessuna 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*».[300]

Il principio del diritto alla legittima difesa in seguito ad un attacco armato è subordinato al rispetto di tre requisiti, i quali, una volta accertata la loro esistenza, legittimano la reazione da parte di uno stato: necessità, imminenza e proporzionalità. Il requisito della necessità è forse quello meno problematico, dal momento che per necessità si intende l'impossibilità di utilizzare un altro mezzo per risolvere pacificamente la questione[301]. Più complicato è quello dell'imminenza. L'art. 51 riconosce la possibilità allo stato soggetto ad un imminente attacco di difendersi legittimamente; tuttavia, questa imminenza risulta particolarmente problematica dal momento che potrebbe astrattamente giustificare una sorta di legittima autodifesa avente carattere preventivo, che si può andare a concretizzare in un'azione assolutamente offensiva, prima che

[299] Kunz, J. L. (1947). Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations. *American Journal of International Law*, *41*(4), 872–879. http://doi.org/10.2307/2193095

[300] Vedi nota 298.

[301] Sklerov, M. J. (2009). Solving the dilemma of sate responses to cyberattacks: A justification for the use of active defenses against states who neglect their duty to prevent. *Mil. L. Rev.*, *201*, 1.

difensiva. Il punto risulta particolarmente problematico, non essendo attualmente uniforme la visione relativa alla definizione di imminente attacco tra i vari stati[302]. In particolare, durante la guerra fredda, diversi stati hanno ritenuto che l'azione di autodifesa sarebbe stata legittima solo ed unicamente se un attacco armato fosse stato effettivamente lanciato. Il Regno Unito, gli Stati Uniti ed altri stati hanno mantenuto un approccio particolare che potrebbe essere definito come il "*Caroline approach*", il quale prevede la possibilità di adottare una legittima autodifesa nel caso in cui l'attacco sia istantaneo, travolgente e non lasci scelta di mezzi né tempo per deliberare[303]. Inoltre, il requisito dell'immediatezza richiede che non sia passato un tempo eccessivo dall'attacco[304]. L'ultimo requisito che deve essere rispettato infine riguarda la proporzionalità della reazione: quest'ultima deve essere della forza necessaria per sconfiggere un attacco in corso o per scoraggiare un'aggressione futura[305].

Il principio essenziale, accolto in maniera unanime, si fonda sulla constatazione che uno stato ha la possibilità di reagire rispondendo solo ed unicamente ad un attacco armato. Nonostante il concetto di quantità e natura della forza sia ancora oggi oggetto di dibattito, quello che può essere agevolmente constatato fa riferimento al fatto che gli stati, nel momento in cui invocano il loro diritto alla legittima difesa, sin dal momento della stipulazione della Carta, si sono preparati ad altri attacchi statali, non ad attacchi da parte di attori non statali o di singoli individui[306]. Lo stesso art.1 della risoluzione n.3314/1974 sancisce che l'aggressione può avvenire solo da parte di uno stato[307]. Il tema, di conseguenza,

---

[302] Wood, M. (2013). International Law and the Use of Force: What Happens in Practice?. *Indian journal of international law, 53*, 345-367. Consultato da https://legal.un.org/avl/pdf/ls/Wood_article.pdf

[303] Green, J. A. (2006). Docking the Caroline: Understanding the relevance of the formula in contemporary customary international law concerning self-defense. *Cardozo Journal of International and Comparative Law, 14(2)*, 429-480.

[304] Hoisington, *op. cit.*, p. 98.

[305] Sklerov, *op. cit*., p. 105.

[306] Arai-Takahashi, Y. (2002). Shifting Boundaries of the Right of Self-Defence-Appraising the Impact of the September 11 Attacks on Fus Ad Bellum. In *Int'l L.*, 36. (Vedi p. 1081).

[307] United Nations General Assembly. (1974). *Resolution 3314 (XXIX)*. *Definition of aggression*. United Nations, New York. Consultato da athttp://www.un.org/documents/ga/res/29/ares29.htm.

dell'attribuzione statale assume un'importanza vitale dal momento che giustifica il carattere di legittima difesa da parte di uno stato. Tuttavia, il regime di responsabilità ed attribuzione è cambiato notevolmente nel corso del tempo tenendo in considerazione due fattori distinti: l'attentato delle torri gemelle e la proliferazione delle organizzazioni terroristiche[308]. Da un punto di vista internazionale, era pacificamente riconosciuto il fatto che una nazione sarebbe stata ritenuta responsabile solo ed unicamente se l'attività adottata da individui singoli fosse riconducibile ad organi o ad entità dello stato[309]. Tuttavia, sulla base del principio di *due diligence* analizzato all'interno del primo capitolo e che verrà ripreso, la giurisprudenza internazionale è arrivata ad ammettere la possibilità di una responsabilità indiretta dello stato per il comportamento di attori non statali, qualora non venga effettuato un controllo effettivo e globale tale da impedire attacchi provenienti dal suo territorio. Gli eventi del 11 settembre sono stati assolutamente determinanti nello sviluppo della responsabilità statale indiretta contemporanea. Il diritto internazionale non poteva ammettere e legittimare una rappresaglia militare in Afganistan unicamente contro Al Qaeda, in quanto un gruppo terroristico non poteva rappresentare una delle cause in cui la legittima difesa era ammessa, dal momento che non si trattava dello stato[310]. Più di due settimane dopo l'11 settembre, il Consiglio di sicurezza delle Nazioni Unite adottò la risoluzione 1387[311], la quale stabilisce che tutti gli stati si devono trattenere dalla fornitura di qualsiasi forma di sostegno, attiva o passiva, ad entità o persone coinvolte in atti terroristici. Gli Stati Uniti inoltre intentarono una causa contro i Taleban, sostenendo la loro incapacità di prevenire un attacco terroristico che ha avuto origine all'interno dei propri confini, in seguito inoltre all'accoglimento di diversi membri di Al Qaeda. A partire da quel momento, lo

[308] Proulx, V. J. (2006). Babysitting terrorists: Should states be strictly liable for failing to prevent transborder attacks. *Berkeley J. Int'l L.*, *23*. (Vedi p. 619).

[309] Bowett, D. (1972, gennaio). Reprisals involving recourse to armed force. *Am. J. Int'l L.*, 66(1), 1-36.

[310] Jinks, D. (2003). State responsibility for the acts of private armed groups. *Chi. J. Int'l L.*, 4(1). Consultato da https://chicagounbound.uchicago.edu/cjil/vol4/iss1/8/ (Vedi p. 89).

[311] United Nations SCOR. (2001, 28 settembre). *Resolution 1373 Doc. S/RES/1373 (2001).* Consultato da https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

standard di responsabilità indiretta è diventato un punto di vista prevalente nel sistema di attribuzione[312].

Una volta che un attacco viene qualificato come un attacco armato, sia esso un attacco online o cinetico, fornisce allo stato ferito il diritto di autodifesa. Il metodo dell'attribuzione, tuttavia, sulla base del quale viene garantita la legittima difesa, trova particolari difficoltà nel caso di attacco cibernetico o di *cyber* terrorismo, per una serie di motivi che saranno di seguito analizzati[313]. Anche se gli stati sono costantemente obbligati nel tentativo di prevenzione di attacchi che hanno origine e partono dal proprio territorio, nel mondo cibernetico l'efficacia di detti tentativi risulta notevolmente limitata dal momento che gli attacchi cibernetici sono particolarmente difficili da evitare[314]. L'attribuzione dell'attacco, nonché la natura dello stesso, sono requisiti imperativi nel contesto di attività cibernetiche[315]. L'attribuzione garantisce che l'attività di difesa sia diretta effettivamente condotta contro il responsabile, evitando così di andare a colpire individui o stati innocenti. Inoltre, l'attribuzione svolge un ruolo critico nella determinazione della tipologia di contro-attività da attuare, sulla base altresì del criterio di proporzionalità precedentemente analizzato; questo importa la scelta sulla natura offensiva o difensiva della condotta legittima da adottare. A differenza del mondo dinamico, due sono gli elementi da considerare: il problema del "*attaccker attribution*", ovvero la determinazione del soggetto responsabile per l'attacco, e "*attack attribution*", ovvero la natura dell'attacco

[312] Proulx, *op. cit*., p. 107. (Vedi p. 638).

[313] Grosswald, L. (2011). Cyberattack attribution matters under article 51 of the U.N. Charter. *Brooklyn Journal of International Law*, 36(3), 1151-1182. Consultato da https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1124&context=bjil

[314] Barkham, *op. cit*., p. 98. (Vedi p. 83).

[315] Condron, S. M. (2007). Getting it right: Protecting American critical infrastructure in cyberspace. *Harvard Journal of Law & Technology, 20(2)*, 403-422. Consultato da https://jolt.law.harvard.edu/assets/articlePDFs/v20/20HarvJLTech403.pdf (Vedi p. 414).

stesso[316]. Mentre per quanto riguarda gli attacchi dinamici il regime dell'attribuzione risulta particolarmente semplice, ciò derivando dal fatto che coloro che agiscono nel mondo dinamico svolgono la propria attività all'interno del mondo tangibile, le difficoltà che si presentano in tema di *cyber attack* attengono all'intangibilità del mondo virtuale; questo avviene perché solitamente la localizzazione dei *server* non coincide con quella reale, dal momento che viene utilizzato uno strumento, denominato "*stepping stone*", in grado di utilizzare computers di soggetti che non si trovano all'interno dello stato. Di conseguenza, la localizzazione di un attacco informatico può essere, *prima facie*, inconcludente, dal momento che chiunque, con le competenze necessarie, ha la possibilità di portare a termine un attacco informatico transnazionale anonimo[317]. Per quanto invece riguarda il secondo punto, anche il tema del "*online attack-attribution*" risulta molto più complicato di quanto avviene per attacchi nel mondo reale; tuttavia, l'identificazione della natura dell'attacco informatico è il primo passo necessario per valutare il caso in cui si tratti di un attacco armato ai sensi dell'art. 51, per riuscire a garantire che qualsiasi risposta sia effettuata alla stregua dei principi di necessità e proporzionalità. Il problema si rileva partendo dalla difficoltà di determinare la natura dell'attacco; infatti, gli indicatori che devono essere utilizzati, quali il punto d'origine dell'attacco o di evento, nonché il motivo, sono in grado di creare un'ambiguità maggiore rispetto a quanto avviene nel mondo reale[318].

Lo scenario che si presenta, con notevoli difficoltà nella determinazione di un'attività alla stregua di un semplice crimine, di un attacco terroristico o di un attacco armato ai sensi dell'art. 51, rappresenta al giorno d'oggi una delle più stimolanti sfide che il modello delineato dall'articolo stesso deve affrontare. La

[316] Brenner, S. W. (2007). At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology, 97(2).* Consultato da https://scholarlycommons.law.northwestern.edu/jclc/vol97/iss2/2/ (Vedi p. 405).

[317] *Ibid*., (p. 414).

[318] *Ibid.,* (p.436.)

problematica, di conseguenza, si sviluppa a monte, dal momento che la mancata capacità di definizione determina la possibilità di violazione del principio di proporzionalità nella controazione. Mentre alcuni tipi di attacchi cibernetici, come ad esempio un attacco in cui l'obiettivo unico è quello di escludere un altro stato dalla rete o ancora un attacco informatico che altro non è se non la parte preliminare di un attacco cinetico[319], rientrano appieno nel contesto di forza armata che legittima l'autodifesa di cui all'art. 51, ne esistono alcuni di minore intensità e di più difficile localizzazione ed attribuzione che destano problemi. Infatti, permettere agli stati di rispondere senza prima determinare l'attacco comporterebbe un vero e proprio indebolimento della forza delle previsioni delle Nazioni Unite. L'aggiramento della regola dell'attribuzione comporterebbe, per gli stati, la possibilità di godere di una troppo ampia autonomia nella determinazione della portata e dell'intensità della risposta[320]. Per questo, il criterio di attribuzione ottiene nel cyberspazio una valenza fondamentale; riuscire a risalire all'origine di un attacco cibernetico ed individuare con precisione i vari effetti di un attacco sono vitali per rispettare i requisiti imposti in tema di autodifesa sulla base della normativa internazionale. La pervasività di attori non statali su internet, nonché la loro abilità nel mascherare le proprie tracce, richiede un rafforzamento del concetto di attribuzione; per questo, al fine di evitare contrattacchi contro stati attuati sulla base di una legittima difesa, è necessario prevenire attività nei confronti di innocenti[321].

Quanto fino a questo momento detto trova riscontro nella *Rule 71* del Tallinn Manual, il quale analizza come uno stato, bersaglio di un'operazione informatica che raggiunge il livello di attacco armato, ha la possibilità di far leva sul

[319] Barkham, *op. cit.*, p. 98. (Vedi p. 80).

[320] *Ibid*., (p. 82).

[321] Grosswald, *op. cit.*, p. 108. (Vedi p. 117).

principio di autodifesa; la valutazione sull'operazione considerata dovrà essere fatta tenendo conto della sua gravità e dei suoi effetti.[322]

Per concludere, per rispondere ad un attacco lo stato considerato deve identificare l'attività cibernetica come attività ostile. A differenza di quanto avviene per gli attacchi cinetici, la natura istantanea dei *cyber attack*s priva gli stati di qualsiasi possibilità di risposta preventiva[323]. Una risposta per questo problema incombente è stata fornita dallo studioso Walter Gary Sharp, il quale ha proposto che tutti gli stati adottino una regola generale di ingaggio, in grado di permettere agli stessi di utilizzare la forza in caso di autodifesa anticipatoria contro qualsiasi stato identificato, il quale dimostri un intento ostile tramite l'entrata o il tentativo di entrata dentro quei sistemi informatici che hanno particolare rilevanza[324]. La capacità di rispondere concretamente ad attacchi cibernetici risulta fondamentale, anche se lo strumento migliore, che vada oltre al tema della legittima difesa statale, prevede un'attività di sicurezza collettiva, come individuata nel Tallinn Manual, cui è dedicato l'intero capitolo 15[325]. Le rules presenti, che verranno trattate specificatamente all'interno del prossimo capitolo, forniscono la possibilità di svolgere una serie di *peace operations* che sarebbero in grado di assicurare una maggiore stabilità internazionale.

[322] Schmitt, *op. cit.*, p. 19. (Vedi p. 339).

[323] Hoisington, *op. cit.*, p. 98. (Vedi p. 451).

[324] Sharp, W. G. (1999). *Cyberspace and the Use of Force*. Aegis Research Corporation. (Vedi p. 130).

[325] Schmitt, *op. cit.*, p. 64. (Vedi p. 357).

Capitolo 3

LE PRINCIPALI ORGANIZZAZIONI INTERNAZIONALI IMPEGNATE NEL CYBER SPAZIO

SOMMARIO: 3.1 L'attività delle organizzazioni internazionali in tema di *cyber security* - 3.2 Le attività dell'UE in materia di *cyber security*: il ruolo dell'Agenzia Europea per la Sicurezza delle reti informatiche (ENISA) - 3.3 Le Nazioni Unite: una costante evoluzione di compiti - 3.3.1 Il ruolo della *General Assembly* in tema di *cyber security* - 3.3.2 Il ruolo del *Security Council* nel *cyberspace* - 3.3.2.1 Il mantenimento della pace e della sicurezza internazionale nell'era *cyber*: verso un'evoluzione del sistema di sicurezza collettiva? - 3.3.4 Il regime di sicurezza collettiva: un'analisi preliminare - 3.3.5 *Digital Blue Helmets* - 3.4 Il ruolo della NATO nel panorama cibernetico - 3.4.1 L'articolo 5 del Trattato del Nord Atlantico e le sue implicazioni - 3.4.2 La creazione di nuovi centri d'eccellenza per lo studio delle nuove sfide: il *Cooperative Cyber Defence Centre of Excellence*.

3.1 L'attività delle organizzazioni internazionali in tema di *cyber security*

Le organizzazioni internazionali sorgono a partire dalla seconda metà del XIX secolo come strumenti creati e messi a disposizione dagli stati per affrontare, in maniera congiunta, problematiche che vanno a toccare ciascuno di essi. In particolare, la nascita delle prime organizzazioni internazionali, di dimensioni incredibilmente inferiori rispetto a quelle attuali (è sufficiente pensare che solo le Nazioni Unite contano oggi quasi la totalità degli stati del mondo, arrivando addirittura a 191 membri), è dovuta essenzialmente alla necessità di affrontare e favorire, da un punto di vista prettamente economico, il commercio internazionale. Il fondamento delle stesse si deve accostare ad un concetto primordiale, ovvero quello di unione: le organizzazioni internazionali, infatti, si fondano su un'unione voluta da più soggetti per la realizzazione di un interesse comune. Esistono due tipologie di unioni: le unioni semplici e le unioni istituzionali. La differenza tra le stesse è che le prime sono unioni di stati che non danno vita ad un ente diverso dagli stati stessi che compongono l'unione. Dall'altra parte, le unioni istituzionali si contraddistinguono per la creazione di

un ente distinto dai soggetti che lo compongono, hanno obiettivi e organi propri, anche se non sempre viene garantita alle stesse la personalità giuridica.[326]

La forza delle organizzazioni internazionali risiede nella cessione, da parte dei singoli stati, di alcuni dei poteri appartenenti normalmente a questi ultimi. Come è possibile constatare, infatti, l'incapacità delle nazioni di soddisfare in maniera totalmente efficace alcune esigenze della popolazione, accomunata ad una capacità sempre maggiore delle organizzazioni internazionali di affrontare problemi congiunti, porta gli stati ad accettare una parziale perdita della propria sovranità in favore di un migliore raggiungimento degli obiettivi tramite un'attività coordinata[327]. Le organizzazioni internazionali sono, dunque, un'unione di due o più soggetti, che hanno una rilevanza da un punto di vista internazionale, che viene creata alla stregua dei requisiti di volontarietà, parità tra le parti e permanenza; le organizzazioni sono altresì dotate di personalità giuridica internazionale, avendo organi propri e specifici e svolgono solo e unicamente quelle tipologie di attività che sono necessarie per il raggiungimento dei fini per i quali l'organizzazione stessa viene creata.[328].

Accanto a questa prima definizione, è necessario riportarne una più completa, la quale può essere rinvenuta nell'art. 2 del "*Draft articles on the responsibility of international organizations*", il quale verrà meglio analizzato nel paragrafo conclusivo dell'elaborato, in tema di responsabilità statale[329]. Sulla base di quanto statuito dall'art. 2(a) per organizzazione internazionale si intende un'organizzazione istituita tramite un trattato o tramite altri strumenti di diritto internazionale, che gode di personalità giuridica. Viene inoltre stabilito come le organizzazioni internazionali possano avere, come membri, non solo gli stati ma

[326] Del Vecchio, A. (2012). *Diritto delle organizzazioni internazionali*. (pp. 22-231). Edizioni Scientifiche Italiane.

[327] *Ibid.*

[328] *Ibid*.

[329] United Nations. (2011). *Draft articles on the responsibility of international organizations*. Consultato da https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf

anche altre entità (come, ad esempio, altre organizzazioni internazionali)[330]. Il paragrafo c del suddetto articolo definisce organo dell'organizzazione internazionale qualsiasi persona od ente che ha quello status, ciò subordinato al rispetto delle regole dell'organizzazione, le quali vengono definite come l'insieme degli strumenti costitutivi, delle decisioni, delle risoluzioni e di tutti gli atti dell'OI adottati in accordo con quegli strumenti e con la ripetizione della pratica da parte dell'OI stessa[331].

L'attribuzione della soggettività giuridica alle organizzazioni internazionali è stata oggetto di ampio dibattito. Il caso fondamentale, che ha portato alla risoluzione del presente quesito, fu il caso "*Bernadotte*"[332]. Tramite la risoluzione del caso la Corte ha osservato che, per potere asserire la soggettività giuridica internazionale dell'OI, due requisiti devono essere presenti, soggettivi e oggettivi[333]. I requisiti soggettivi sono quelli che presuppongono uno studio di competenze, obiettivi e di una struttura che permetta all'OI di svolgere la propria attività in modo autonomo; questi elementi sono direttamente subordinati alle volontà degli stati membri, che sono state messe per iscritto tramite il trattato istitutivo. I requisiti oggettivi, invece, prevedono che le attività dell'OI che gode di soggettività giuridica internazionale possano concretizzarsi nella realtà. Di conseguenza, la soggettività giuridica internazionale delle OI, diversamente dalla personalità degli stati che è piena, è una soggettività funzionale, ovvero strettamente legata all'esercizio delle competenze che le vengono attribuite direttamente dagli stati membri[334].

La soggettività delle organizzazioni internazionale viene anche ripresa nel parere consultivo del 1980, relativo all'interpretazione di un accordo stipulato fra

---

[330] *Ibid.*

[331] *Ibid.*

[332] International Court of Justice (ICJ). (1949). *Reparation for injuries suffered in the service of the United Nations, Advisory Opinion: I.C.J.* Reports 1949. (Vedi p. 174).

[333] Focarelli, C. (2015). *Diritto internazionale*. Vicenza: Wolters Kluwer.

[334] *Ibid.*

l'Organizzazione Mondiale della Sanità (OMS) e l'Egitto, nel quale veniva affermato che l'organizzazione internazionale è un soggetto di diritto internazionale. Inoltre, proprio per questa caratteristica, è vincolata al rispetto di tutti gli obblighi e i principi che regolano il diritto internazionale, dal suo atto costitutivo e dagli accordi internazionali di cui è parte[335].

Accanto agli elementi strutturali comuni a qualsiasi organizzazione internazionale, per fornire una classificazione generale, è possibile suddividere le stesse in: universali, regionali, aperte e chiuse.[336]. Per raggiungere i propri obiettivi, le organizzazioni internazionali, sulla base del conferimento di poteri che normalmente rientrerebbero nelle prerogative dei singoli stati, hanno la possibilità di adottare una serie di atti che sono integralmente o parzialmente vincolanti, oppure senza effetti obbligatori[337].

Le organizzazioni internazionali sono dunque uno strumento fondamentale che viene messo a disposizione degli stati per raggiungere obiettivi comuni e necessari per ognuno, partendo da un presupposto collaborativo che riesce concretamente a portare, nella maggior parte dei casi, risultati più che positivi. I compiti delle varie organizzazioni internazionali si sono notevolmente evoluti nel tempo, passando da obiettivi standard, come la tutela e il mantenimento della pace, ad obiettivi sempre più impellenti ed attuali. Detta evoluzione viene eseguita in due modalità distinte: tramite la creazione di nuove organizzazioni internazionali con il compito di proteggere, tutelare e raggiungere un particolare obiettivo o tramite l'evoluzione interpretativa di quanto stabilito nello statuto (come avviene solitamente nel caso del *cyberspace*), o ancora tramite la creazione di organi sussidiari con compiti in materia.

---

[335] Loffredo, F. (2010). *Le persone giuridiche e le organizzazioni senza personalità giuridica. Manuale e applicazioni pratiche dalle lezioni di Guido Capozzi.* Terza edizione. Giuffrè Editore. (Vedi p. 23).

[336] Pustorino, P. (2012). *Lo status di membro delle organizzazioni internazionali*. In Diritto delle organizzazioni internazionali (pp. 141-204). Napoli: Edizioni scientifiche italiane.

[337] Virzo, R. (2012). *Gli atti delle organizzazioni internazionali. Diritto delle organizzazioni internazionali*. Edizioni Scientifiche Italiane.

Il tema della sicurezza cibernetica, così come definita nel primo capitolo, ha assunto per gli stati e per le organizzazioni internazionali un ruolo di sempre maggiore rilevanza. In particolare, il mondo della *cyber security* viene a identificarsi come un "ecosistema istituzionale", costituito da un assortimento complesso di soggetti di diritto internazionale distinti, tra i quali annoveriamo le organizzazioni nazionali, internazionali, intergovernative ed infine private[338]. Per la parte che interessa il seguente elaborato, è possibile asserire come le organizzazioni internazionali, sulla base dei cambiamenti degli ultimi 20 anni, si siano più volte trovate a dover rapportarsi con l'evoluzione derivante dall'avvento del cyberspazio.

In particolare, una delle prime organizzazioni internazionali che è andata a prendere in considerazione l'ambito relativo alle attività cibernetiche è stata senz'altro l'ONU, anche se ancora le attività dell'organizzazione in materia di sicurezza informatica risultano altamente frammentate, dal momento che il tema viene affrontato in molti dei suoi organi e tramite piattaforme organizzative distinte[339]. Su questa materia, l'attività dell'ONU si è esplicata prevalentemente tramite l'adozione di risoluzioni; nonostante diverse entità appartenenti all'organizzazione abbiano la possibilità di adottarle, nella realtà dei fatti sul tema le stesse sono state approvate solo dall'Assemblea Generale delle Nazioni Unite (UNGA) e, almeno per ora, nessuna dal Consiglio di Sicurezza (UNSC)[340]. La caratteristica peculiare di queste risoluzioni è che quasi tutte non risultano

[338] Choucri, N., Madnick, S., & Koepke, P. (2016, agosto). *Institutions for Cyber Security: International Responses and Data Sharing Initiatives.* Cambridge, MA: Sloan School of Management, Cybersecurity Interdisciplinary Systems Laboratory (CISL). Consultato da http://web.mit.edu/smadnick/www/wp/2016-10.pdf

[339] Maurer, T. (2011, settembre). Cyber norm emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security. *Discussion Paper, 2011-11, Science, Technology, and Public Policy Program.* Cambridge, MA: Belfer Center for Science and International Affairs. Consultato da https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security

[340] NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *United Nations.* Consultato da https://ccdcoe.org/organisations/un/

vincolanti per gli stati membri, ad eccezione quelle adottate dal Consiglio di Sicurezza.

La prima di una lunga serie di risoluzioni in tema di *cyber security* è senz'altro la risoluzione 53/70[341], adottata dall'Assemblea Generale su iniziativa della Federazione Russa. Con questa risoluzione, l'Assemblea constatava la necessità di ricercare meccanismi utili per cercare di mitigare i rischi derivanti da un uso malevolo delle *Information and Communication Technologies* (ICTs), per migliorare inoltre la cooperazione internazionale all'interno dello spazio cibernetico.

Accanto alla suddetta risoluzione, un'altra è stata adottata nel gennaio del 2001[342], e, anche se sarà meglio analizzata nel paragrafo dedicato espressamente alle Nazioni Unite, risulta particolarmente importante dal momento che riafferma con maggior vigore l'impellenza di una lotta contro l'uso illecito delle tecnologie dell'informazione. Inoltre, l'attività delle Nazioni Unite si esplica nell'importanza che viene riconosciuta all'operato effettuato prevalentemente da tre comitati dell'Assemblea Generale: il comitato per il Disarmo e la Sicurezza internazionale[343], il comitato Economico e Finanziario[344] ed il comitato Sociale, Umanitario e Culturale[345]. L'attività concretamente effettuata da questi comitati è quella relativa allo studio di possibili progetti per l'adozione di risoluzioni sui diversi aspetti della *cyber security*. Probabilmente, gli sviluppi più degni di nota si sono verificati in seno al primo comitato, il quale può essere considerato un

[341] United Nations General Assembly. (1999, 4 gennaio). *Developments in the field of information and telecommunications in the context of international security, UN Doc.* A/RES/53/70. Consultato da https://digitallibrary.un.org/record/265311#record-files-collapse-header

[342] United Nations General Assembly. (2001, 22 gennaio). *Combating the criminal misuse of information technologies, UN Doc.* A/RES/55/63. Consultato da https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[343] United Nations General Assembly. (n.d.). *Disarmament and International Security (First Committee).* Consultato da https://www.un.org/en/ga/first/index.shtml

[344] United Nations General Assembly. (n.d.). *Economic and Financial Committee (Second Committee).* Consultato da https://www.un.org/en/ga/second/index.shtml

[345] United Nations General Assembly. (n.d.). *Social, Humanitarian & Cultural Issues (Third Committee).* Consultato da https://www.un.org/en/ga/third/index.shtml

forum unico per attori "chiave" come la Cina, gli Stati Uniti o la Russia (particolarmente attiva da questo punto di vista) per discutere sulle varie minacce derivanti dalle attività cibernetiche[346].

Come visto antecedentemente, le organizzazioni internazionali sono altresì attive nell'ambito di tutela della sicurezza informatica, dal momento che possono istituire, come è avvenuto sempre in seno all'ONU o alla NATO, gruppi con compiti di ricerca e studio delle minacce esistenti a livello globale in tema di sicurezza, con la possibilità di prospettare possibili misure di cooperazione che potrebbero essere utili per affrontarle[347]. Accanto, di conseguenza, alle risoluzioni considerate ed alla possibilità di creare detti gruppi, le organizzazioni internazionali sono particolarmente attive per quanto riguarda il tentativo, come analizzato nel primo capitolo, di creare una base per la redazione di trattati internazionali che favoriscano la cooperazione e che siano in grado di trovare una disciplina unitaria e un'uniformità di visione tra gli stati, anche se, per il momento, nessuno di questi tentativi è andato buon fine[348].

Accanto all'ONU sono presenti moltissime altre organizzazioni internazionali che si sono trovate ad affrontare problemi relativi al mondo cibernetico. Oltre ad ENISA e alla NATO, che verranno trattate con precisione nei prossimi paragrafi, è possibile analizzare una serie di organizzazioni che hanno natura totalmente differente ma che svolgono simili attività: in particolare si tratta di organizzazioni che operano a livello universale, regionale o statale o ancora organizzazioni non governative.

Tra queste un ruolo di particolare rilevanza a livello regionale è affidato all'organizzazione denominata "*Association of Southeast Asian Nations*"

[346] Tikk-Ringas, E. (Cur.). (2012). *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*. ICT4Peace Foundation. Consultato da https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

[347] United Nations Office for Disarmament Affairs. (n.d.). *Group of Governmental Experts*. Consultato da https://www.un.org/disarmament/group-of-governmental-experts/

[348] Ruotolo, *op. cit*., p. 61.

(ASEAN)[349]. Quest'ultima è stata istituita a Bangkok l'8 agosto 1967 e si compone di 10 stati membri[350]; uno degli obiettivi primari è quello di garantire e promuovere concretamente la pace e la stabilità nell'area geografica considerata, garantendo il rispetto della giustizia e dello stato di diritto nelle relazioni tra i paesi delle regioni, aderendo inoltre ai principi della Carta delle Nazioni Unite[351]. Già a partire dalla fine degli anni 90', l'ASEAN ha incominciato a discutere sui temi connessi al mondo cibernetico, andandosi a focalizzare sui concetti di *cyber crime* a livello transnazionale e sulle nuove questioni di sicurezza cibernetica, totalmente distinte dalla sicurezza vista in maniera tradizionale fino a quel momento, arrivando a prospettare inoltre la creazione di squadre nazionali che siano in grado di rispondere alle emergenze informatiche[352]. Un elemento particolarmente importante, in grado di far capire la rilevanza che possono avere le organizzazioni internazionali in tema di cooperazione, è rappresentato dall'introduzione, da parte dell'ASEAN, del "*ASEAN regional forum*" (ARF), il quale si concretizza in riunioni annuali a cui partecipano non solo ed unicamente gli stati membri dell'organizzazione internazionale, ma anche stati esterni come China, Russia e Stati Uniti o anche organizzazioni internazionali regionali, come fatto dall'Unione Europea[353]. L'obiettivo e la rilevanza di questi incontri si evidenzia già nella relazione del primo incontro, avvenuto nel 1994, nel quale si sottolinea come la finalità sia quella di promuovere dialoghi e consultazioni costruttive su questioni politiche e di sicurezza, in grado di migliorare la tutela

[349] Association of Southeast Asian Nations (ASEAN). (n.d.). About ASEAN. Consultato da https://asean.org/asean/about-asean/

[350] Gli stati sono: Singapore, Filippine, Indonesia, Malesia, Thailandia, Brunei, Vietnam, Birmania, Laos, Cambogia.

[351] Association of Southeast Asian Nations, *op. cit.*, p. 119.

[352] NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Shanghai Cooperation Organisation*. Consultato da https://ccdcoe.org/organisations/sco/

[353] NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Association of Southeast Asian Nations.* Consultato da https://ccdcoe.org/organisations/asean/

degli interessi delle parti considerate[354]. L'importanza del tema della sicurezza cibernetica all'interno degli incontri "ARF" è stata rilevata per la prima volta nel 2012, anno in cui è stato prodotto il *"Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security"*[355], con il quale i partecipanti ribadiscono la necessità di intensificare ulteriormente la cooperazione regionale in materia di sicurezza e di utilizzo degli strumenti informatici attraverso una serie di misure: tra queste quelle più rilevanti sono relative alla promozione dell'esame delle strategie che possono essere apprestate per affrontare le incombenti minacce cibernetiche, nel rispetto del diritto internazionale e dei suoi principi fondamentali o ancora il rafforzamento della cooperazione nella promozione di una cultura di massa relativa alla sicurezza informatica.

Sempre da un punto di vista regionale, un'attività prospera in materia di sicurezza cibernetica è stata svolta dall'Organizzazione degli Stati Americani (OAS), nata nel 1945 con la ratifica della Carta dell'organizzazione[356]. Al fine di sostenere gli stati membri nella lotta alla *cyber* criminalità, l'organizzazione, tramite il comitato interamericano contro il terrorismo (CICTE) e l'adozione di un "*cyber security program*", si è impegnata a sviluppare e a promuovere l'agenda per l'implementazione della sicurezza informatica all'interno delle Americhe[357]. Cooperando, infatti, con un'ampia gamma di enti nazionali e regionali, sia del settore pubblico che privato, oltre che con altre organizzazioni internazionali, l'OAS cerca di costruire e rafforzare la capacità di sicurezza informatica negli stati membri fornendo assistenza tecnica e processi di

[354] U.S. Department of State. (Archivio 2001-2009). *Chairman's Statement: The First ASEAN Regional Forum Ministerial Meeting, Bangkok, Thailand, 25 July 1994.* Consultato da https://www.google.com/search?client=firefox-b-d&q=first+arf+statement+1994

[355] Association of Southeast Asian Nations. (2012). *2012 Asean Regional Forum Statement By The Ministers Of Foreign Affairs On Cooperation In Ensuring Cyber Security*. Consultato da https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf

[356] Organization of American States (OAS). (2021). *Who we are.* Consultato da http://www.oas.org/en/about/who_we_are.asp

[357] Organization of American States (OAS). (2021). *Cyber Security.* Consultato da https://www.oas.org/en/topics/cyber_security.asp

formazione che comprendono esercizi di gestione della crisi e scambio di informazioni relative alle migliori pratiche tecnologiche[358]. In particolare, il *cyber security program* comprende l'aiuto agli stati membri nello sviluppo di capacità tecniche e politiche per prevenire, identificare e rispondere con successo ad incidenti cibernetici, nonché il tentativo di aumentare la disponibilità e la facilità di accesso a conoscenze ed informazioni sulle minacce ed i rischi esistenti nel mondo cibernetico[359].

Le organizzazioni considerate fino a questo momento sono solo una parte delle innumerevoli organizzazioni che, in modi diversi, hanno cercato di svolgere un'attività rilevante in tema di *cyber* sicurezza. Sulla base di quanto detto finora, quello che è possibile constatare preliminarmente è come il livello di cooperazione tra le varie organizzazioni internazionali negli ultimi dieci anni sia stato implementato notevolmente. Sino a questo momento, tuttavia, l'attività delle stesse si è andata a focalizzare sull'adozione di risoluzioni, solitamente non vincolanti, relative alle materie considerate, con la creazione di organi sussidiari dell'organizzazione stessa, con compiti non direttamente "operativi" ma contraddistinti da caratteri ausiliari, in grado cioè di svolgere attività di studio delle nuove minacce nascenti e solo e unicamente di proporre ai vari stati possibili soluzioni, o ancora tramite tentativi (più volte proposti ma senza successo) di creare un'uniformità di visioni ed una possibilità per gli stati di affrontare allo stesso modo le minacce incombenti. Proprio quest'ultimo tema è alla base del seguente elaborato. In particolare, la possibilità di avere attacchi cibernetici che siano in grado di causare una minaccia od una violazione della pace internazionale lasciano presagire la necessità di avere strumenti in grado di

[358] *Ibid.*

[359] Organization of American States (OAS). (2021). *CICTE's Cybersecurity program.* Consultato da http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

contrastare suddetti attacchi utilizzando la stessa "arma" con cui sono scagliati: la forza cibernetica[360].

Le Nazioni Unite avranno su questo tema una particolare rilevanza e responsabilità dal momento che rappresentano l'unica organizzazione internazionale che si è occupata con forza, da un punto di vista dinamico, di affrontare le minacce che provengono quotidianamente dal mondo "offline", tramite anche la predisposizione di strumenti come le operazioni del mantenimento della pace le quali vengono definite nel seguente modo:

> «*Action undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers*»[361].

Sulla base della possibilità riconosciuta all'ONU di effettuare dette operazioni, è stato prospettato come, in futuro, potrebbe essere necessario ampliare il regime considerato andando ad includere, all'interno dello stesso, altre tipologie di operazioni che avranno un compito fondamentale nella tutela della pace nello spazio cibernetico: le *cyber peacekeeping operations*[362]. Per *cyber peacekeeping operations* si intende quanto segue:

> *«Action undertaken in cyberspace to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers».*[363]

La possibilità di introdurre un organo in seno all'ONU con dette funzioni, subordinato ad una decisione ed al controllo del consiglio di sicurezza, si

[360] Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications*, *114*, 70-87. Consultato da https://www.researchgate.net/publication/324704165_An_Introduction_to_Cyber_Peacekeeping

[361] De Coning, C., Aoi, C., & Karlsrud, J. (Cur.). (2017, 3 febbraio). *UN Peacekeeping doctrine in a new era.* Routledge. Consultato da https://cedricdeconing.net/2017/02/03/un-peacekeeping-doctrine-in-a-new-era/

[362] Robinson, *op. cit.*, p. 121.

[363] *Ibid.*

prospetterebbe come una misura assolutamente rilevante, la quale garantirebbe un grande passo avanti in tema di cooperazione internazionale. Anche se le caratteristiche generali di detto organo saranno analizzate con precisione nel successivo capitolo, la svolta che suddetta creazione riuscirebbe a garantire segnerebbe un cambiamento epocale nella lotta alle minacce considerate.

3.2 Le attività dell'UE in materia di *cyber security*: il ruolo dell'Agenzia Europea per la Sicurezza delle reti informatiche (ENISA)

L'evoluzione tecnologica e l'utilizzo sempre maggiore degli strumenti informatici nello svolgimento di attività quotidiane ha portato alla nascita di concreti problemi di sicurezza; mentre da un lato, infatti, le opportunità che vengono ogni giorno create sono sempre maggiori, dall'altro una serie di pericoli, molti dei quali precedentemente analizzati con particolare riferimento al tema di *cyber attacks*, hanno comportato un'impellente necessità di uniformità nell'affrontare gli stessi, non solo ed unicamente da un punto di vista prettamente statale. Quanto detto rappresenta anche un'urgenza per tutte quelle organizzazioni internazionali regionali o universali che ogni giorno si trovano ad affrontare le stesse problematiche. Per questi motivi, l'Unione Europea non ha potuto sottrarsi dalla predisposizione di una serie di strumenti che risultano necessari per affrontare con efficacia i problemi fino a qui considerati[364]. Lo sviluppo del tema della necessarietà di implementazione e adeguamento ai tempi correnti della *cybersecurity* si rafforza, all'interno dell'Unione Europea, a partire dagli attacchi *Denial of Service*[365] (DoS) effettuati contro istituzioni ed infrastrutture pubbliche e private dell'Estonia nel 2007[366]. Da quel momento ad

[364] Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Springer.

[365] Definizione di *Denial of Service*. Vedi nota 15.

[366] Schmidt, A. (2013). The Estonian cyberattacks. In Jason Healey (Cur.), *The Fierce Domain – Conflicts in Cyberspace 1986-2012* (pp. 174-193). Washington, D.C.: Atlantic Council.

oggi si sono verificati molti casi di alto profilo concernenti violazioni ed attacchi alla sicurezza informatica contro organismi dell'UE, come quelli effettuati contro la Commissione Europea, contro il Parlamento europeo e anche contro il servizio europeo per l'azione esterna (SEAE)[367]. È difficile, infatti, trovare oggi un'area in cui le tecnologie dell'informazione e della comunicazione non siano importanti, dal tema del *e-health*[368], del *cloud computing*[369] o degli *smart systems*. Prima di andare ad analizzare nel dettaglio il funzionamento dell'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), è necessario soffermarsi sulle strategie disposte dall'Unione Europea per far fronte ai pericoli che si materializzano nel mondo del *cyberspace*. In particolare, risale al 2013 la strategia per la sicurezza informatica dell'Unione Europea (CSSEU), la quale individua cinque aree di azione prioritarie volte a realizzare politiche correnti ed efficaci che aumentino le possibilità di fronteggiare con forza le minacce derivanti dall'incremento dell'uso di internet e delle reti informatiche[370]. Il punto cardine di queste cinque aree viene visto nell'adozione della direttiva sulle reti e sui sistemi d'informazione (NSI), adottata dal parlamento europeo nel

[367] Servizio Europeo per l'Azione Esterna (SEAE). Definizione: quest'organo europeo ha il compito di gestire "le relazioni diplomatiche dell'UE con altri paesi al di fuori dell'UE e conduce la politica estera e di sicurezza dell'Unione europea". Consultato da https://europa.eu/european-union/about-eu/institutions-bodies/eeas_it, Unione Europea sito ufficiale.

[368] Treccani. (2020). *E-health.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «Utilizzo di strumenti e servizi basati su tecnologie e comunicazioni informatiche nel corso di attività per la prevenzione, diagnosi, trattamento, controllo e gestione della pratica medica. In alcuni ambiti il termine indica l'infrastruttura elettronica in cui le informazioni sono gestite e comunicate al paziente e quella tra le strutture mediche stesse; in altri casi si riferisce all'esercizio delle cure a distanza (telemedicina), attraverso assistenza o monitoraggio del paziente fino all'effettiva esecuzione di interventi chirurgici robotizzati. Questioni particolarmente rilevanti riguardano la progettazione e l'uso delle infrastrutture per la condivisione dei dati in modo da garantire la piena accessibilità, l'interoperabilità a livello globale e la tutela del diritto alla riservatezza dei pazienti». Consultato da https://www.treccani.it/enciclopedia/e-health_%28Lessico-del-XXI-Secolo%29/

[369] Treccani. (2020). *Cloud computing.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «Letteralmente "nuvola informatica", termine con cui ci si riferisce alla tecnologia che permette di elaborare e archiviare dati in rete. In altre parole, attraverso internet il c.c. consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla workstation locale. Per le aziende di grosse dimensioni implica dunque un ingente abbattimento dei costi; non sono più necessari hardware potenti (costosi e soggetti a frequenti manutenzioni), ma basta una macchina in grado di far funzionare l'applicativo d'accesso alla nuvola». Consultato da https://www.treccani.it/enciclopedia/cloud-computing

[370] Christou, G. (2019). The collective securitization of cyberspace in the European Union. *West European Politics*, *42*(2), 278-301.

luglio del 2016. Questa è infatti la prima direttiva che mira a garantire una capacità istituzionale minima per segnalare gli incidenti informatici in tutti gli stati membri e fornisce quindi la possibilità di gestire concretamente i rischi che vengono associati agli attacchi informatici[371].

L'Agenzia dell'Unione europea per la sicurezza informatica, con sede a Candia in Grecia, si occupa del raggiungimento di un elevato livello comune di sicurezza informatica nel panorama europeo. ENISA è stata creata ed istituita ufficialmente il 13 marzo 2004 tramite il regolamento n.640/2004 dal Consiglio e dal Parlamento europeo[372], con il nome "*European network and security agency*". Anche se attualmente il regolamento a cui è necessario rifarsi è il n.881/2019[373], l'insieme delle attività e degli obiettivi che l'agenzia persegue è già definito tramite il regolamento del 2004, anche se ampiamente rinnovato dal regolamento precedentemente nominato e da una serie di regolamenti che sono andati con forza ad incidere sulle sue funzioni. L'agenzia contribuisce efficacemente alla politica informatica dell'Unione, ne rafforza l'affidabilità dei prodotti, dei servizi e dei processi con sistemi di certificazione della sicurezza informatica, collabora con tutti gli stati membri e rappresenta uno strumento fondamentale per l'Europa per fronteggiare le sfide che, da un punto di vista informatico, si presentano giorno dopo giorno[374]. Tramite, inoltre, la condivisione di conoscenze e l'attività di rafforzamento della consapevolezza relativa all'importanza delle materie trattate dall'agenzia, quest'ultima collabora con i suoi principali soggetti

[371] Commissione Europea. (2017, 4 ottobre). *Comunicazione Della Commissione Al Parlamento Europeo E Al Consiglio Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*. Consultato da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017DC0476&from=IT

[372] EUR-lex. (2004, 13 marzo). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance).* Consultato da https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0460

[373] EUR-lex. (2019, 17 aprile). *Regulation (Eu) 2019/881 Of The European Parliament And Of The Council Of 17 April 2019.* Consultato da https://eur-lex.europa.eu/eli/reg/2019/881/oj/

[374] ENISA. (2020). *About ENISA: The European Union Agency for Cybersecurity*. Consultato da https://www.enisa.europa.eu/about-enisa

interessati, con il fine di incrementare la fiducia nell'economia collegata e di rafforzare le forze delle infrastrutture dell'Unione, soprattutto per mantenere la sicurezza digitale della società e dei cittadini europei. Vivendo in un mondo iperconnesso, dove la possibilità di andare a causare danni inimmaginabili a stati e organizzazioni internazionali va di pari passo con l'evoluzione tecnologica, i criminali informatici (siano essi semplici individui o organizzazioni o addirittura stati) rappresentano una significativa minaccia per la sicurezza interna dell'Ue e per la sicurezza online dei suoi cittadini. La necessità di una tutela maggiore si è venuta ad amplificare, inoltre, sulla base della pandemia dovuta al COVID-19; le persone hanno infatti aumentato notevolmente la loro presenza *online,* non solo per mantenere meglio le loro relazioni interpersonali ma anche e soprattutto per esigenze lavorative e i criminali informatici, con maggior frequenza approfittando della situazione suddetta, hanno deciso di rivolgere spesso la loro "attenzione" in particolare sulle imprese che operano nel mondo del "*e-commerce*[375]" e del pagamento elettronico e su quelle che operano nel mondo sanitario. Anche per questo, l'attività di ENISA si esplica nell'istituzione di un vero e proprio centro di competenza in materia di sicurezza informatica, in grado di raccogliere e fornire consulenze tecniche indipendenti e assistenza agli stati membri dell'UE e agli stessi organismi dell'Unione[376].

Lo sviluppo dell'Agenzia è stato inoltre particolarmente complesso e il ruolo della stessa ha subito cambiamenti radicali durante tutta la sua evoluzione. Questi problemi si sviluppano già nel 2004, a partire dalla sua nascita, tenuto conto della base giuridica su cui l'agenzia è stata creata[377]. Inizialmente, la base giuridica che

[375] Treccani. (2020). *E-commerce.* Enciclopedie on line, Istituto della Enciclopedia Italiana: «Transazione e scambio di beni e servizi effettuati mediante l'impiego della tecnologia delle telecomunicazioni e dell'informatica (Internet, Intranet, personal computer, televisione digitale ecc.)». Consultato da https://www.treccani.it/enciclopedia/e-commerce

[376] ENISA. (2020, giugno). *A TRUSTED AND CYBER SECURE EUROPE. ENISA Strategy*. Consultato da https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

[377] Brun, L., & Bellanova, R. (2020). *The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity*. Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain.

riconosceva la possibilità concreta dell'istituzione di un'agenzia come quella considerata veniva a rifarsi all'interno dell'articolo 95 dell'allora Trattato della Comunità Europea (TEC)[378], rimpiazzato nel 2009 dal Trattato sul Funzionamento dell'EU (TFEU). Successivamente, i vari regolamenti hanno sempre trovato una base giuridica per l'operato dell'Agenzia all'interno dell'art.114 del TFEU[379] in alternativa all'art. 95 TEC. Nonostante la scelta dell'articolo in questione possa sembrare astrattamente priva di significato, utilizzare l'art. 95 come base giuridica per il regolamento istitutivo del 2004 ha causato notevoli problemi ed aspri dibattiti tra gli stati membri, disaccordo che è stato tuttavia annullato in seguito ad una decisione della Corte di Giustizia europea. Il caso da prendere in considerazione, nella spiegazione della legittimità del rimando all'art. 95, è il caso C-217/04[380]; all'interno dello stesso il Regno Unito contestava la validità dell'art. 95 come base giuridica del regolamento del 2004 che istituiva ENISA, argomentando che una migliore base per il regolamento suddetto fosse fornita dall'articolo 308 TEC, richiedendo di conseguenza l'annullamento del regolamento con successiva dissoluzione dell'apparato appena costituito. Le argomentazioni britanniche facevano leva sulle osservazioni che vedevano l'art. 95 TEC come solida base per l'armonizzazione delle leggi nazionali, non in grado tuttavia di legittimare l'istituzione di organi comunitari. Inoltre, ad ENISA veniva riconosciuto il compito di creare una cultura della sicurezza informatica tramite l'UE, competenza che veniva vista come eccedente rispetto a quelle che erano riconosciute dall'art. 95. Tuttavia, la risoluzione adottata dalla Corte di giustizia

[378] Official journal of the European Community. (2002). *Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community*, Brussels. C 325/1, Articolo 95. Consultato da https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12002E/TXT&from=FR

[379] Official Journal of the European Union. (2012). *Consolidated version of the Treaty on the Functioning of the European Union,* Brussels. C 115/47, Articolo 114. Consultato da https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

[380] Regno Unito. Parlamento e Consiglio. (2006, 2 maggio). *SENTENZA DELLA CORTE (Grande Sezione)*. Consult. da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62004CJ0217&from=EN

europea ha confermato la legittimità dell'art. 95 TEC come base giuridica per l'istituzione di ENISA; infatti, un cambiamento così radicale avrebbe avuto, come risultato, la modificazione del bilanciamento intercorrente fra il Parlamento europeo e il Consiglio Europeo[381].

La storia di ENISA, nonostante i suoi soli 16 anni di attività, si è contraddistinta per ampi problemi di operabilità e di complessità delle sue azioni. Le attività di ENISA sono raggruppabili in cinque macrocategorie. La prima di queste comporta il compito di responsabilizzazione della comunità europea: essendo la sicurezza informatica una responsabilità condivisa, non appartenente quindi soltanto alla giurisdizione esclusiva di un unico stato, l'organo svolge un ruolo fondamentale nello sviluppo della cooperazione in tema di sicurezza informatica, cercando di garantire la complementarietà degli sforzi comuni, esplorando le varie sinergie ed utilizzando in modo efficace ed idoneo le competenze e le risorse possedute. Per questo motivo è stata, inoltre, creata la mappa istituzionale dell'UE sulla sicurezza informatica a fini identificatori dei soggetti maggiormente interessati[382]. La seconda attività attiene alla creazione di una politica di sicurezza informatica, che risulta essere la pietra angolare del processo di trasformazione digitale che ha contraddistinto l'ultimo ventennio. La sicurezza informatica non deve di conseguenza essere limitata ad un gruppo di tecnici informatici specializzati ma deve andare a coprire tutti i settori della politica europea. La frammentazione, infatti, lascia ampio spazio ai criminali informatici ed impedisce una migliore capacità di controbattere alle minacce degli stessi. La terza attività coperta da ENISA riguarda la necessità di risolvere la frammentazione appena accennata, andando ad attuare una politica di cooperazione operativa; infatti, i *cyber attacks* non conoscono frontiere e tutti gli strati della società possono essere colpiti. Per questo l'Unione deve essere pronta ad una risposta ad attacchi anche su ampia scala, facendo leva sulla necessaria

[381] Brun, *op. cit.*, p. 126. (Vedi pp. 28-29).

[382] ENISA. (2020). *About ENISA - The European Union Agency for Cybersecurity: Towards a Trusted and Cyber Secure Europe.* Consultato da https://www.enisa.europa.eu/about-enisa

rapidità della risposta stessa, la quale è in grado di prevenire danni o, quantomeno, limitarli. La quarta attività fa leva sulla cooperazione vista come capacità di costruire e formare. Infatti, la domanda di competenze informatiche al giorno d'oggi supera notevolmente l'offerta. Per questo motivo compito di ENISA è anche quello di investire nella creazione di competenze e talenti a tutti i livelli, dal meno esperto al professionista informatico. Gli stessi investimenti però non devono essere limitati alla formazione ma devono altresì essere concentrati per garantire che tutte le diverse comunità operative possiedano capacità adeguate ad affrontare le minacce stesse. L'ultima attività, infine, che merita di essere analizzata fa riferimento alla diffusione della conoscenza; l'informazione e la conoscenza rappresenta la linfa vitale della sicurezza informatica. Per fare in modo che i professionisti che lavorano in ENISA siano concretamente in grado di affrontare le minacce che si ripercuotono nel panorama europeo con risultati soddisfacenti, è necessario che agli stessi venga messo a disposizione un processo di raccolta, sintesi, analisi, organizzazione di tutte le conoscenze in materia di sicurezza informatica. Tutte queste fasi sono inoltre conosciute e rese pubbliche all'interno dell'UE per rispettare quei principi che concretizzano l'attività dell'organo stesso. Tra questi principi è possibile annoverare il principio di trasparenza, di integrità, di responsabilità e di eccellenza[383].

Un ruolo di sempre maggiore importanza viene assunto dalla *European Defence Agency (EDA)*, istituita anch'essa nel 2004. Quest'organo dell'UE, di cui fanno parte 26 stati, ha il compito fondamentale di sostenere i progetti cooperativi di difesa europea e di offrire una piattaforma per i ministeri della difesa europei[384]. L'EDA ha tre differenti missioni che assumono una rilevanza particolare: sostenere lo sviluppo delle capacità di difesa e la cooperazione militare tra gli stati membri dell'UE, stimolare la ricerca, la tecnologia nel settore della difesa e

[383] Vedi nota 183.

[384] Unione Europea. (2020). *Agenzia europea per la difesa (AED).* Consultato da https://europa.eu/european-union/about-eu/agencies/eda_it

rafforzare l'industria europea della difesa ed infine ha il compito di fungere da interfaccia militare con le politiche dell'Ue[385]. Queste attività si sono andate inevitabilmente a scontrare con il mondo cibernetico. La strategia per la sicurezza informatica dell'Ue, pubblicata nel febbraio del 2013 e approvata dal Consiglio europeo nel giugno dello stesso anno, sottolinea che la " *Cyber security efforts in the EU also involve the cyber defence dimension*.[386]" andandosi ad esplicare nella realizzazione di cinque attività: sostenere lo sviluppo della capacità di difesa informatica degli stati in materia di "*Cyber Defence Policy Framework*"(CDPF), rafforzare la protezione delle reti di comunicazione, promuovere la cooperazione civile e militare fra le maggiori forze informatiche europee e il settore privato, favorire la formazione di esperti ed infine rafforzare la cooperazione con i *partner* internazionali che si occupano degli stessi temi.

3.3 Le Nazioni Unite: una costante evoluzione di compiti

L'ONU rappresenta al giorno d'oggi forse il tentativo maggiormente riuscito di cooperazione a livello internazionale.

Le Nazioni Unite nascono a partire dal 24 ottobre 1945, anno in cui la Carta istitutiva è stata ufficialmente ratificata da parte di Cina, Unione sovietica, Francia, Inghilterra e Stati Uniti[387], in seguito alla Conferenza di San Francisco. Tuttavia, quello che è possibile osservare è come i lavori preparatori, i quali portarono effettivamente ad una discussione con 50 stati del mondo durante la conferenza sopra nominata, sono stati effettuati antecedentemente alla conferenza e i principi fondamentali ai quali l'organizzazione ha l'obbligo di rifarsi, contenuti esplicitamente nella Carta ed obbligatoriamente accettati da tutti gli

[385] European Defence Agency. (2020). *Mission*. Consultato da https://www.eda.europa.eu/Aboutus/Missionandfunctions

[386] European Defence Agency. (2020, 7 agosto). *Cyber Defence*. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

[387] Kelsen, H. (2000). *The law of the United Nations: a critical analysis of its fundamental problems: with supplement* (Vol. 11). The Lawbook Exchange, Ltd.

stati che l'hanno ratificata, sono stati redatti principalmente dalle 4 superpotenze mondiali uscite vincitrici dalla seconda guerra mondiale[388].

Infatti, la conferenza principale che ha gettato le basi della Carta delle Nazioni Unite è senza dubbio la Conferenza di *Dumbarton Oaks*, la quale incominciò il 21 agosto 1944 e terminò il 7 ottobre dello stesso anno. Questa conferenza risultava limitata nel numero dei partecipanti: alla stessa parteciparono solo ed unicamente le quattro superpotenze (Stati Uniti, Russia, Cina, Inghilterra). In particolare, venne redatto un progetto che aveva ad oggetto la struttura, il ruolo e le responsabilità, le metodologie di voto ed infine il tema delle forze armate per il mantenimento della pace[389]. L'art. 7 della Carta statuisce quali siano gli organi fondamentali delle Nazioni Unite che si articolano in: un'Assemblea Generale, un Consiglio di sicurezza, un Consiglio economico e sociale, un Consiglio di amministrazione fiduciaria, una Corte di Giustizia internazionale e il segretariato[390]. I principi e le finalità, dall'altra parte, sono contenuti nell'art. 1, il quale stabilisce i quattro punti fondamentali che sono: il mantenimento della pace e della sicurezza da un punto di vista internazionale (con le relative attività ammesse per contrastare fenomeni che possano turbare la pace), lo sviluppo tra le nazioni di interazioni amichevoli, la promozione della cooperazione internazionale tra le varie nazioni da un punto di vista economico e sociale ed infine la creazione di un centro di coordinamento per l'attività fino a qui considerata.[391]

---

[388] Hilderbrand, R. C. (2001). *Dumbarton Oaks: the origins of the United Nations and the search for postwar security*. UNC Press Books.

[389] United Nations. (2020). *1944-1945: Dumbarton Oaks and Yalta.* Consultato da https://www.un.org/en/sections/history-united-nations-charter/1944-1945-dumbarton-oaks-and-yalta/index.html

[390] United Nations. (2006, 24 ottobre). *Charter of the United Nations and Statute of the International Court of Justice*. (Traduz. Italiana). (Originariamente pubblicato nel 1945). Consultato da https://www.admin.ch/opc/it/classified-compilation/20012770/200609120000/0.120.pdf

[391] *Ibid.*

3.3.1 Il ruolo della *General Assembly* in tema di *cyber security*

L'Assemblea Generale è stata il centro focale per decenni per i tentativi di negoziati diplomatici sulle tecnologie dell'informazione e dei suoi effetti reali e personali, tenuto conto del già citato principio di sovranità statale; di conseguenza risultava naturale che il *cyber* spazio prima o poi finisse tra i temi da trattare contenuti all'interno dell'agenda dell'Assemblea[392]. Fino ad oggi, la maggior parte delle discussioni, avvenute sul tema del "*Information and Communications Technology"* (ICTs) nel contesto della pace e della sicurezza internazionale, si sono svolte in seno al primo comitato dell'Assemblea Generale, impegnato nel disarmo e nella sicurezza internazionale[393]. Come già rilevato nel corso dell'elaborato, molto spesso l'attività dell'Assemblea Generale si è contraddistinta per la creazione di gruppi di esperti (GGE), aventi il compito di studiare ed indagare le nuove emergenze e minacce che, da un punto di vista internazionale, si sviluppano[394].

Nell'ambito del tema delle ICTs, le sfide poste dal rapido sviluppo delle minacce cibernetiche, dal momento che vanno a colpire non solo gli stati ma anche gli attori non statali, hanno portato ad un ampiamento del dibattito e ad un maggiore interesse per gli stati, i quali si sono impegnati notevolmente nello svolgimento dello dibatto stesso all'interno del comitato o di altri gruppi[395]. Lavorare tramite continui dibattiti con l'obiettivo di ottenere un ambiente tecnologico pacifico, aperto, sicuro, stabile ha permesso di generare alcuni risultati normativi di

[392] Kavanagh, C. (2018). IT and Cyber Capabilities as a Force Multiplier for Transnational Crime. In *Organized Crime and Illicit Trade* (pp. 37-77). Palgrave Macmillan, Cham.

[393] Kavanagh, C. (2017). *The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century.* United Nations Institute for Disarmament Research.

[394] Lewis, J., & Vignard, K. (2016). *Report of the International Security Cyber Issues Workshop Series.* United Nations Institute for Disarmament Research (UNIDIR), Center for Strategic & International Studies (CSIS). (pp. 4–7). Consultato da https://www.google.com/search?client=firefox-b-d&q=Report+of+the+International+Security+Cyber+Issues+Workshop+Series%E2%80%9D%2C+pp.+4%E2%80%937%2C

[395] Kavanagh, C., Maurer, T., & Tikk-Ringas, E. (2014). *Baseline Review: ICT-related Processes & Events: Implications for International and Regional Security (2011-2013)*. ICT4Peace Foundation. Consultato da https://ict4peace.org/wp-content/uploads/2017/11/Baseline-Review-2014-ICT-Processes-colprint.pdf

assoluta rilevanza[396] . Infatti, tramite queste discussioni del GGE (ad oggi sei), si è sviluppato inconsapevolmente un processo che aveva originariamente, come base iniziale, la prevenzione di una possibile corsa agli armamenti cibernetici; la discussione poi si è incanalata verso un dibattito più produttivo sulle norme che dovrebbero disciplinare l'attività degli stati e l'utilizzo delle armi nel cyberspazio[397]. Per quanto riguarda i risultati riportati da queste attività, è possibile analizzare come gli stessi abbiano portato ad una visione comune del gruppo, stante la quale il diritto internazionale, e di conseguenza la Carta delle Nazioni Unite, dovrebbero essere applicabili agli stati anche in materia cibernetica[398]. Oltre a questo, nei rispettivi *report* sono state redatti una serie di comportamenti non vincolanti che gli stati dovrebbero seguire nello svolgimento di attività cibernetiche. L'importanza e la rilevanza assunta dai GGE si esplica inoltre alla stregua dell'aumento del numero di partecipanti; il primo gruppo prevedeva la presenza di 15 esperti mentre l'ultimo è arrivato a contarne 25. L'aumento del numero di esperti rafforza l'idea che gli stati stessi hanno iniziato ad avvertire, sempre con maggiore impellenza, la necessità di trovarsi preparati per affrontare i problemi di questo tempo sempre più in via di sviluppo. A discapito del loro carattere non vincolante, le relazioni del gruppo di esperti hanno rappresentano uno strumento fondamentale per la creazione di una maggiore stabilità nel cyber spazio. Il compimento di detti incontri ha inoltre facilitato la nascita di iniziative effettuate a livello globale e regionale volte ad implementare la consapevolezza e la conoscenza intorno al tema[399].

Mentre il primo incontro, effettuato tra il 2004 ed il 2005, non ha portato concreti risultati, il secondo, tenuto tra il 2009 ed il 2010, ha segnato il primo grande passo in avanti in termini di riconoscimento delle minacce derivanti dal ICTs: in

[396]Maurer, *op. cit*., p. 116.

[397] *Ibid.*

[398] United Nations General Assembly. (2015, 22 luglio). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN Doc. A/70/174. Consultato da https://undocs.org/pdf?symbol=en/a/70/174

[399] *Ibid.*

particolare, è stato rilevato come vettori di dette minacce non siano solo ed unicamente criminali e gruppi terroristici ma possano essere anche gli stessi stati[400]. Inoltre, è stato sottolineato come la mancanza di un'uniforme visione relativa alle norme che disciplinano l'uso, per gli stati, delle ICTs stava creando una situazione di pericolosità elevata che avrebbe potuto portare ad incidenti gravi[401]. Il *report* si concludeva con una serie di misure di cooperazione per rispondere a queste sfide, andando a sottolineare l'importante ruolo del settore privato e della società civile, per raggiungere un ambiente sicuro e resiliente[402].

Tramite il *report* del 2012/2013 il gruppo ha confermato che le norme internazionali ma soprattutto i principi costitutivi della sovranità statale dovrebbero essere applicabili anche all'attività condotta dagli stati in tema di ICTs ed alla giurisdizione sulle infrastrutture ICTs che svolgono attività all'interno del rispettivo territorio[403]. Il *report* del 2014/2015, pur non avendo affrontato la discussione relativa ad un attacco cibernetico che raggiunge la valenza di un attacco armato, è risultato importante dal momento che, oltre a ribadire quanto analizzato all'interno dei precedenti, ha evidenziato gli impegni e i principi della Carta che gli stati dovrebbero garantire anche nel mondo cibernetico: l'uguaglianza sovrana, il principio di composizione delle controversie internazionali con mezzi pacifici, il principio di astensione dalla minaccia o dall'uso della forza contro l'integrità territoriale o l'indipendenza politica di qualsiasi stato ed il rispetto delle libertà fondamentali e dei diritti umani[404].

---

[400] United Nations General Assembly. (2010, 30 luglio). *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/65/201. Consultato da https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

[401] *Ibid*.

[402] *Ibid.*

[403] Vedi nota 342, United Nations General Assembly. (n.d.). *Economic and Financial Committee (Second Committee).*

[404] United Nations General Assembly. (2015, 22 luglio), *op. cit.*, p. 133.

Accanto all'attività svolta dai gruppi fino a questo momento considerati, una particolare rilevanza è stata assunta da una serie di risoluzioni dell'Assemblea Generale, le quali si sono occupate direttamente del tema della *cyber security*. La prima di queste risale al gennaio 2001 ed è la prima risoluzione adottata dall'Assemblea con cui vengono invitati gli stati a "combattere" e ad evitare un utilizzo sbagliato delle tecnologie informatiche[405]. Tramite la stessa, vengono invitati gli stati a adottare i comportamenti tipici contenuti all'interno della risoluzione, come per esempio evitare che le rispettive leggi diano possibilità di ottenere "rifugi sicuri" per coloro che abusano delle tecnologie dell'informazione o ancora cercare di facilitare la cooperazione e lo scambio tra stati di informazioni relativi alle modalità di lotta contro l'uso illecito delle predette tecnologie[406].

Con la seconda risoluzione, adottata nel gennaio del 2002, l'Assemblea Generale, oltre a riprendere la risoluzione dell'anno prima, ha invitato altresì gli stati a prendere in considerazione, nel momento dell'elaborazione da parte degli stessi della normativa statale e della prassi nazionale relativa all'uso improprio delle tecnologie dell'informazione, tutto il lavoro ed i risultati analizzati dalla "*Commission on Crime Prevention and Criminal Justice"* (CCPCJ)[407] o di altre organizzazioni internazionali universali o regionali[408].

È a partire tuttavia dal 2003 che inizia un processo di sviluppo di consapevolezza di una necessaria tutela a livello di *cyber security*, la quale è evidenziata, *in primis*, dalla risoluzione del 31 gennaio 2003[409]. In particolare, con la risoluzione vengono invitati non solo gli stati membri, ma anche tutte le altre organizzazioni

[405] United Nations General Assembly. (2001, 22 gennaio), *op. cit*., p. 117.

[406] *Ibid*.

[407]United Nations Office on Drugs and Crime. (2021). *Official Website*. Consultato da https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

[408] United Nations General Assembly. (2002, 23 gennaio). *Combating the criminal misuse of information technologies*", UN Doc. A/RES/56/121. Consultato da https://digitallibrary.un.org/record/454952

[409] United Nations General Assembly. (2003, 31 gennaio). *Creation of a global culture of cybersecurity*, UN Doc. A/RES/57/239.Da http://www.itu.int./ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

internazionali pertinenti a prendere in considerazione tutti gli elementi, che verranno di seguito analizzati, necessari per creare una cultura globale per la tutela della sicurezza informatica. Questa cultura globale, secondo l'Assemblea Generale, si dovrebbe base su nove elementi complementari:

1) Consapevolezza. Solo tramite la consapevolezza dei pericoli e delle minacce è possibile conoscere i migliori strumenti per migliorare la cyber security.
2) Responsabilità. Anche se il tema verrà trattato specificatamente al termine del successivo capitolo, gli stati che operano nel panorama cibernetico risultano responsabili della sicurezza dei sistemi e delle reti di informazione.
3) Risposta. La cooperazione e la condivisione di informazioni sulle minacce, esistenti e future, dovrebbero essere in grado di facilitare la consapevolezza per garantire la possibilità di adottare le migliori risposte in seguito ad incidenti che minacciano la sicurezza.
4) Etica. Gli stati dovrebbero comportarsi essendo consapevoli dei propri interessi legittimi, rispettando, tuttavia, gli interessi degli altri stati.
5) Democrazia. Lo svolgimento di attività informatiche per la tutela della sicurezza cibernetica deve essere sempre svolto seguendo una serie di principi riconosciuti in tutti gli stati democratici, come per esempio la libertà di pensiero, il libero flusso di informazioni o la riservatezza.
6) Valutazione dei rischi. Le valutazioni periodiche con il fine di individuare vulnerabilità ed eventuali nuove minacce dovrebbero essere fondamentali per garantire una sicurezza continua ed efficace.
7) Progettazione di una strategia di sicurezza. Come rilevato all'interno del capitolo relativo ad ENISA, il funzionamento e la tutela della sicurezza cibernetica dovrebbe essere subordinata all'attuazione di una strategia precisa.
8) Gestione della sicurezza.

9) Rivalutazione.[410]

Questi dovrebbero essere, secondo l'Assemblea Generale, gli elementi in grado di fornire una tutela effettiva ed efficace della sicurezza cibernetica.

Con la risoluzione del 30 gennaio 2004[411], è stato avanzato l'invito agli stati e alle varie organizzazioni internazionali a prendere in considerazione la tutela e la protezione delle infrastrutture informatiche critiche che assumono una particolare rilevanza. La tutela della sicurezza cibernetica delle stesse può essere implementata tramite la creazione di reti di allarme e di emergenza in grado di rilevare *cyber* vulnerabilità minacce o incidenti o ancora tramite attività di sensibilizzazione delle parti interessate, per comprendere la criticità che un eventuale attacco potrebbe causare all'infrastruttura considerata[412].

L'ultima risoluzione che merita di essere analizzata è la risoluzione del 2010[413]. Oltre a riaffermare quanto detto tramite le risoluzioni precedenti in tema di *cyber* sicurezza, l'Assemblea Generale invita le parti considerate a richiedere l'intervento di uno strumento predisposto alla valutazione degli sforzi compiuti a livello nazionale per proteggere le infrastrutture critiche di informazione, per valutare il livello di sicurezza informatica raggiunto ed evidenziare i settori in cui intervenire ulteriormente. Da un punto di vista di cooperazione internazionale, l'Assemblea invita inoltre tutti gli stati membri e le organizzazioni universali e regionali competenti in materia, i quali hanno sviluppato strategie per la sicurezza informatica e per la protezione delle infrastrutture critiche, a

[410] *Ibid.*

[411] United Nations General Assembly. (2004, 20 Novembre) *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* UN Doc. A/RES/58/199. Consultato da https://undocs.org/pdf?symbol=en/A/RES/64/211

[412] *Ibid*.

[413] United Nations General Assembly. (2010, 17 marzo). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, UN Doc. A/RES/64/211.1. Consultato da https://digitallibrary.un.org/record/672141

condividere le loro migliori pratiche e misure che potrebbero aiutare tutti gli stati ad implementare e migliorare le rispettive strategie di sicurezza informatica[414].

Infine, nel 2018 l'Assemblea Generale ha indetto l'istituzione di due nuovi processi di discussione nell'ambito della sicurezza informatica che si sono sviluppati a partire dal 2019 e termineranno alla fine del 2021. Accanto ad un nuovo gruppo di esperti governativi è stato istituito un "*Open-Ended Working Group*" (OEWG), cui tutti gli stati membri sono stati invitati a partecipare.[415] Sulla base della sua risoluzione fondante, l'OEWG si impegna nel tentativo di sviluppare norme, regole e principi di comportamento responsabile degli stati e delle possibili modalità di loro attuazione[416].

Di conseguenza, è possibile riassumere come l'attività dell'Assemblea Generale delle Nazioni Unite molto viva in termini di *cyber security*. In particolare, dall'inizio del secolo è stata avvertita la necessità di discutere su temi fino a questo momento considerati e di cercare, tramite gli strumenti messi a disposizione, di creare una visione comune a livello internazionale. Le difficoltà che però sono state riscontrate su questo punto fanno leva sulla mancata vincolatività delle risoluzioni dell'Assemblea Generale, cosa che invece non avviene per le risoluzioni del Consiglio di Sicurezza[417]. L'art.10 della Carta delle Nazioni Unite sancisce infatti che l'Assemblea Generale ha la possibilità solo ed unicamente di fare raccomandazioni, non aventi carattere vincolante, nei confronti degli stati membri o del Consiglio di sicurezza stesso, pur avendo la possibilità di discutere su qualsiasi questione o argomento rientrante nello statuto[418].

---

[414] *Ibid.*

[415] United Nations. (n.d.). *Open-ended Working Group*. Consultato da https://www.un.org/disarmament/open-ended-working-group/

[416] United Nations General Assembly. (2018, 11 dicembre). *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/73/27. Consultato da https://undocs.org/pdf?symbol=en/A/RES/73/27

[417] Benedetto, C., & Carlo, F. (2000). *Le Nazioni Unite*. Padova: Cedam. (Vedi p. 192).

[418] *Ibid.*

3.3.2 Il ruolo del *Security Council* nel *cyberspace*

Oltre ai diversi organi dell'Assemblea Generale che si sono concentrati nello studio del mondo cibernetico e delle minacce che comporta nel contesto di pace e sicurezza internazionale, molti stati membri si aspettano che il Consiglio di Sicurezza svolga un ruolo "più forte" sulle questioni relative alla sicurezza informatica[419]. Quello che rileva in questo studio è che il CdS non ha ancora tenuto un dibattito formale sull'impatto delle tecnologie dell'informazione e della comunicazione che siano in grado di compromettere il mantenimento e la stabilità della pace internazionale; dall'altra parte, il tema è stato trattato in maniera informale e nell'ambito di una discussione più ampia[420].

Fino ad adesso si registrano solo due discussioni del Consiglio di Sicurezza tenute, tuttavia, tramite la modalità che si riconduce all'Arria-formula[421]: questi incontri Arria-formula del CdS sono contraddistinti da un ampio grado di informalità e sono convocati su iniziativa di uno o più membri del Consiglio per ascoltare le opinioni di persone, di organizzazioni, o di istituzioni su questioni di competenza del CdS[422]. Nel novembre del 2016 Spagna e Senegal hanno convocato un incontro con la formula predefinita per parlare di "*Cybersecurity and International Peace and Security"* mentre l'iniziativa del 2017 è stata proposta dall'Ucraina, consistente nella trattazione del tema di "*Hybrid Wars as*

[419] United Nations Institute for Disarmament Research (UNIDIR). (2017). *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century.* Consultato da https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

[420] Security Council Report. (2020, gennaio). *Monthly Forecast.* Consultato da https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/2020_01_forecast.pdf

[421] Security Council Report. (2020, 16 dicembre). *Arria-Formula Meetings*. Consultato da https://www.securitycouncilreport.org/un-security-council-working-methods/arria-formula-meetings.php

[422] *Ibid.*

a Threat to International Peace and Security", durante il quale i temi relativi alle minacce cibernetiche sono stati trattati[423].

Nel primo incontro è stato constatato come contrastare gli attacchi informatici possa essere particolarmente impegnativo a causa, tra gli altri fattori, della velocità con cui vengono scagliati e della difficoltà di stabilire la rispettiva fonte e di seguito la responsabilità per gli stessi. I membri del Consiglio inoltre sono stati incoraggiati a valutare le vulnerabilità e la possibilità di creare strumenti in grado di prevenire gli attacchi informatici, cercando di aumentare la cooperazione in seno alle varie strategie e politiche nazionali, nonché favorendo la formazione di partenariati fra governi, imprese, organizzazioni regionali o subregionali[424].

L'incontro invece del 2017 sulle guerre "ibride" è andato a toccare un'ampia gamma di temi relativi agli interventi ostili. Sulla base della nota apportata al termine della riunione, è stato analizzato, come, nel compimento di suddette attività, sia compreso l'utilizzo di sistemi avanzati di armi, *cyber attacks*, attività quasi militari, operazioni di *intelligence* segreta e di abuso e manipolazione degli strumenti informatici disponibili[425]. A livello di organi ausiliari del CdS, ci sono state discussioni relative alle minacce informatiche. Un esempio che può essere riportato è la riunione speciale tenuta nel 2016 dal comitato antiterrorismo sulla prevenzione dello sfruttamento delle nuove armi informatiche per scopi terroristici.[426]

Infine, è possibile constatare come il CdS non abbia mai, fino a questo momento, affermato che un attacco cibernetico, così come indicato dalla rule 30 del Tallinn Manual, sia in grado di arrivare ad un livello di minaccia o violazione della pace

[423] Security Council Report. (2019, 23 dicembre). *In Hindsight: The Security Council and Cyber Threats.* Consultato da https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php

[424] *Ibid.*

[425] *Ibid.*

[426] *Ibid.*

e della sicurezza internazionale, non solo non essendosi mai espresso ma soprattutto non essendosi mai riunito formalmente per discutere questo tema. Dichiarazioni molto forti, tuttavia, sono state fornite dal Segretario generale António Guterres, il quale, intervenendo durante l'annuale workshop "*Hitting the Ground running*", in quel caso tenuto in Finlandia nel 2017, ha evidenziato come la guerra informatica sia diventata una minaccia di primo ordine per la pace e la sicurezza internazionale, sottolineando come un *"massive cyberattacks could well become the first step in the next major war*", ribadendo la necessità che il CdS concettualizzi il suo ruolo nell'anticipare, prevenire e, se necessario, rispondere a tali minacce[427].

3.3.2.1. Il mantenimento della pace e della sicurezza internazionale nell'era *cyber*: verso un'evoluzione del sistema di sicurezza collettiva?

Partendo anche da un'analisi di queste parole, è possibile constatare come sempre più necessaria ed impellente sia la ricerca di una metodologia per fare fronte, comunemente e a livello internazionale, alle continue minacce che hanno la capacità di turbare la pace e la sicurezza internazionale[428]. Accanto ad una indefettibile urgenza di avere più di un "semplice" incontro informale da parte del Consiglio di Sicurezza, uno strumento congiunto in grado di prevenire, limitare o rispondere a tali minacce potrebbe essere rappresentato dalla creazione del *cyber peacekeeping team* tanto prospettato, strumento che sarebbe in grado di ampliare in maniera eccellente la cooperazione a livello internazionale ma che è ancora molto lontano dall'essere creato[429]. Sulla base della legittimità da parte del CdS di decidere in tema di utilizzo delle normali attività di *peacekeeping*, si potrebbe riscontrare altresì la legittimità delle azioni suddette su una base

[427] United Nations Security Council. (2018, 3 maggio). *Letter dated 30 April 2018 from the Permanent Representative of Finland to the United Nations addressed to the President of the Security Council*, UN doc. S/2018/404. Consultato da https://undocs.org/S/2018/404.

[428] Christou, *op. cit.,* p. 124.

[429] Almutawa, *op. cit.*, p. 27.

analogica, solo ed unicamente in seguito ad una vera e propria dichiarazione, disposta dal CdS riunitosi formalmente, della capacità degli attacchi cibernetici di assurgere al rango di atti in grado di minacciare o violare la pace e la stabilità internazionale[430].

Infine, il lavoro creato dal gruppo di esperti che hanno redatto il Manuale di Tallinn 2.0 ha portato ad un'analisi, contenuta nel capitolo 15, relativa alla difesa collettiva. Si tratta ovviamente, come già rilevato antecedentemente, di un tentativo posto in essere dal gruppo di esperti, i quali, sulla base delle loro opinioni, hanno cercato "semplicemente" di raccogliere la normativa che dovrebbe essere osservata nel panorama internazionale in materia di *cyber space*. In questa sezione, quello che si evidenzia è come la *Rule 76* del Manuale vada ad ipotizzare la possibilità, nel caso in cui il CdS ritenga che una *cyber operation* assurga al rango di minaccia o di violazione della pace o, ancora, di aggressione, di autorizzare una serie di misure che non prevedano l'uso della forza, includendo, tra le stesse, una serie di operazioni cibernetiche[431]. Al tempo stesso, però (l'argomento verrà meglio approfondito nel successivo capitolo), nel caso in cui il Consiglio stesso dovesse ritenere inadeguate le misure anzidette, dovrebbe avere la possibilità di utilizzare misure cibernetiche implicanti l'uso della forza[432]. Sulla base, infatti, di quanto stabilito all'art.39 della Carta delle Nazioni Unite, rientra, senza dubbio, tra le funzioni devolute al CdS la possibilità di determinare se una *cyber operation* rientri all'interno di quei casi che abilitano il Consiglio a adottare misure di risposta[433]. Ciò nonostante, mai si è arrivato a tanto, non avendo in realtà l'organo nemmeno mai discusso formalmente sul tema. Tuttavia, nel caso in cui venisse determinato che un'operazione cibernetica abbia portato ad una minaccia o violazione della pace, al CdS spetterebbe la possibilità decidere quali misure adottare tra quelle rientranti in misure non

[430] Robinson, *op. cit*., p. 121.

[431] Jensen, E. T. (2016). The Tallinn Manual 2.0: Highlights and Insights. *Geo. J. Int'l L., 48*, 735.

[432] *Ibid.*

[433] Schmitt, *op. cit*., p. 64.

implicanti l'uso della forza, la cui natura è determinata in maniera non esaustiva all'interno dell'art. 41, oppure tra una serie di misure implicanti l'uso della forza, la cui legittimità è sancita all'art. 42[434]. Nel primo caso, la previsione contenuta all'art. 41, relativa all'adozione di misure che includono l'interruzione completa o parziale di, tra le altre, posta, telecomunicazione, radio od altri mezzi di comunicazione, diviene particolarmente importante per far rientrare, tra le competenze del Consiglio, anche la possibilità di adottare misure cibernetiche che comportino l'interruzione, in maniera totale o parziale, delle comunicazioni da un punto di vista cibernetico. Nel caso invece in cui il CdS ritenga che le misure considerate, a causa della loro inadeguatezza, non siano in grado di raggiungere gli obiettivi prefissati, dovrebbe avere la possibilità di adottare misure comprendenti l'uso della forza, includendo, tra le stesse, l'utilizzo di mezzi informatici.

Per capire meglio questo tema, il gruppo di esperti ha riportato il seguente esempio: nel caso in cui uno stato abbia sviluppato e continui a sviluppare pericolose armi nucleari, ignorando le richieste di terminare lo svolgimento del progetto da parte del Cds, il quale, conseguentemente, adotti una delle misure non implicanti l'uso della forza disciplinate dall'art. 41, e ciò nonostante la richiesta di sospensione delle attività dovesse rimanere inascoltata, il medesimo CdS dovrebbe avere la possibilità di autorizzare gli stati membri alla conduzione di operazioni cibernetiche, comprendenti l'uso della forza, per distruggere il programma di creazione delle armi[435].

3.3.4 Il regime di sicurezza collettiva: un'analisi preliminare

Come evidenziato, il capitolo 15 del Tallinn Manual fa riferimento alla disciplina applicabile al tema della sicurezza collettiva. Accanto agli stati, come analizzato

[434] *Ibid*., (pp. 357-359).

[435] *Ibid*., (p. 360).

tramite la Rule 77, il CdS avrebbe la possibilità di devolvere l'esecuzione delle stesse operazioni, subordinata all'emissione di un mandato o di un'autorizzazione, ad organizzazioni internazionali o ad agenzie internazionali regionali. La regola qui analizzata è prevista dalle disposizioni contenute nella Carta delle Nazioni Unite ai capitoli VI e VII. Mentre, inoltre, è pacificamente ammessa la possibilità, per un'organizzazione internazionale regionale, di intraprendere azioni che non comportano l'uso della forza di cui all'art. 41 della Carta senza un'espressa autorizzazione del CdS, nel contesto delle operazioni cibernetiche non risulta ancora chiaro se la stessa organizzazione possa intraprendere le attività di cui all'art. 42 senza l'autorizzazione considerata[436]. Il termine "regionale", contenuto nella *Rule 77,* viene ripreso da quello dell'art.52 della Carta, nel quale viene esplicato che le agenzie che hanno la possibilità di svolgere le suddette operazioni rientrano tra i sistemi regionali di sicurezza collettiva, i quali sono appropriati ed efficaci per l'azione regionale. Come rilevato nel Manuale, la qualifica di ente o ente regionale non è chiara; tuttavia, detta qualificazione come organizzazione regionale risulta del tutto irrilevante, dal momento che il CdS ha la possibilità di autorizzare un qualsiasi gruppo di stati, indipendentemente dalla collocazione geografica degli stessi[437], all'adozione di misure che comprendono l'uso della forza. Il termine inglese di "*enforcement actions*" deriva dal potere, conferito al CdS di autorizzare o incaricare stati o organizzazioni internazionali regionali di adottare misure non coercitive o comprendenti l'uso della forza per ristabilire e mantenere la pace e la sicurezza internazionale[438]. Queste tipologie di attività, che comprendo anche la conduzione di operazioni cibernetiche, vengono a tutti gli effetti distinte dalle azioni di autodifesa collettiva, effettuate dalle agenzie regionali.

[436] *Ibid.*

[437] *Ibid.*

[438] *Ibid.*

Prima di evidenziare la *Rule 78*, potrebbe essere utile fornire un esempio di attività di autodifesa collettiva come reazione a seguito di un *cyber attack* tramite un'organizzazione internazionale regionale. L'art. 51 della Carta, infatti, contempla anche la possibilità di avere un'autodifesa collettiva, non solo singola. I problemi che derivano in questo senso sono stati imputati ad un'eventuale attività della NATO; in particolare, ci si è chiesti come l'art.5 del trattato istitutivo delle NATO, che ammette la possibilità di avere un'attività di autodifesa collettiva, sia ricollegabile all'art. 51 della Carta delle Nazioni Unite anche se l'attacco sferrato è di tipo cibernetico[439]. Come analizzato dallo studioso Marco Roscini, l'espressione "attacco armato" nell'autodifesa collettiva di cui all'art. 5 dovrebbe essere interpretata come legittimamente relazionata all'art. 51 per due motivi. Il primo fa leva sull'interpretazione evolutiva dei trattati, già ripresa nel primo capitolo, relativamente a quanto espresso dall'art. 31(3)(c) della Convenzione di Vienna, nel quale è sancito che i trattati internazionali dovranno essere interpretati tenendo conto di qualsiasi regola di diritto internazionale applicabile nelle relazioni tra parti: la consistenza dell'art.5 della NATO con l'art. 51 della Carta si esplica soprattutto per il fatto che quest'ultima risulta essere la matrice dei trattati di autodifesa collettiva, come viene riconosciuto dallo stesso art. 5[440]. Il secondo motivo è che il trattato delle NATO contiene espressamente una "clausola di subordinazione", la quale prevede l'obbligo di rispetto della Carta delle Nazioni Unite[441]. Accanto a questo, quello che è possibile constatare è che, anche nel caso in cui uno dei requisiti sopra delineati venga a mancare, il rispetto della Carta viene generalmente riconosciuto tramite l'art. 103 della stessa, la quale stabilisce che, nel caso di conflitto tra le obbligazioni assunte dagli stati membri derivanti dalla Carta e le obbligazioni derivanti da altri accordi internazionali, quelli derivanti dalla Carta dovrebbero prevalere. Quanto asserito porta a concludere che l'attacco armato di cui all'art. 5

[439] Roscini, *op. cit.*, p. 6.

[440] *Ibid.*, (p. 96).

[441] *Ibid*., (p. 97).

ha lo stesso campo di applicazione dell'art. 51; di conseguenza, il regime di sicurezza collettiva rappresentato da un'autodifesa non individuale risulta a tutti gli effetti ammessa anche nel caso di compimento di operazioni informatiche[442].

Infine, anche se il tema sarà meglio sviluppato nel prossimo capitolo, il Manuale di Tallinn prevede la possibilità di avere operazioni di mantenimento della pace che abbiano carattere cibernetico, esattamente come avviene per le operazioni dinamiche. Lo svolgimento di tali tipologie di *peace operations*, come infine evidenziato dalla *Rule 78*, dovrebbe essere subordinato, oltre che al rispetto dei limiti imposti dal mandato e dai controlli del CdS, al rispetto dei principi del diritto internazionale applicabili in materia[443]. La base giuridica per poter effettuare le operazioni considerate coinciderebbe totalmente con quella prevista per le classiche operazioni di mantenimento della pace; i fini sarebbero gli stessi ma le attività avrebbero una natura totalmente differente. Le operazioni considerate nel Manuale si rifanno alla classica distinzione intercorrente fra le "*peacekeeping operations*" e le operazioni di "*peace enforcement*"[444]. Infine, sarà analizzata anche la *Rule 79*, la quale evidenzia come tutto il personale delle Nazioni Unite, il quale è adibito alla protezione dei civili, nello svolgimento delle proprie attività dovrà essere tutelato e protetto anche dagli attacchi cibernetici[445] . Accanto alla protezione del personale, dovrà essere garantita anche una protezione alle varie installazioni, ai materiali e ai veicoli del personale; da un punto di vista cibernetico, detta tutela dovrà esplicarsi anche nei confronti dei sistemi e delle reti cibernetiche create dalle forze considerate.

[442] *Ibid.*

[443] *Ibid.*, (p. 361).

[444] Tharoor, S. (1995). The changing face of peacekeeping and peace-enforcement. *Fordham Int'l LJ*, *19*, 408.

[445] Schmitt, *op. cit.*, p. 64. (Vedi p. 368).

3.3.5 *Digital Blue Helmets*

Nel 2016 è stato lanciato dalle Nazioni Unite un programma del tutto particolare sotto l'ufficio che si occupa di informazioni e comunicazioni tecnologiche (OICT): il "D*igital Blue Helmets program*". Pur non essendo esattamente un vero e proprio organo con le classiche funzioni di *peacekeeping* come fino a quel momento inteso, è possibile asserire come sia senza dubbio quello che maggiormente si avvicini a quell'idea.

All'interno del sito ufficiale dell'ONU, la *brochure* dei *Digital Blue Helmets* contiene una definizione degli stessi come un *team* di professionisti della sicurezza informatica competenti e preparati, specializzati nel monitoraggio di eventi, test ambientali, analisi forense digitale ed operazioni informatiche[446]. La nascita di questo programma, che ha come obiettivo principale la tutela e la sicurezza informatica dei siti istituzionali dell'ONU e l'aiuto per un miglioramento delle difese cibernetiche per i paesi che ne fanno parte, è dovuta ad una serie di eventi la cui risoluzione, già nel 2016, risultava particolarmente impellente. Si tratta di uno strumento volto, almeno in parte, a far fronte alle minacce che da un punto di vista cibernetico vanno ad annidarsi nelle singole sfaccettature del mondo reale. Si parla infatti di paure fisiche, come quella relativa all'utilizzo di energia nucleare, o ancora economiche, come la minaccia per il furto di carte di credito o di conti bancari, o anche personali, come per esempio la raccolta di impronte digitali utilizzate illegittimamente. Compito dei *Digital Blue Helmets* è quindi quello di proteggere le Nazioni Unite da queste minacce cibernetiche, prevenendole, individuandole e, nel caso in cui si siano verificate, cercando di limitarne il più possibile i danni causati[447]. Le minacce cibernetiche possono verificarsi in tutti i settori in cui normalmente le Nazioni Unite svolgono le proprie attività; è infatti possibile avere attacchi cibernetici ai

[446] Office of Information and Communication Technology. (n.d.). *Digital Blue Helmets*. Consultato da https://unite.un.org/digitalbluehelmets/sites/unite.un.org.digitalbluehelmets/files/docs/digitalbluehelmets_brochure_final.pdf

[447] *Ibid.*

sistemi di distribuzione delle varie catene alimentari, alle reti di approvvigionamento o ai mercati adibiti allo scambio di merci, o ancora minacce che comportano *cyber* bullismo o lo sfruttamento minorile[448]. Le minacce si possono riverberare anche e soprattutto tramite violazioni dei diritti umani. Uno dei motivi principali per cui i *DBH* sono stati creati è la lotta continua al *dark web*, all'interno del quale non solo ed unicamente viene favorito il traffico di sostanze stupefacenti (la cui vendita porta un ricavo stimato tra i 100 e i 180 milioni l'anno), ma anche il traffico di esseri umani. Compito fondamentale dei *DBH* è quello di riuscire a creare quello che potrebbe essere semplicemente definito come *"the light web"*[449].

Per i primi anni, il programma *DBH* si è concentrato prevalentemente sul tema della criminalità cibernetica e sul mercato informatico. Essendo sfide prive di confini e delimitazioni geografiche, accanto al ruolo fondamentale di protettore delle strutture dell'ONU, i *DHB* mirano a coinvolgere tutti i soggetti di diritto internazionale[450]; in seguito infatti ad una costante interazione, in particolar modo con il segretariato, continui rapporti sono intrattenuti con gli stati membri, con soggetti esterni come organizzazioni non governative, con particolare riferimento al coinvolgimento del settore pubblico e privato. Il reclutamento per il *DBH program* ebbe inizio nel febbraio 2016. Il programma aveva come base la fornitura di una piattaforma nodale per lo scambio di informazioni e per il coordinamento delle misure di difesa da attuare contro incidenti in grado di minare la sicurezza delle infrastrutture dell'ONU e delle sue varie agenzie.

---

[448] United Nations Digital Blue Helmets. (2020). *Activities.* Consultato da https://unite.un.org/digitalbluehelmets/activities

[449] Nabeel, F. (2020). Cyber Peacekeeping: Critical Evaluation of Digital Blue Helmets Program. *NUST Journal of International Peace and Stability*, 3(2), 17-27. Consultato da https://www.researchgate.net/publication/343224548_Cyber_Peacekeeping_Critical_Evaluation_of_Digital_Blue_Helmets_Program

[450] Akatyev, N., & James, J. I. (2017, giugno). United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping. In *European Conference on Cyber Warfare and Security* (pp. 8-16). Academic Conferences International Limited. Consultato da https://arxiv.org/abs/1711.04502

Nonostante la sua nascita sia essenzialmente recente, valutare la capacità e la funzionalità di questo programma risulta, per i soggetti esterni, particolarmente difficile e complicato poiché i resoconti relativi all'attività sono molto limitati. Questo avviene per due motivi distinti: in primis, i DHB devono mantenere sempre un alto livello di segretezza per quanto riguarda le proprie operazioni interne (cosa che avviene, in generale, in tutte le agenzie di *intelligence*), mentre il secondo riguarda la mancata elasticità, per sua natura, del mandato istitutivo[451]. Proprio quest'ultimo punto risulta cruciale per valutare l'impossibilità di classificare il DHB *program* come un programma che statuisce un *cyberpeacekeeping team*.

Infine, nel lungo periodo, è stata ipotizzata l'evoluzione dei compiti e dei campi di intervento da parte del DHB in 8 grandi misure[452]: la costruzione di una difesa unitaria per le Nazioni Unite contro qualsiasi minaccia esterna, l'arricchimento delle potenzialità delle difese nazionali di sicurezza informatica per i vari stati membri, mitigare gli effetti di possibili vulnerabilità "*zero-day*"[453], favorire la nascita di nuove norme in materia di sicurezza informatica, promuovere le identità digitali ed incoraggiare il passaggio alla biometrica, aumentare l'utilizzo della crittografia nello scambio di messagistica, combattere il traffico illecito online ed infine migliorare le capacità dell'ONU di adempiere i suoi mandati tramite l'utilizzo delle nuove tecnologie.

[451] Nabeel, *op. cit.*, p. 148.

[452] *Ibid.*

[453] Chivers, K. (2019, 28 agosto). *Zero-day vulnerability: What it is and how it works.* Consultato da Security Center https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html Definizione: Il termine "zero-day" si riferisce ad una vulnerabilità del software appena scoperta. Non avendo lo sviluppatore stesso previsto detta possibilità, non esiste nessun aggiornamento disponibile per risolvere il problema. Di conseguenza, il termine si riferisce al fatto che gli sviluppatori hanno "zero giorni" per risolvere il problema che è appena sorto e che probabilmente è già stato sfruttato dagli hacker.

3.4 Il ruolo della NATO nel panorama cibernetico

La "*Nord Atlantic Treaty Organization"* (NATO) rappresenta una delle manifestazioni più conclamate della capacità delle organizzazioni internazionali di cambiare e modificarsi nel corso del tempo. Quest'organizzazione nasce ufficialmente tramite la firma del trattato del nordatlantico il 4 aprile 1949, trattato che venne ratificato da 10 stati europei, oltre alla firma apportata da Stati Uniti e Canada[454]. Al giorno d'oggi conta ben 30 paesi membri[455] che l'hanno ratificato e che sono impegnati nel mantenimento della sicurezza interstatale e nell'attuale e impellente lotta al terrorismo, anche se lo scopo iniziale dell'organizzazione risultava essere differente.

Sin dalla sua nascita, lo scopo principale della NATO è stato solo quello di rispondere alla minaccia proveniente dalla vecchia URSS, anche se questo è solo parzialmente vero. Infatti, la creazione di questa alleanza militare faceva parte di uno sforzo più ampio, subordinato al raggiungimento di tre scopi distinti: scoraggiare l'espansionismo sovietico, impedire la rinascita di un militarismo nazionalista in Europa tramite una costante presenza nord-americana all'interno del continente ed infine incoraggiare un'integrazione politica europea[456]. Le conseguenze della Seconda guerra mondiale videro l'Europa devastata in un modo che risulta difficile anche solo da immaginare, a distanza di 70 anni. Per questo fu avvertita una duplice necessità, la quale è alla base dell'attività dei primi 30 anni della NATO: la ricostruzione dell'economia (tramite il cosiddetto piano Marshall)[457] e il mantenimento della sicurezza. Questo secondo punto

[454] Duignan, P. (2000). *NATO: Its Past, Present, Future*. Hoover Press.

[455] Questi 30 paesi sono: Belgio (1949), Canada (1949), Danimarca (1949), Francia (1949), Islanda (1949), Italia (1949), Lussemburgo (1949), Norvegia (1949), Paesi Bassi (1949), Portogallo (1949), Regno Unito (1949), Stati Uniti (1949), Grecia (1952), Turchia (1952), Germania (1955), Spagna (1982), Polonia (1999), Repubblica Ceca (1999)Ungheria (1999), Bulgaria (2004),Estonia (2004), Lettonia (2004), Lituania (2004), Romania (2004), Slovacchia (2004), Slovenia (2004), Albania (2009), Croazia (2009), Montenegro (2017), Macedonia del Nord (2020)

[456] NATO Official Website. (2020). *A short history of NATO*. Consultato da https://www.nato.int/cps/en/natohq/declassified_139339.htm

[457] Jackson, S. (1979). Prologue to the Marshall plan: the origins of the American commitment for a European recovery program. *The Journal of American History*, *65*(4), 1043-1068. Oxford University

aveva come fine quello di evitare qualsiasi possibilità di rinascita dello stato nazista tedesco e quello di cercare di impedire qualsiasi incursione attraverso i territori europei da parte dell'Unione Sovietica. La firma del trattato ha essenzialmente ha imposto un obbligo fondamentale di assistenza militare: nel caso in cui uno degli stati membri venga attaccato, tutti gli altri dovranno assisterlo nell'ambito della legittima difesa statale garantita dall'art.51 della Carta delle Nazioni Unite, sintetizzato all'art.5, che verrà analizzato nel dettaglio nel prossimo paragrafo.

Fino al 1960, la NATO decise di adottare la dottrina della "rappresaglia di massa": in caso di un attacco da parte dell'Unione Sovietica, l'organizzazione avrebbe risposto utilizzando armi nucleari[458]. L'effetto voluto da questa dottrina era quello di scoraggiare entrambe le parti dall'assunzione di rischi inutili, dal momento che qualsiasi attacco, seppur piccolo, avrebbe potuto comportare uno scontro nucleare effettivo. L'esistenza di questo stallo derivante dalla dottrina della rappresaglia di massa permise agli stati membri di concentrare le loro energie sulla crescita economica piuttosto che sul mantenimento di grandi eserciti convenzionali.

Subito dopo la fine della guerra fredda, molti predissero che l'alleanza atlantica sarebbe terminata. Con la perdita del "nemico", anche lo scopo stesso dell'organizzazione, che altro non è che la base della sua legittimità ma soprattutto saldo collante tra i membri, sembrava svanito. Tuttavia, contrariamente alle aspettative, la NATO persiste ed è considerata, ad oggi, come l'organizzazione internazionale dell'emisfero occidentale più importante in tema di sicurezza centrale.

Per spiegare come la NATO è riuscita non solo a sopravvivere ma anche e soprattutto a ritagliarsi un ruolo di assoluta rilevanza all'interno del panorama

---

Press. Definizione: il piano Marshall, annunciato il 5 giugno 1947 dal segretario di stato statunitense John Marshall, prevedeva lo stanziamento di una somma pari a 12.7 miliardi di dollari per la ricostruzione economica europea.

[458] Vedi nota 456.

internazionale, è necessario rifarsi alle considerazioni relative all'obbligatorietà di tener conto del ruolo delle norme, dei principi e dell'identità[459]. La capacità di un'organizzazione di adattarsi al cambiamento dipende dal fatto che le sue attività, le sue norme, regole e procedure siano specifiche o generali ma anche dal fatto che l'insieme delle sue attività corrisponda al tipo di problemi relativi alla sicurezza che vengono affrontati quotidianamente da ciascuno degli stati membri[460]. Infatti, è stato più volte sostenuto come la NATO non sia solo ed unicamente un'alleanza militare, tenuta insieme da una minaccia esterna comune; si tratta di un'organizzazione internazionale con, alla base, una comunità di valori e di norme liberal-democratiche[461]. Il ruolo della NATO si è dunque sviluppato ampiamente nel corso del tempo, tanto che al giorno d'oggi il compito fondamentale è garantire la libertà e la sicurezza dei paesi membri attraverso mezzi politici e militari[462]. Promovendo sempre e comunque i valori democratici all'interno dei vari paesi, garantisce e favorisce la cooperazione in tema di sviluppo di strategie di difesa e di sicurezza, anche e soprattutto cibernetica, tra i vari stati membri: ha il compito di aumentare la fiducia tra gli stessi e, nel lungo periodo, di prevenire i conflitti. Da un punto di vista invece militare, la NATO, come l'ONU, è improntata ad una risoluzione pacifica delle controversie; solo nel caso di fallimento di ogni tentativo diplomatico, ha la possibilità di intraprendere operazioni che vengono definite di "gestione della crisi"[463]. Quest'ultima possibilità, nel rispetto del principio di legittima difesa definito all'art. 51 della Carta delle Nazioni Unite, è subordinata alle condizioni di cui all'art. 5 del trattato, da soli o in collaborazione con altre organizzazioni

[459] Waterman, H., Zagorcheva, D., & Reiter, D. (2002). NATO and Democracy. *International Security*, *26*(3), 221-235. Consultato da https://www.researchgate.net/publication/249564772_NATO_and_democracy

[460] Wallander, C. A. (2000). Institutional assets and adaptability: NATO after the Cold War. *International organization*, 705-735. The IO Foundation and the Massachusetts Institute of Technology.

[461] Sjursen, H. (2004). On the identity of NATO. *International Affairs*, 80(4), 687–703, Consultato da https://doi.org/10.1111/j.1468-2346.2004.00411.x

[462] NATO Sito ufficiale. (2020). *Che cos'è la NATO?* Consultato da https://www.nato.int/nato-welcome/index_it.html

[463] *Ibid.*

internazionali o in seguito all'ottenimento di un mandato da parte delle Nazioni Unite stesse, anche se, per il momento, come verrà meglio analizzato nel paragrafo successivo, solo una volta è stato invocato l'art.5, in seguito all'attentato del 11 settembre[464].

Da ultimo, è stato adottato nel 2010 il Concetto strategico[465], il quale stabilisce quali siano i compiti fondamentali, gli obiettivi e i principi che sottostanno all'attività dell'organizzazione internazionale, andando a comprendere, all'interno dello stesso, anche la tutela della sicurezza e della pace nel mondo cibernetico. Proprio su questo punto la NATO si è sempre dimostrata particolarmente attenta. In particolare, l'attacco *Denial of service* avvenuto contro l'Estonia nel 2007, il quale ha temporaneamente paralizzato l'infrastruttura internet nazionale estone, da un punto di vista storico ha rappresentato un momento fondamentale nell'evoluzione dell'alleanza, perché per la prima volta si è verificata formalmente una richiesta di assistenza, a seguito di un attacco digitale[466]. Nonostante l'attacco non abbia portato alcun morto, lo stesso è stato fatto rientrare all'interno della definizione fornita dalla *Rule 30* del *Tallinn Manual* dal momento che ha causato ingenti danni, tenuto anche in considerazione che la gravità e la durata dell'assalto hanno portato ad una crisi nazionale all'interno dell'alleanza. L'attacco *e-raid* che ha subito l'Estonia ha dimostrato che esistono una serie di sfide dinamiche nel mondo multipolare della rete.

Dall'altra parte, è possibile constatare come l'alleanza abbia reagito prontamente alla crisi e alle difficoltà derivanti dal tema della *cyber-defense,* anche adottando una serie provvisoria di strumenti in grado di aiutare i suoi membri da attacchi

[464] *Ibid.*

[465] NATO Heads of State and Government. (2010, 19-20 novembre). *Strategic Concept of the Defence and Security of the Members of the North Atlantic Treaty Organization.* Consultato da https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

[466] Hughes, R. (2009). NATO and Cyber Defence. *Atlantisch Perspectief*, 33. Consultato da https://scholar.google.com/citations?user=ORnkIVgAAAAJ&hl=en

cibernetici futuri[467]. Nonostante il lavoro da fare sia assolutamente impegnativo e di livello, la maggior parte degli stati si sono sentiti rassicurati dalle misure, fino al momento, adottate dall'alleanza. L'elemento fondamentale della *cyber* difesa è diventato un compartimento autonomo nell'attività dell'organizzazione. La NATO ha inoltre già aggiunto due pietre miliari nella creazione della sua "difesa cibernetica 1.0": *in primis*, ha istituito il *cyber defense management authority*, inoltre ha realizzato una piattaforma intellettuale per il pensiero dottrinale e strategico a lungo termine sul dominio informatico attraverso la formazione del Centro di Difesa Informatica Cooperativo di Eccellenza (CCDCOE).

La seconda grande iniziativa adottata dalla NATO risale al 2016, durante il vertice di Varsavia; in seguito, a questo vertice fu approvato il *cyber defense pledge*, ovvero l'impegno ufficiale nella difesa cibernetica. Dal momento in cui la NATO stessa ha dichiarato l'esistenza nonché la necessità di operare nel mondo cibernetico visto come quinto dominio[468], il *cyber defense pledge* obbliga essenzialmente gli alleati a destinare una parte supplementare di investimenti per il miglioramento delle difese cibernetiche nazionali, pur non essendoci un importo minimo specificato[469]. Infatti, un'efficiente difesa informatica dipende soprattutto dalla costruzione di una comunità basata sulla fiducia e sullo scambio di informazioni e innovazioni che assumono una rilevanza a livello tecnologico, comunità in cui non sono presenti anelli palesemente più deboli di altri.

3.4.1 L'articolo 5 del Trattato del Nord Atlantico e le sue implicazioni

Il principio di difesa collettiva, statuito tramite la firma del trattato del Nord Atlantico già nel 1949, risulta essere il cuore pulsante dell'alleanza e l'articolo

[467] *Ibid.*

[468] NATO. (2016, 8-9 luglio). *NATO Summit Guide.* Consultato da https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf

[469] Shea, J. (2017). How is NATO meeting the challenge of cyberspace?. *Prism*, *7*(2), 18-29. Consultato da https://cco.ndu.edu/News/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/

che ha senza dubbio destato più dibattito. Si concretizza infatti come un principio unico e duraturo che obbliga vicendevolmente tutti gli stati che fanno parte dell'alleanza, impegnandoli a proteggersi e a difendersi tutti insieme[470]. L'art. 5 prevede che se un alleato della NATO è vittima di un attacco armato, ogni altro membro dell'alleanza sarà obbligato a considerare questo atto di violenza come un attacco armato contro tutti i membri e prenderà tutte le azioni che risulteranno necessarie per proteggere lo stato attaccato. L'art. 5 del trattato infatti statuisce che:

> «*Le Parti convengono che un attacco armato contro una o più di esse, in Europa o nell'America settentrionale, costituirà un attacco verso tutte, e di conseguenza convengono che se tale attacco dovesse verificarsi, ognuna di esse, nell'esercizio del diritto di legittima difesa individuale o collettiva riconosciuto dall'art.51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti così attaccate, intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'impiego della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale.*
>
> *Qualsiasi attacco armato siffatto, e tutte le misure prese in conseguenza di esso, verrà immediatamente segnalato al Consiglio di Sicurezza. Tali misure dovranno essere sospese non appena il Consiglio di Sicurezza avrà adottato le disposizioni necessarie per ristabilire e mantenere la pace e la sicurezza internazionali»*[471] .

Sebbene sia stato solo formalmente evocato una volta, l'art. 5 costituisce il pilastro principale su cui è fondata l'alleanza e funge da deterrente contro le ostilità da parte di nazioni non NATO ed attori non statali. Dalla creazione della

[470] NATO. (2019, 25 novembre). *Collective defence – Article 5*. Consultato da https://www.nato.int/cps/en/natohq/topics_110496.htm

[471] Pubblicazioni Centro Studi per la Pace. (1999, 20 giugno). *Trattato del Nord Atlantico 1949.* Consultato da http://www.studiperlapace.it/documentazione/natotreaty.html#FN1

NATO nel 1949, il modo in cui le nazioni si impegnano all'interno della guerra è cambiato radicalmente. Questa evoluzione infatti è arrivata ad includere l'incorporazione del *cyberspace* all'interno della conduzione della guerra, con il fine di assicurare una migliore protezione alle difese nazionali; ciò può essere testimoniato sulla base delle dichiarazioni rilasciate dal deputato assistente del segretario della difesa Aaron Hughes, che ha asserito come il dipartimento della difesa debba affrontare con particolare tenacia le problematiche derivanti dal cyberspazio, essendo oggi il mondo cibernetico uno dei dominii considerati [472]. Sulle base delle premesse relative alla capacità della NATO di contrastare gli attacchi armati avanzati, il 5 settembre 2014 i capi di stato e di governo del consiglio Nord Atlantico hanno emesso una dichiarazione, definita "*the Wales Declaration*"; con la stessa veniva delineata la minaccia e l'attacco informatico, ribadendo in quei casi la politica della NATO basata su prevenzione, individuazione, resilienza, recupero e difesa[473]. Accanto a questo, la dichiarazione di Wales ha altresì affermato come le norme del diritto internazionale, tra le quali lo stesso *jus in bello* e la Carta delle Nazioni Unite, vengano applicate allo stesso modo nei casi concernenti il *cyber* spazio[474]. La dichiarazione termina esplicitando che l'art. 5 del trattato si applica di fatto agli attacchi informatici, come stabilito dal consiglio del nordatlantico, caso per caso. Inoltre, direttamente un anno dopo, il segretario generale della NATO ha ribadito che un attacco informatico potrebbe essere senza dubbio un attacco armato, andando di conseguenza ad innescare le disposizioni di difesa collettiva come previste all'art. 5[475].

---

[472] Aaron Hughes, Deputy Assistant Secretary of Defense. (2016). Statement on *Digital Acts of War: Evolving the Cybersecurity Conversation, Before the H. Comm. on Oversight and Government Reform Subcomms. on Information Security and National Security*, 114th Cong. 1.

[473] NATO. (2018, 30 agosto). *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.* Consultato da https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[474] *Ibid.*

[475] NATO. (2015, 19 maggio). *Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar*. Consultato da http://www.nato.int/cps/en/natohq/opinions_118435.htm.

Come qualsiasi altro trattato internazionale, anche il trattato del Nord Atlantico è subordinato, nel suo contenuto, al periodo in cui lo stesso è stato stipulato. Di conseguenza, risulta assolutamente normale non riuscire a trovare, al suo interno, nessuna specificazione relativa al mondo cibernetico. Nonostante la NATO abbia continuato ad utilizzare un espresso linguaggio, contenuto all'art. 5, per governare tutti gli aspetti degli attacchi armati, gli attacchi cibernetici riportano ostacoli assolutamente unici nel suo genere[476]. Come analizzato nel corso dell'elaborato, gli attacchi cibernetici presentano notevoli modificazioni identificative rispetto a quanto avviene per i classici modelli di guerra dinamica; molto spesso, a differenza di questi ultimi, i quali sono in grado di creare danni immediatamente visibili, gli attacchi cibernetici hanno la capacità di devastare una nazione senza effetti fisici, il che lascia intendere la difficoltà di adottare, stante il carattere dell'imminenza, un'effettiva ed efficace risposta di difesa nel minor tempo possibile. L'art. 5 è infatti utile per valutare le azioni poste in essere da attori statali e non statali utilizzate nella guerra tradizionale. Tuttavia, gli alleati della NATO hanno redatto il trattato all'art. 5 tenendo solo in considerazione la tecnologia e le tattiche di conflitto subito successive alla Seconda guerra mondiale. Il punto cardine per riuscire legittimamente a fornire una tutela contro gli attacchi cibernetici invocabile alla stregua dell'art. 5 parte dalla capacità, per l'alleanza stessa, di riuscire a fornire concretamente una definizione unitaria di quelle attività che assurgono al rango di attacco armato, così come tutelato all'art.5, equiparabile all'attacco cibernetico. La mancanza di un'uniformità definitoria porterebbe inevitabilmente tutti gli stati alleati ad un dibattito relativo a qualsiasi operazione adottata contro uno stato alleato, essendo stabilito, nella stessa *Wales Summit Declaration,* il fatto che ciascuno attacco vada individuato caso per caso.

[476] Jackson, S. (2016). NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack. *The CIP Report*. Consultato da https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

Le nozioni più importanti in tema di difesa cibernetica sono contenute nel paragrafo n. 72 e del paragrafo n. 73 della *Declaration*. La dichiarazione stessa ha rappresentato per la NATO il primo, grande ed innovativo cambiamento in tema di sicurezza cibernetica, dal momento che mai prima di quello momento, anche e soprattutto tenendo conto dei plurimi attacchi avvenuti, tra i quali quelli subiti da Estonia (2007), Stati Uniti (2008) e Georgia (2008)[477], nessuna organizzazione internazionale era arrivata ad un simile esplicitazione. Il paragrafo 72 riscontra infatti come gli attacchi e le minacce cibernetiche continueranno ad essere sempre più usuali, più sofisticati e potenzialmente in grado di creare danni sempre maggiori[478]. Ogni dubbio in tema di *cyber attack* viene inoltre fugato al termine dello stesso paragrafo 72 in cui viene esplicitato che:

> «*Cyber-attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber-attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis*»[479].

Sulla base di ciò, il paragrafo 73 statuisce che compito fondamentale dell'alleanza sarà quello di sviluppare ulteriormente le capacità nazionali di difesa cibernetica, migliorare la sicurezza informatica delle reti nazionali, da cui dipendono le attività della NATO e favorire il più possibile il passaggio di informazioni, nonché aumentare la consapevolezza delle varie situazioni tra gli

[477] Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 russian-georgian cyber conflict. *Loyola of Los Angeles International and Comparative Law Review, 32(2),* 303-334. Consultato da https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=ilr

[478] Vedi nota 473.

[479] *Ibid.*

alleati[480]. Inoltre, con la *Wales declaration*, la NATO si impegna altresì nello scambio e nella condivisione di informazioni con le altre organizzazioni internazionali, aventi quest'ultime carattere universale o regionale, come avviene continuamente con l'Unione Europea, intensificando anche la cooperazione con il settore privato, dal momento che risulta uno dei metodi migliori per implementare la forza delle varie difese informatiche. Per ultimo, la NATO si impegna a favorire la condivisione di conoscenze anche con singoli individui, con programmi adibiti all'educazione, formazione ed esercizio nel tema di difesa cibernetica.

Due sono le annotazioni che sono state portate alla luce in seguito all'adozione della *Wales Declaration* che meritano di essere analizzate. Come enfatizzato dal diplomatico e funzionario di governo polacco, Grzegorz Kostrzewa Zorbas, la NATO avrebbe bisogno di integrare in modo completo, rapido e preciso il tema della guerra informatica, della difesa cibernetica e delle armi informatiche[481]. Esiste un percorso di revisione ciclico che avrebbe portato a rianalizzare la dichiarazione nel 2020, ma a causa della pandemia globale quest'ultima attività è stata rinviata. La seconda annotazione fa invece riferimento alla possibile e necessaria creazione di un *cyber Command*, avente una portata globale e direttamente agli ordini del *Allies Command Operation* (ACO)[482]. Come sostiene lo studioso polacco, tutte le innovazioni strutturali che vengono delineate tramite il paragrafo 73 potrebbero non rivelarsi a pieno sufficienti. L'attuale *cyber defense committee* ed il centro di eccellenza *Cyber defense cooperative* della NATO con sede a Tallinn, che verranno analizzati nel paragrafo successivo, non

[480] *Ibid.*

[481] Kostrzewa-Zorbas, G. (2014). NATO in the new strategic environment: Cyberattacks now Covered by article 5 of the north atlantic Treaty. *Studia Bezpieczeństwa Narodowego, 4(6), 397-418.* Consultato da http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-a3e2b0d5-a7ae-4a61-993e-5e05997253b4

[482] NATO. (2020, 23 ottobre). *Allied Command Operations (ACO).* Consultato da https://www.nato.int/cps/en/natolive/topics_52091.htm. L'ACO è l'organo responsabile per la programmazione ed esecuzione materiale delle operazioni della NATO. Si compone di un numero piccolo di sedi permanenti, ciascuna con un ruolo specifico.

sono in grado di assurgere al ruolo che avrebbe un vero e proprio *cyber Command*. Non sarebbe necessaria, dunque, una nuova istituzione di ricerca, formazione o pianificazione, ma un vero e proprio "*combat command*"[483].

3.4.2 La creazione di nuovi centri d'eccellenza per lo studio delle nuove sfide: il *Cooperative Cyber Defence Centre of Excellence*

La NATO ha deciso di lanciare, in seguito agli attacchi cibernetici verificatisi in Estonia, il "*Cooperative cyber defense Centre of Excellence*". Collocato all'interno della capitale estone, il centro di Tallinn rappresenta un luogo assolutamente all'avanguardia dove poter liberamente svolgere la propria attività. Infatti, la scelta dell'Estonia non è casuale poiché, oltre ad avere un'esperienza diretta di guerra informatica, il paese è sede di una fiorente industria *hi-tech*, tanto da aver fornito al paese il soprannome di "E-stonia"[484]. Al giorno d'oggi risulta essere uno dei migliori "centri di eccellenza" NATO[485].

Il centro è stato formalmente creato il 14 maggio 2008 con il pieno appoggio della NATO, anche se diventò formalmente operativo il 28 ottobre 2008, ottenendo la qualifica di organizzazione internazionale militare[486]. La missione principale che viene svolta dal centro è quella di sostenere le nazioni che fanno parte del centro e la NATO stessa con competenze interdisciplinari uniche nel campo di ricerca, formazione ed esercitazioni di difesa informatica che vanno a

[483] Kostrzewa-Zorbas, *op. cit.*, p. 159.

[484] Staff Writers. (2008, 14 maggio). *NATO launches cyber defence centre in Estonia*. Consultato da Space War, https://www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html

[485] NATO. (2020, 3 novembre). *Centres of Excellence.* Consultato da https://www.nato.int/cps/en/natohq/topics_68372.htm. I centri di eccellenza NATO sono organizzazioni internazionali militari che formano e educano leader e specialisti dei paesi membri NATO e dei paesi partner. Aiutano nello sviluppo della dottrina, identificano le lezioni apprese, migliorano le capacità in seguito a plurimi esperimenti.

[486] *Ibid.*

coprire le aree di interesse di tecnologia, strategia e diritto[487]. Nonostante inizialmente solo 7 stati avevano firmato formalmente i documenti relativi alla creazione del centro, al giorno d'oggi quest'ultimo comprende 29 partecipanti[488] ed all'interno dello stesso lavora un gruppo di esperti da 29 nazioni differenti.

Il comitato direttivo, che si riunisce almeno due volte l'anno, è l'organo principale di orientamento, sorveglianza, e decisioni su tutte le questioni relative all'amministrazione, alle politiche e al funzionamento del CCDCOE. Ha compiti di approvazione e sovrintende alla redazione del bilancio, del piano di sviluppo e del programma di lavoro. Il comitato è composto da un rappresentante votato per ciascuna nazione sponsor, mentre lo stato di membro è disponibile solo ed unicamente per quelle nazioni alleate NATO. I paesi che non aderiscono alla NATO, infatti, possono partecipare ai lavori della CCDCOE, come partecipanti sponsor. Il presidente del Comitato direttivo, infine, è sempre un nazionale estone.[489]

[487] The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *About us*. Consultato da https://ccdcoe.org/about-us/.

[488] Gli stati attualmente sono: Austria, Belgio, Bulgaria, Croazia, Repubblica ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Ungheria, Italia, Lettonia, Lituania, Montenegro, Olanda, Norvegia, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svizzera, Turchia, Regno Unito e Stati Uniti.

[489] The NATO Cooperative Cyber Defence Centre of Excellence, *op. cit.*, p. 160.

Capitolo 4

LA NECESSITÀ DI UN "AUTONOMO" *CYBER-PEACEKEEPING TEAM* ALL'INTERNO DELLE NAZIONI UNITE

SOMMARIO: 4.1 Profili generali e normative eventualmente applicabili - 4.2 Struttura ed attività del *CPK team* - 4.2.1 *Department for Conflict Operations* - 4.2.2 Sub-dipartimento per la prevenzione dei conflitti - 4.2.3 Sub-dipartimento per l'implementazione di accordi di pace - 4.2.4 *Department for Stabilization Affairs* - 4.2.5 Il sub-dipartimento per gli affari sociali ed economici - 4.2.6 Sub-dipartimento per gli affari e la sicurezza dello stato - 4.3 Principali problematiche - 4.4 La responsabilità internazionale dello Stato per gli attacchi cibernetici - 4.4.1 La responsabilità statale nel *cyberspace* - 4.4.2 Applicabilità del principio di due diligence nel *cyberspace*: le maggiori difficoltà.

4.1 Profili generali e normative eventualmente applicabili

Varie e plurime possono essere le misure che l'ONU può, nella realtà dei fatti, adottare qualora lo ritenga necessario, alla stregua dei limiti e delle competenze che sono delineate nella Carta delle Nazioni Unite. Nella maggior parte dei casi, l'organizzazione cerca concretamente di evitare l'uso della forza, predisponendo tramite la legittimazione derivante dall'art.41[490], una serie di misure che possono essere adottate qualora uno stato abbia effettuato un'attività in grado di costituire un attuale pericolo per la pace. Le misure previste all'art.41 comprendono per lo più misure aventi carattere economico, come l'interruzione di qualsiasi relazione commerciale con lo stato considerato, oppure l'interruzione di qualsiasi mezzo per la comunicazione con lo stesso. Essendo l'articolo rientrante all'interno del cap. VII, le misure adottate dal consiglio di sicurezza non saranno soggette al limite di "*domestic jurisdiction*" di cui all'art.2 par.7.[491] Il più grande esempio che ha portato ad incredibili risultati in seguito all'applicazione di queste misure da parte dell'ONU attiene alle sanzioni economiche imposte all'Iraq in seguito

[490] United Nations. (2020). *Office of legal affairs. OLA*. Consultato da https://legal.un.org/repertory/art41.shtml Art. 41: «*The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations*».

[491] Conforti, *op. cit.*, p. 62. (Vedi pp. 148-149).

all'invasione, da parte di quest'ultimo, del Kuwait[492]. L'annessione militare del Kuwait, avvenuta il 2 agosto 1990, ha portato il Consiglio di sicurezza a adottare la risoluzione 660/1990[493], condannando quindi l'invasione irachena, chiedendo l'immediato ritiro delle truppe e imponendo sanzioni economiche. La tipologia principale di queste misure risiede, senz'altro, nell'applicazione di un embargo, con il conseguente divieto per gli stati di commerciare ed intrattenere qualsiasi tipologia di rapporto commerciale con lo stato considerato colpevole di aggressione. Dall'altra parte, un ruolo fondamentale può al giorno d'oggi essere rappresentato dalla possibilità per gli stati del mondo, qualora venga richiesto, di "tagliare fuori" qualsiasi comunicazione proveniente dallo stato considerato[494].

Compito dell'elaborato seguente è analizzare i margini e le prospettive per la creazione di quello che, ad oggi, risulta un istituto di assolutamente lontana fattibilità ma che sarebbe in grado di garantire una migliore cooperazione e una migliore tutela della sicurezza e della pace internazionale: un *cyber peacekeeping team*. Prima però di esaminare direttamente quest'ultimo punto è necessario fare un passo indietro e studiare l'istituzione delle generali *peacekeeping operations*, differenti dalle operazioni di *peace enforcement;* l'ammissibilità di queste operazioni fornirà le basi per poter ammettere anche un'attività cibernetica.

Non avendo direttamente un esercito proprio, la Carta delle Nazioni Unite predispone, agli art.43, 44, e 45 un obbligo per gli stati membri di concludere accordi con il Consiglio di Sicurezza per stabilire numero e grado di preparazione delle forze armate utilizzabili dall'organizzazione in maniera totale o parziale[495]. La definizione di *peacekeeping operation* ci viene data dalla stessa organizzazione:

---

[492] Bohr, S. (1993). Sanctions by the united nations security council and the European community. *European Journal of International Law, 4(2),* 256-268.

[493] UNSCR. (n.d.). *Resolution 660 Iraq-Kuwait (2 August).* Consultato da http://unscr.com/en/resolutions/doc/660

[494] *Ibid.*

[495] Conforti, *op. cit.,* p. 62. (Vedi pp. 165-166).

> "*Action undertaken to preserve peace, however fragile, where fighting has been halted and to assist in implementing agreements achieved by the peacemakers"*[496].

La prima di queste operazioni relative al mantenimento della pace è stata effettuata da parte dell'ONU nel 1948, dove gli operatori sono stati inviati per controllare lo sviluppo dell'armistizio tra Israele, Libano, Giordania, Siria ed Egitto[497]. Fino agli anni 90', le operazioni di *peacekeeping* si sono rivelate tremendamente efficaci; maggiori difficoltà, tuttavia, si sono sviluppate con la guerra in Bosnia del 1992 e con la seconda operazione in Somalia nel 1993, entrambe ritenute attività di *peacekeeping* assolutamente fallimentari[498]. Mentre nel caso bosniaco gli operatori hanno fallito totalmente nel mantenere al sicuro i civili, nel caso somalo diventarono effettivi partecipanti del conflitto. Questi due casi portarono ad una rivalutazione dell'attività di *peacekeeping* nella sua interezza, rivalutazione che oggi porta le Nazioni Unite ad affrontare, sul tema, una serie di problematiche sempre maggiori.

Innanzitutto, è necessario fornire una chiarificazione relativa alle due tipologie di *peacekeeping operations*: quelle aventi carattere tradizionale e quelle aventi carattere multidimensionale[499]. Il carattere tradizionale si concretizza in attività di osservazione, monitoraggio e comunicazione di quanto osservato; il carattere multidimensionale invece presuppone operazioni più complesse che possono andare ad integrare l'attività di *peace building*[500]. Le attività stesse sono finalizzate ad ottenere vari risultati, come la prevenzione dei conflitti con interventi diretti ad evitare lo scoppio degli stessi o come l'attività di

---

[496] United Nations. (2008, gennaio). *United Nations Peacekeeping Operations: Capstone Doctrine*. Consultato da http://pbpu.unlb.org/pbps/library/capstonedoctrineeNg.pdf

[497] MacQueen, N. (1999). *The United Nations Since 1945: Peacekeeping and the Cold War*. Addison-Wesley Longman.

[498] Roberts, A. (2008, 3 marzo). The crisis in UN peacekeeping. *Survival*, 36(3), 93–120. Consultato da https://www.tandfonline.com/doi/abs/10.1080/00396339408442752

[499] Robinson, *op. cit.*, p. 121.

[500] *Ibid.*

peacemaking (tramite anche l'attuazione di misure diplomatiche per favorire un cessate il fuoco. Sulla falsariga del *Brahimi report*[501] è inoltre possibile sottolineare una serie di principi che determinano la legittimità delle *peacekeeping operations:* tra questi il principio del consenso delle parti, dell'imparzialità e del mancato utilizzo della forza se non in caso di autodifesa o nel caso in cui il mandato lo preveda. Il consenso delle parti risulta di fondamentale importanza, dal momento che legittima l'attività svolta sia da un punto di vista materiale che politico; senza il consenso delle parti l'attività rischia di sfociare in un conflitto[502]. L'imparzialità si concretizza nel senso che tutte le attività eseguite dai cosiddetti "caschi blu" devono essere subordinate alla ricerca del mantenimento della pace e della sicurezza internazionale e mai devono essere attutate andando a ricercare e tutelare singoli interessi statali[503]. L'utilizzo della forza, infine, deve essere visto solo ed unicamente come ultima spiaggia, da utilizzare qualora non esista altro modo di risolvere pacificamente la controversia. Le altre operazioni invece vengono definite come *peace enforcement,* le quali si contraddistinguono per il tentativo di ristabilire la pace senza il consenso delle parti, cui segue solitamente la seconda attività di *peace building*, cioè la predisposizione di solide basi in grado di mantenere la pace ed evitare un futuro conflitto. I tre requisiti sopra considerati si applicano solo ed unicamente alle operazioni tradizionali, non applicandosi, di conseguenza, alle operazioni di *peace enforcement* che hanno come base un'autorizzazione da parte del CdS[504]. Su questo tema la legittimità delle *cyber operations* che raggiungono il livello di uso della forza dipenderà strettamente dalle caratteristiche e dagli elementi fondanti dell'autorizzazione. Se, in particolare, il CdS ha autorizzato

[501] United Nations General Assembly and Security Council. (2000, 21 agosto). *Comprehensive Review of the Whole Question of Peacekeeping Operations in All Their Aspects A/55/305.* Consultato da *https://www.un.org/ruleoflaw/files/brahimi%20report%20peacekeeping.pdf*

[502] Robinson, *op. cit*., p. 121.

[503] Gibbs, D. N. (2000). The United Nations, international peacekeeping and the question of 'impartiality': revisiting the Congo operation of 1960. *The Journal of Modern African Studies, 38*(3), 359–382. Consultato da http://doi.org/10.1017/S0022278X00003384

[504] Schmitt, M. N. (Cur.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

l'utilizzo di misure comprendenti l'uso della forza nell'attività di *peace enforcement* allora anche le cyber operazioni, che sono necessarie a supportare le operazioni cinetiche, saranno considerate legittime[505]

Con sempre maggiore insistenza negli ultimi anni, si sta facendo strada l'idea di una necessità assoluta di attività di *cyber peacekeeping (CKP),* essendosi evoluto notevolmente il dominio in cui sfociano i conflitti; come già rilevato, al giorno d'oggi, il famoso "quinto dominio" si va a identificare come il futuro scenario di guerra, per una serie di elementi già analizzati nel primo capitolo. Prima di andare ad esaminare le singole voci degli studiosi in materia, è necessario fornire una definizione dei caratteri strutturali che contraddistinguono le operazioni di *cyber peacekeeping*: queste attività comprendono la prevenzione o la mitigazione dei conflitti cibernetici, la tutela e la promozione della sicurezza online in accordo con i principi di diritto internazionale e la protezione dei civili come fine principale[506], garantendo sempre l'imparzialità di ciascuno stato. Accanto alla funzione di protettori dei civili, i diversi ruoli, svolti dagli addetti inviati per compiere quelle operazioni, saranno quelli di guardiani, mediatori, coordinatori e *builder*[507].

Sotto forma di guardiano, vengono affrontate le minacce direttamente, utilizzando mezzi tecnici e non offensivi per proteggere i civili e garantire la pace nel *cyberspace*; il guardiano ha il compito di monitorare e rispondere alle minacce da un punto di vista tecnico e le sue funzioni sono quelle di prevenire, monitorare ed eventualmente tentare di rimuovere le conseguenze[508].

La qualifica di mediatore, invece, prevede l'impegno contro le minacce cibernetiche attraverso una serie di attività che coinvolgono direttamente gli

[505] *Ibid.*

[506] Akatyev, N., & James, J. I. (2015, ottobre). Cyber peacekeeping. In *International Conference on Digital Forensics and Cyber Crime* (pp. 126-139). Springer, Cham.

[507] *Ibid.*, (p. 131).

[508] *Ibid.*, (p. 132).

attori partecipanti ad un conflitto, con l'obiettivo di ridurre i danni derivanti da operazioni cibernetiche e di prevenire lo sviluppo di ulteriori conseguenze. Il ruolo del mediatore assomiglia notevolmente al ruolo svolto dai "tradizionali" *peacekeeper operators*, i quali compiono un'attività di facilitazione del dialogo fra le parti, con il fine di prevenire l'aggravamento del conflitto ed estirparlo[509]. Non esistendo norme direttamente ed unicamente applicabili al cyberspazio o standard uniformi nell'ambito delle relazioni internazionali in materia, il ruolo svolto dal coordinatore sarebbe quello di sviluppare detti standard in tempo di pace e, di comune accordo con il ruolo del mediatore, cercare al massimo di promuoverli. Come il mediatore, infatti, il coordinatore basa la sua attività sul dialogo, con la differenza che il primo si rivolge solo alle parti del conflitto mentre il secondo ad una pluralità di entità che operano nel *cyberspace*[510]. L'ultima attività invece viene svolta sulla falsariga del cosiddetto "*builder*", ovvero un "costruttore", il quale si occuperebbe di rafforzare costantemente la capacità e la resilienza dei sistemi governativi statali, delle rispettive infrastrutture critiche ed infin delle varie organizzazioni internazionali[511].

Il problema principale, relativo alle attività considerate, rientra nel fatto che nessuna organizzazione internazionale ha, fino a questo momento, fatto riferimento ad una delle varie *CPK operation* così come indicate alla stregua dei parametri forniti da Akatyev e James[512]. Molte organizzazioni internazionali, con i rispettivi organi sussidiari, potrebbero astrattamente avere la possibilità di prevedere strumenti in grado svolgere suddette attività, come per esempio la NATO o ancora la *Shangai Cooperation Organization*. Tuttavia, proprio per la specificità delle organizzazioni di questo tipo, solo le Nazioni Unite, fino ad ora,

[509] *Ibid.*

[510] *Ibid.*

[511] *Ibid*., (p. 133).

[512] Akatyev, N., & James, J. (2017, giugno). United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping. In *European Conference on Cyber Warfare and Security* (pp. 8-16). Academic Conferences International Limited.

potrebbero essere in grado di ospitare un organo in grado di svolgere attività di CKP[513].

Una delle prime voci a farsi sentire in materia di *cyber peacekeeping*, senza eccessivi risultati pratici, fu quella dello studioso Cahill, il quale, nel suo elaborato, ha individuato il mondo cibernetico come punto focale su cui la guerra si incentrerà con maggior vigore; ha inoltre esaminato la corrente disciplina delle attività di mantenimento della pace delle Nazioni Unite, cercando di interpretarla andando ad includere anche le operazioni di mantenimento della pace cibernetiche[514]. Come analizzato inoltre da Jann K. Kleffner e Heather A. Harrison Dinniss, si è sviluppata una tendenza evidente da parte del Consiglio di sicurezza ad autorizzare varie forme di operazioni di pace con compiti distinti e differenti in situazioni di conflitti armati e crisi di altro genere[515]. L'aumento di situazioni di conflitto o di crisi che presentano una componente informatica, accanto alla diffusione di sempre più complesse operazioni di pace, lasciano intendere che i *peacekeepers operators* si troveranno in situazioni contraddistinte da numerosi incidenti informatici[516]. La sempre più attuale proposta della necessarietà per le Nazioni unite di dotarsi di un gruppo specifico per affrontare gli innumerevoli incidenti informatici che si verificano tra stati è indicativa della rilevanza che le *cyber operations* stanno ottenendo per l'ONU, anche se alcuna discussione in modo formale è ancora avvenuta sul tema in seno al CdS. Infatti, da una prospettiva pienamente giuridica, risulterebbe assolutamente lecito per il Consiglio di Sicurezza effettuare una valutazione e, conseguentemente, determinare se un'operazione cibernetica assurga ad una attività avente stessa

[513] *Ibid*., (p 9).

[514] Cahill, T. P., Rozinov, K., & Mule, C. (2003). Cyber warfare peacekeeping. *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, 100-106. West Point, NY, USA. doi: 10.1109/SMCSIA.2003.1232407.

[515] Kleffner, J. K., & Harrison Dinniss, H. A. (2013). Keeping the cyber peace: international legal aspects of cyber activities in peace operations. *International Law Studies*, *89*(1), 4. Consultato da https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1039&context=ils

[516] *Ibid.*

intensità e valenza di minaccia alla pace e alla sicurezza internazionale[517], stante l'art.39 della Carta delle Nazioni Unite[518].

Un'altra accorta constatazione effettuata dagli studiosi Akatyev e James vede, nelle operazioni di *cyber peacekeeping*, un ruolo fondamentale durante i tre distinti momenti del conflitto: il momento che anticipa il conflitto, il conflitto stesso e il momento immediatamente successivo al conflitto[519]. Infatti, nel primo momento, compito degli operatori delle Nazioni Unite sarebbe quello di attuare tutte quelle attività in grado di prevenire il conflitto, come la stipulazione di accordi. Nel secondo, le funzioni cambiano radicalmente, dal momento che le priorità, una volta esploso il conflitto, mutano[520]. L'attività degli operatori, in questo secondo momento, avrebbe dunque ad oggetto l'individuazione di possibili attacchi informatici e il tentativo seguente di ridurre quanto possibile i danni per i civili, nonché fornire, conseguentemente, assistenza alle nazioni le cui infrastrutture critiche e di fondamentale importanza risultano attaccate. Infine, nel momento successivo al conflitto, l'attività consisterebbe nell'aiuto per la ricerca e lo sviluppo di nuove contromisure in grado, in futuro, di contrastare le armi informatiche utilizzate durante il conflitto, aiutando le nazioni inoltre a ricostruire le loro difese cibernetiche[521].

---

[517] Read, D. (2013). Heather Harrison Dinniss, cyber warfare and the laws of war. *Nordic Journal of Human Rights, 31(2),* 284-[ii].

[518] United Nations. (2006, 24 ottobre). *Charter of the United Nations and Statute of the International Court of Justice*. (Traduz. Italiana). (Originariamente pubblicato nel 1945). Consultato da https://www.admin.ch/opc/it/classified-compilation/20012770/200609120000/0.120.pdf Art. 39: «Il Consiglio di Sicurezza accerta l'esistenza di una minaccia alla pace, di una viola-zione della pace, o di un atto di aggressione, e fa raccomandazione o decide quali misure debbano essere prese in conformità agli articoli 41 e 42 per mantenere o ristabilire la pace e la sicurezza internazionale».

[519] Akatyev, N., & James, J. I. (2015). Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. *Revised Selected Papers, ch. Cyber Peacekeeping*, 126– 139. Springer International Publishing. http://dspace.conacyt.gov.py/xmlui/handle/123456789/15838

[520] *Ibid.*

[521] *Ibid.*

Il tema delle *peace operations*, in ottica cibernetica, è stato inoltre oggetto di studio e di dibattito durante i lavori per la redazione del Tallinn Manual 2.0. Nel capitolo relativo alla sicurezza collettiva, due *Rules* assumono particolare rilevanza: la *Rule 78* e la *Rule 79*[522]. La prima evidenzia come gli stati, mentre conducono operazioni di pace, avrebbero la possibilità di compiere operazioni cibernetiche in conformità con il mandato o l'autorizzazione e, in ogni caso, con il diritto internazionale applicabile. Il mandato o l'autorizzazione possono essere concessi non solo a forze direttamente sotto il controllo delle Nazioni Unite ma anche a stati individuali o a coalizioni di stati, oltre che ad organizzazioni internazionali regionali[523]. In ogni caso, inoltre, le *cyber operations* condotte devono sempre essere subordinate ai limiti e alle imposizioni imposte dal mandato; devono anche sottostare alla disciplina prevista dalla tutela dei diritti umani e dalla legge sui conflitti armati[524]. La *Rule 79* sottolinea come, nel momento stesso in cui le forze sono impegnate nella protezione dei civili, il personale delle Nazioni Unite, le sue unità e i suoi veicoli, nonché i computer e le reti informatiche create devono essere tutelate e protette, non possono subire attacchi cibernetici[525]. Le parti del conflitto hanno l'obbligo di garantire la sicurezza e la salvezza del personale; nessuna tipologia di attività che si concretizzi in un'interferenza per il compito affidato al personale può essere attuata. Questo comporta l'obbligo di rispetto del personale delle Nazioni Unite e specifica che è vietato attaccare, minacciare o nuocere in qualsiasi modo il personale, anche tramite operazioni informatiche[526]. Gli stati interessati hanno l'obbligo di adottare tutte le misure che risulteranno necessarie per garantire la

[522] Schmitt, *op. cit*., p. 64.

[523] *Ibid*., (p. 362).

[524] *Ibid*., (p. 365).

[525] *Ibid.*, (p. 368).

[526] *Ibid.*

sicurezza del personale anche contro i *cyber attacks* che potrebbero subire, imponendo agli stessi un obbligo di cooperare per prevenire gli stessi.[527]

La necessità di un organo operativo nel settore di *cyber peacekeeping* all'interno delle Nazioni Unite fa leva sulla Carta delle Nazioni Unite stessa e sulla sua interpretazione evolutiva. Senza alcun dubbio, nel momento esatto in cui è stata redatta la Carta, gli stati che l'hanno ratificata non si sono preoccupati di inserire, specifiche previsioni relative al mondo cibernetico, ciò derivante dalla inesistenza concreta del famoso quinto dominio. Tuttavia, l'esigenza di attuare un'interpretazione evolutiva si dispiega in seno alla concezione dell'obiettivo primario svolto dall'organizzazione, ovvero la tutela della pace e della sicurezza internazionale. Mentre è pacifico ammettere che nel 1945 il tema fondamentale era l'allontanamento di qualsiasi possibilità di conflitto interstatale in seguito alle due guerre mondiali, l'evoluzione interpretativa ha portato ad ampliare la visione di conflitto. Dal momento che la guerra informatica potrebbe minacciare la pace e la sicurezza internazionale, l'ONU ha il compito di prevenire detta minaccia attuando, allo stesso modo, operazioni di mantenimento della pace.[528]

Le attività che verrebbero svolte da suddetto organo possono essere così sintetizzabili. Il *CPK team* potrebbe essere utilizzato dall'ONU inserendo la sua attività nel mondo digitale con mandati e funzionalità specifiche; l'attività svolta si contraddistinguerebbe, analogamente a quella dei classici *peacekeeper operators* ma con modalità differenti, per l'utilizzo dello strumento della navigazione su Internet, il che comporterebbe il "semplice" sfruttamento di computer innovativi, invece della più dispendiosa attività di dinamica di vigilanza che spesso comporta l'utilizzo di veicoli blindati[529]. I *CPK operators* avrebbero il compito di "vagare" all'interno del panorama digitale e dei suoi poco delineati confini, impedendo la realizzazione di attacchi informatici o

[527] *Ibid*., (p. 370).

[528] Robinson, *op. cit*., p. 18. (Vedi pag. 4).

[529] Dorn, W. (2017). Cyberpeacekeeping: A New Role for the United Nations? *Georgetown Journal of International Affairs*, 18(3), 138-146. Consultato da https://walterdorn.net/257

avvisando lo stato bersaglio dell'imminenza dell'attacco. Potrebbero ancora avere il compito di indagare ed investigare sul compimento di determinate attività digitali che comportano violazioni, comprese quelle che causano crisi informatiche tramite la perdita diffusa di dati informatici e che hanno la possibilità di mettere in pericolo vite umane o infrastrutture critiche, svolgendo, nel caso, anche un'attività di eventuale mediazione tra le parti nel conflitto[530]. Potrebbero cercare di trovare soluzione di comune accordo per l'adozione di un "cessate il fuoco" cibernetico, aiutare lo sviluppo di accordi e visioni comuni relativamente al *cyberspace*, con il fine di terminare conflitti e supervisionare i livelli di sicurezza cibernetica per garantire ai vari stati di riuscire a limitare al massimo le conseguenze di attacchi.

L'attività del *CPK team*, contraddistinto da soggetti con un elevatissimo grado di preparazione in materia informatica, potrebbe portare ad un aiuto nello sviluppo della protezione dei sistemi delle infrastrutture critiche nazionali, garantendo anche agli stati che non avrebbero le potenzialità degli stati più forti di ottenere un livello di cyber sicurezza simile[531]. Potrebbero altresì svolgere attività di formazione di cyber funzionari nazionali, contribuendo a portare più ordine e sicurezza nel cyber spazio così scarsamente governato. Nello stesso modo di quanto avviene per le tradizionali azioni di mantenimento della pace, l'attività del CPK potrebbe consistere anche in un'azione "umanitaria": come le azioni dinamiche possono avere ad oggetto l'assistenza alle vittime che si sono trovate in mezzo ad un conflitto, allo stesso modo il *CPK team* potrebbe portare assistenza a tutti quei soggetti che sono stati vittima di un attacco cibernetico[532]. La tutela dei civili si potrebbe esplicare come difesa degli innocenti anche nel *cyberspace*, tramite la supervisione di "aree sicure", dove tutti i servizi e le prestazioni risultano meglio protetti da abusi ed attacchi. Estendendo

[530] *Ibid.*

[531] *Ibid.*

[532] *Ibid.*

ulteriormente l'analogia con le normali attività di *peacekeeping*, si potrebbe includere la rimozione di *cyber-mine*, le quali sono software maligni dormienti che vengono attivate inconsapevolmente dagli utenti. In conclusione, l'istituzione di un simile organo avrebbe la forza di rendere più sicuro il mondo digitalizzato e reale[533]. Per raggiungere però l'obiettivo considerato, dovrebbe dotarsi di una struttura, la quale verrà analizzata all'interno del prossimo paragrafo.

4.2 Struttura ed attività del *CPK team*

La tecnologia cibernetica, contraddistinta da una forte dinamicità e da una grande elasticità, riuscirebbe non solo a proteggere vite umane di civili ma anche la vita degli operatori di mantenimento della pace; un esempio che può essere riportato è come operatori cibernetici in grado di pilotare un aereo a distanza garantirebbero una maggiore sicurezza, non avendo un equipaggio all'interno[534]. Un sistema di questo tipo avrebbe senza dubbio salvato la vita dei 7 operatori che sono stati uccisi in Costa d'Avorio[535], durante un'operazione di mantenimento della pace.

Per avere un funzionamento efficiente dell'organo prospettato è tuttavia necessario realizzare un processo per la formazione di specialisti, i quali sappiano affrontare gli impellenti problemi del mondo cibernetico, alla stregua di uno studio sulla comunicazione informatica, sull'intelligenza artificiale e su una serie di temi relativi al mondo ICTs. La mancanza di detta specializzazione comporterebbe un'incapacità dei *peacekeeper operators* di riuscire a far fronte a tutte le minacce ed i problemi che riguardano il loro mandato, con una

[533] *Ibid.*

[534] Powles, A., Partow, N., & Nelson, M. N. (Cur.). (2015). *United Nations Peacekeeping Challenge: The Importance of the Integrated Approach*. Ashgate Publishing, Ltd..

[535] United Nations. (2012, 8 giugno). *UN condemns deadly attack on peacekeepers in Côte d'Ivoire*. Consultato da https://news.un.org/en/story/2012/06/412772-un-condemns-deadly-attack-peacekeepers-cote-divoire

conseguente inutilità degli stessi[536]. Per essere in grado di far fronte all'impellenza della specializzazione qui considerata, le Nazioni Unite hanno eseguito quello che può essere evidenziato come il primo vero passo avanti nel settore cibernetico, seppur con finalità e funzioni totalmente differenti da quelle qui prospettate: la creazione dei caschi blu digitali[537]. Anche se molto spesso la loro attività può andare a coincidere con quella dell'organo prospettato, le finalità risultano completamente differenti: l'attività dei *DBH* è indirizzata prevalentemente alla protezione delle infrastrutture delle Nazioni Unite, escludendo, in tal modo, l'attività di mantenimento della pace destinata a persone o ad infrastrutture non ONU. Tra questi ultimi possiamo far rientrare la protezione delle infrastrutture rilevanti per paesi confinanti stati che presentano conflitti oppure la predisposizione di un supporto tecnologico o una educazione online post-conflitto, con l'obiettivo di facilitare la transizione verso una maggiore stabilità[538].

Nonostante l'evidente importanza che potrebbe avere un organo come quello considerato, diversi studiosi hanno fatto leva sulle difficoltà che lo stesso porterebbe. Tra questi, un esempio è la voce "fuori dal coro" della studiosa Ellyne Phneah, la quale ha evidenziato come, nonostante la forza dell'idea, la creazione di un team così specializzato incontrerebbe difficoltà evidenti di realizzazione[539]. Le difficoltà anzidette potrebbero partire dalla concezione di necessaria specializzazione precedentemente analizzata: convincere i "contribuenti" dell'ONU ad acquistare materiale tecnologico specialistico e di

[536] *Ibid.*

[537] Nabeel, F. (2019). Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges. *NUST Journal of International Peace and Stability*, *2*(2).

[538] *Ibid.*

[539] Phneah, E. (2012, 6 febbraio). *Idea of Cyber Peacekeepers Premature, "Redundant"*. ZDNet News. Consultato da http://www.zdnet.com/idea-of-cyber-peacekeepers-prematureredundant-2062303742/

"nicchia" che magari l'organizzazione non possiede o possiede in minima quantità, potrebbe risultare particolarmente arduo[540].

Per poter realizzare concretamente la propria attività, l'organo considerato dovrebbe possedere una struttura salda, in grado di garantire, su più livelli, un'efficienza operativa constante, la quale si fonderebbe su una predefinita e delineata ripartizione di compiti. L'idea strutturale qui prospetta prende le mosse dalla proposta del professore Ahmed Almutawa, il quale ha evidenziato quelle che dovrebbero essere le caratteristiche essenziali, nonché i problemi relativi[541].

Per essere in grado di identificare una struttura, secondo Almutawa, è necessario partire da una considerazione relativa alle funzioni che l'organo andrebbe a svolgere ma soprattutto sulla ripartizione delle stesse in capo agli organi sussidiari: suddividere l'attività, ancora di più nelle organizzazioni internazionali, rappresenta lo strumento migliore messo a disposizione per raggiungere in modo congiunto l'obiettivo prefissato, sulla base del principio che vede nella divisione del lavoro il miglior veicolo per raggiungere l'efficienza prospettata[542]. Le funzioni che andrebbe a ricoprire l'organo, partendo anche da quanto analizzato nel paragrafo precedente, sarebbero 11, ciascuna delle quali affidata espressamente a determinati dipartimenti. La differenziazione di queste 11 attività si basa sulle normali operazioni di *peacekeeping* fino a questo momento effettuate dall'ONU[543]. Le funzioni sarebbero di:

1) Prevenzione dello scoppio di un conflitto.

---

[540] Bellamy, A. J., & Williams, P. D. (Cur.). (2013). *Providing peacekeepers: the politics, challenges, and future of United Nations peacekeeping contributions*. OUP Oxford.

[541] Almutawa, *op. cit*., p. 27.

[542] Smith, A., & Stewart, D. (1963). *An Inquiry into the Nature and Causes of the Wealth of Nations* (Vol. 1). Homewood, Ill: Irwin.

[543] United Nations. (2008). *United Nations Peacekeeping Operations: Principles and Guidelines ("The Capstone Doctrine")*. (United Nations Department of Peacekeeping Operations and the United Nations Department of Field Support 2008) 97. Consultato da https://www.un.org/ruleoflaw/blog/document/united-nations-peacekeeping-operations-principles-and-guidelines-the-capstone-doctrine/.

2) Stabilizzazione della situazione di conflitto dopo un "cessate il fuoco", con l'obiettivo di istituire od implementare un ambiente favorevole alle parti per poter arrivare alla conclusione di un accordo di pace duraturo.
3) Assistenza nell'attuazione di accordi di pace.
4) Guida, per gli stati, verso una transizione che li dovrebbe portare alla creazione di un governo stabile, basato su principi democratici e contraddistinti da un buon livello di sviluppo economico.
5) Attività di smobilitazione, disarmo e reintegrazione degli ex-combattenti
6) Azioni "antimine", come precedentemente analizzato.
7) Attività di riforma del settore della sicurezza ed altre attività connesse alla creazione di uno stato di diritto
8) Protezione e promozione dei diritti dell'uomo.
9) Assistenza elettorale.
10) Azioni per il ripristino e l'estensione dell'autorità statale.
11) Promozione della ripresa e dello sviluppo economico sociale.

La proposta che in questa sede sarà esaminata prevede la creazione di due dipartimenti: il primo è un dipartimento per le operazioni di conflitto mentre il secondo è un dipartimento per una maggiore stabilità. Il primo andrà a ricoprire tutti i temi relativi ai conflitti, così come vengono affrontati dai *peacekeeper operators*, riguardanti cioè la prevenzione dello scoppio del conflitto (1) e l'assistenza nell'attuazione di accordi di pace (2). Il secondo dipartimento andrà invece a ricoprire tutte quelle funzioni rimanenti, che si articolano nella predisposizione di piani di stabilizzazione che servono a favorire la ripresa economica, sociale e governativa dei paesi in un momento successivo al conflitto[544]. La proposta prevede inoltre la creazione di due sub-dipartimenti all'interno del primo, a ciascuno dei quali verrà conferita una delle due attività: il primo sub-dipartimento avrà il compito di prevenire lo scoppio di conflitti, mentre il secondo quello di implementare e promuovere la redazione di accordi

[544] Almutawa, *op. cit.*, p. 27.

in seguito a conflitti. Allo stesso modo, il secondo dipartimento necessiterà due sub-dipartimenti[545]. Il primo è il sub-dipartimento per i problemi sociali ed economici, che avrà come compito quello di stabilizzare le situazioni di conflitto dopo un cessate il fuoco (2), di facilitare la creazione di una stabilità governativa successiva ad un conflitto (4), di svolgere attività di smobilitazione, disarmo e reintegrazione degli ex-combattenti (5), di proteggere e promuovere i diritti umani (8) ed infine di promuovere il restauro e lo sviluppo economico e sociale (11). Il secondo sub-dipartimento, quello per la sicurezza degli stati, avrà ad oggetto le restanti attività[546].

4.2.1 *Department for Conflict Operations*

Il ruolo senza dubbio principale dell'attività degli operatori per il mantenimento della pace è devoluto alla prevenzione dei conflitti o alla prevenzione della possibile diffusione ulteriore degli stessi.

4.2.2 *Sub-dipartimento per la prevenzione dei conflitti*

Questo sub-dipartimento avrà il compito di istituire quelle che possono essere definite "zone cuscinetto": la creazione delle stesse costituirà uno strumento fondamentale per la protezione delle infrastrutture critiche sia per le parti interessate, che subiscono determinati attacchi informatici, sia per gli stati confinanti, sui quali potrebbero ricadere determinati effetti. Tramite l'istituzione di queste misure e tramite la prevenzione di eventuali attacchi cibernetici con l'utilizzo di queste zone cuscinetto, all'interno delle quali viene implementato il livello di sicurezza delle infrastrutture critiche, risulta possibile evitare una serie di danni e di problemi che porterebbero, in breve tempo, allo scoppio di un

[545] *Ibid.*

[546] *Ibid.*

conflitto[547]. È necessario che l'attività del sub-dipartimento si concentri, inoltre, sull'individuazione di quelle infrastrutture che potrebbero, a seguito di un attacco cibernetico, presentare maggiori difficoltà, dal momento che ciascuno stato possiede una vasta rete di infrastrutture critiche che possono avere una distinta importanza per ciascuno[548]. Le attività che rientrerebbero nelle funzioni del sub-dipartimento qui considerato sono 4: la valutazione dei rischi e delle vulnerabilità per la sicurezza dell'informazione, la prevenzione dei *cyber attacks*, l'individuazione degli stessi ed infine l'elaborazione di una o più possibili risposte[549].

La valutazione dei rischi concerne la collezione e lo studio dei dati che riguardano i rischi per la sicurezza delle informazioni che sono connesse alle infrastrutture critiche delle parti considerate; lo studio degli stessi può permettere all'organo di riuscire a valutare le eventuali vulnerabilità nella sicurezza dell'infrastruttura critica e tutte le sfaccettature con le quali un *cyber attack* potrebbe causare i maggiori danni. Un'analisi efficace dovrebbe avere come base una serie di requisiti tra i quali: completezza, ripetibilità, comparabilità e consistenza[550]. Il parametro di completezza si esplica alla stregua di un'effettiva valutazione, con accorta diligenza, di tutte le possibili vulnerabilità e minacce mentre la ripetibilità fa leva sul fatto che la valutazione, nel momento in cui viene eseguita più volte, deve portare a risultati simili se non identici. La comparabilità invece si riferisce a plurime valutazioni, effettuate a distanza di tempo, che devono essere paragonate tra loro per poter analizzare al meglio i risultati[551].

---

[547] *Ibid.*

[548] Lewis, T. G., Darken, R. P., Mackin, T., & Dudenhoeffer, D. (2012). Model-based risk analysis for critical infrastructures. *WIT Transactions on State-of-the-Art in Science and Engineering, 54*.

[549] Flammini, F. (2012). *Critical infrastructure security: assessment, prevention, detection, response*. WIT Press.

[550] Gallotti, C. (2019). *Information security: Risk assessment; information security management systems; the ISO/IEC 27001 standard*. Cesare Gallotti.

[551] *Ibid.*

La prevenzione degli attacchi cibernetici, invece, comprende due possibilità: la prima prevede direttamente l'applicazione di misure che ostacolano l'eventualità di subire attacchi informatici mentre la seconda si concretizza nella predisposizione di piani di formazione, da mettere a disposizione delle parti che li richiedono, che siano in grado di aiutare gli stati nell'adozione di eventuali misure preventive. Le attività di prevenzione di un *cyber attack* possono consistere nell'installazione di strumenti "*anti-malware*", nella predisposizione di reti più sicure di quelle comunemente usate o anche nel monitoraggio dei file logs[552].

L'individuazione dei *cyber attack* è l'attività più importante che dovrebbe essere effettuata da un organo di questo tipo. Infatti, la stessa prevede l'utilizzo di sensori o altri strumenti tecnologici in grado di monitorare l'attività che viene svolta online ed individuare i casi in cui vengano effettuati movimenti insoliti o tentativi di ingresso in vari siti tramite applicazioni di password erronee o attività che comportano un rallentamento radicale della normale velocità di rete[553]. Tutti questi elementi potrebbero costituire campanelli d'allarme, i quali vanno individuati e studiati, per evitare che gli stessi si propaghino irrimediabilmente e riescano a bloccare tutte le operazioni di rete. Una modalità di individuazione delle attività anzidette potrebbe essere l'applicazione di strumenti cibernetici in grado di rilevare automaticamente dette attività, i quali siano in grado di riconoscere un *cyber attack*[554]. Queste applicazioni si potrebbero spingere anche oltre la "semplice" individuazione di un tentativo di attacco cibernetico, potendo le stesse provare, nel momento in cui dette attività vengono rilevate, a scoprirne l'origine, dando la possibilità alle Nazioni Unite di adottare misure diplomatiche

[552] ZeroUno. (2020, 28 settembre). *Che cosa sono i file log e perché non c'è sicurezza senza log management*. Consultato da https://www.zerounoweb.it/techtarget/searchsecurity/che-cosa-sono-i-file-log-e-perche-non-c-e-sicurezza-senza-log-management/. Definizione di log: «Un log è la registrazione sequenziale e cronologica delle operazioni effettuate da un sistema informatico (server, storage, client, applicazioni o qualsiasi altro dispositivo informatizzato o programma)».

[553] Flammini, *op. cit*., p. 178.

[554] Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. " O'Reilly Media, Inc.".

o aventi differente carattere nei confronti dello stato autore delle attività. Tuttavia, sulla base di quanto rilevato durante la redazione dell'elaborato, quest'ultima operazione potrebbe risultare eccessivamente difficoltosa o particolarmente fuorviante, dal momento che l'identificazione del luogo di provenienza di un attacco potrebbe risultare assolutamente irreale, dal momento che molto spesso gli attacchi vengono sferrati utilizzando sistemi informatici intermedi in grado di impedire il collegamento con il reale autore dell'attacco[555].

L'ultima funzione risulta quella che presenta le maggiori problematiche. Riuscire a adeguare una coerente e proporzionale risposta all'attacco cibernetico può senza dubbio essere in grado di limitare i danni ma deve essere subordinata alla predisposizione e allo sviluppo di un delineato piano di risposta. Un tentativo, in questo senso, è stato ad oggi apprestato dal *National Institute of Standards and Technology (NIST)*, un'agenzia del governo degli Stati Uniti che si occupa dello sviluppo della tecnologia[556]; nel *"Computer security incident handling guide"* vengono evidenziati determinate modalità su come predisporre un efficace piano di risposta[557].

4.2.3. Sub-dipartimento per l'implementazione di accordi di pace

Questo secondo sub-dipartimento si andrebbe ad occupare di attività di implementazione e rispetto di varie e plurime clausole, relative alla sicurezza informatica, stipulate in seguito ad accordi di pace. In particolare, possono esistere clausole che obbligano tutte le parti a scambiarsi informazioni sulle vulnerabilità dei propri sistemi di sicurezza e delle altre parti, clausole che obbligano alla disinstallazione di eventuali malware installati su computer altrui

[555] Liaropoulos, A., & Ryan, J. (2011). War and ethics in cyberspace: cyber-conflict and just war theory. *Leading Issues in Information Warfare & Security Research*, *1*(2).

[556] National Institute of Standards and Technology (NIST). U.S. Department of Commerce. (n.d.). *Official Website Homepage*. Consultato da https://www.nist.gov/

[557] Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.

o ancora clausole che obbligano tutte le parti ad evitare o cessare attacchi informatici[558].

4.2.4 *Department for Stabilisation Affairs*:

Analizzato il primo dipartimento, è necessario procedere allo studio del secondo, il quale svolgerebbe un ruolo fondamentale nel tentativo di stabilizzazione delle relazioni internazionali tra i vari stati, con compiti prevalentemente preventivi, anch'esso suddiviso in due sub-dipartimenti[559]. Infatti, la parte più rilevante delle operazioni di *peacekeeping* in generale riguarda la stabilizzazione, a livello economico, sociale, di sicurezza e governativo di quei paesi che sono stati teatro di un conflitto. L'impellenza del compimento di dette operazioni si riscontra nella necessità di creare delle basi solide per il mantenimento, a lungo termine, della pace e della stabilità nel paese considerato.

L'attività degli operatori nella stabilizzazione e implementazione di una maggiore stabilità a livello sociale si riverbera nella creazione di migliori condizioni da un punto di vista economico e viceversa[560]. Un esempio di ciò si ha nel fatto che il disarmo ed il reinserimento degli ex-combattenti risulta una misura sociale che può portare anche a benefici economici, nel momento in cui gli stessi ex-combattenti si uniscono alla forza-lavoro del paese. È per questo motivo che Almutawa ritiene necessaria la suddivisione in due sub-dipartimenti distinti: il primo improntato all'attuazione di misure che da, un punto di vista sociale ed economico, possano implementare e favorire la creazione di una stabilità che garantirà al meglio la pace da un punto di vista internazionale, il secondo per fronteggiare e fornire un aiuto per migliorare la stabilità governativa e la sicurezza di uno stato. Per garantire la pace e la sicurezza internazionale, e,

[558] Robinson, *op. cit*., p. 121.

[559] Almutawa, *op. cit.*, p. 27.

[560] *Ibid*., (p. 20).

di conseguenza, evitare lo scoppio di un nuovo conflitto, risulta ineluttabile il processo di creazione di una stabilità governativa che sia contraddistinta da un ampio grado di sicurezza, di certezza del diritto per quanto riguarda l'applicabilità delle leggi o di miglioramento dell'attività di intelligence in grado di rilevare tutte le minacce, anche quelle cibernetiche[561].

4.2.5 Il sub-dipartimento per gli affari sociali ed economici

Il sub-dipartimento per gli affari sociali ed economici andrebbe a ricoprire cinque attività distinte: la stabilizzazione successiva ad un "cessate il fuoco" durante un conflitto, l'aiuto e la promozione di una stabilità governativa basata su uno sviluppo economico, la smobilitazione, il disarmo e la reintegrazione degli ex-combattenti, la protezione e la promozione dei diritti umani ed infine la promozione della ripresa e dello sviluppo economico e sociale[562].

Per quanto riguarda il primo punto, è stato riscontrato come, molto spesso, le aree che hanno ospitato un conflitto, nel breve periodo, siano prive di sistemi di telecomunicazioni e sistemi finanziari efficienti, i quali sono alla base del tentativo del raggiungimento di una stabilità nazionale. L'attività del sub-dipartimento per gli affari sociali ed economici si tradurrebbe nel sostegno per la stipulazione di accordi di pace con gli altri stati, fornendo molto spesso garanzie; queste attività possono essere un aiuto concreto nel ripristino delle reti di telecomunicazione e di un sistema finanziario adeguato[563].

Per facilitare il raggiungimento di una stabilità governativa, i *CPK operators* potrebbero istituire determinati sistemi di informazione legale che diano la possibilità ad imprese e civili di raggiungere un livello di consapevolezza dei loro diritti, presenti anche nel mondo cibernetico. Una maggiore conoscenza

[561] Robinson, *op. cit*., p. 121.

[562] Almutawa, *op. cit*., p. 27.

[563] *Ibid*., (p. 14).

delle normative applicabili ad entrambi potrebbe rafforzare la fiducia nelle transizioni commerciali, soprattutto quelle effettuate digitalmente, evitando controversie legali[564]. Molto spesso infatti, i governi statali, soprattutto dopo un conflitto, si trovano in una situazione di difficoltà nella predisposizione di sistemi informativi informatici di qualità, che siano cioè in grado di garantire una veloce ed efficace conoscenza della normativa vigente[565]. L'attività per lo sviluppo economico dei paesi che sono stati luogo di conflitto da parte dei *CPK operators* potrebbe consistere nella predisposizione degli strumenti necessari per ottemperare a suddetta mancanza, tramite la progettazione, il lancio ed il controllo di suddetti sistemi di informazione legale[566].

La terza attività da considerare consisterebbe nello smobilizzo, nel disarmo e nella successiva reintegrazione degli ex-combattenti dello stato che è uscito dal conflitto (DDR activities). A partire dall'inizio nel 1990 si contano più di 60 operazioni di questo tipo autorizzate dal Consiglio di Sicurezza, la maggior parte delle quali sono state lanciate sulla scia di violenti conflitti internazionali o civili e, nonostante ciascuna di esse abbia avuto caratteristiche peculiari, sono sempre state concepite come strumenti di fondamentale importanza per il ripristino della stabilità e della pace internazionale[567]. Le attività DDR sono state definite direttamente dall'ONU come quelle attività che vengono svolte con l'obiettivo di affrontare il problema della sicurezza, in seguito ad un conflitto che si verifica quando i combattenti sono lasciati senza mezzi di sussistenza o reti di supporto[568]. Uno dei maggiori propositi del sub-dipartimento potrebbe essere, su

[564] *Ibid*., (p. 15).

[565] Botero, J. C., Janse, R., Muller, S., & Pratt, C. (Cur.). (2012, 24 settembre). *Innovations in Rule of Law. A Compilation of Concise Essays*. HiiL and The World Justice Project. Consultato da https://worldjusticeproject.org/our-work/publications/edited-volumes/innovations-rule-law-compilation-concise-essays

[566] Almutawa, *op. cit.*, p. 27.

[567] Muggah, R. (2010). Innovations in disarmament, demobilization and reintegration policy and research. Reflections on the last decade. *NUPI Working Papers*. Oslo: The Norwegian Institute for International Affairs. Consultato da https://www.files.ethz.ch/isn/119784/WP-774-Muggah.pdf

[568] United Nations. (2014). *Operational Guide to the Integrated Disarmament, Demobilization and Reintegration Standards.* Consultato da https://www.google.com/search?client=firefox-b-

questo tema, quello di aiutare la ricollocazione e il reintegro nella società lavorativa degli ex-combattenti, favorendo anche la creazione posti di lavoro nel mondo cibernetico, fornendo servizi di formazione digitale[569].

Quella che viene definita come "*demobilisation"* si riferisce al processo, sia fisico che psicologico, che prevede la transizione del combattente dalla vita militare alla vita da "civile". Da un punto di vista cibernetico, il dipartimento potrebbe incanalarlo al ruolo di "*cyber combatants*", aiutandolo ed impiegandolo nei vari sistemi di sicurezza tecnologici[570]. Accanto al disarmo materiale degli armamenti bellici, potrebbe essere necessario il disarmo cibernetico, tramite la distruzione di software in grado di scagliare un attacco cibernetico. Tuttavia, questo processo potrebbe risultare particolarmente difficoltoso per due motivi: il primo è che il software considerato potrebbe anche essere utilizzato per scopi pacifici, mentre il secondo è che le armi cibernetiche possono essere ricreate e raddoppiate in millesimi di secondo, ad un prezzo irrisorio. Per queste motivazioni il disarmo di software potrebbe essere inefficace.

Mentre i primi due processi, seppur di difficile realizzazione, sono senz'altro più rapidi e veloci, quello di reintegrazione nella società può comportare periodi di tempo più elevati. La reintegrazione viene definita come il processo che comporta il passaggio dal ruolo di combattente a semplice civile, con conseguente reinserimento nel mondo del lavoro[571]. La reintegrazione è subordinata al reinserimento sociale degli ex-combattenti che porta gli stessi a intrattenere relazioni e svolgere le proprie attività lavorative quotidiane tra i civili; necessario non è solo il reinserimento all'interno della società con fini basilari, come la garanzia dell'ottenimento di beni primari, ma si deve spingere

---

d&q=United+Nations%2C+%E2%80%98Operational+Guide+to+the+Integrated+Disarmament%2C+Demobilizationand+Reintegration+Standards%E2%80%99+%28United+Nations%2C+2014%29

[569] Almutawa, *op. cit.*, p. 27. (vedi pag. 15).

[570] Robinson, *op. cit.*, p. 121.

[571] Rolston, B. (2007). Demobilization and reintegration of ex-combatants: The Irish case in international perspective. *Social & Legal Studies*, *16*(2), 259-280.

alla realizzazione delle idee e delle capacità degli ex-combattenti[572]. La reintegrazione può avvenire secondo una modalità individuale oppure collettiva, tramite un processo che vedrà la creazione di una comunità di ex-combattenti. Come rilevato antecedentemente, l'attività del sub-dipartimento, nel primo senso, si potrebbe concretizzare nella previsione di corsi di formazione digitale, che sarebbero in grado di fornire le competenze necessarie per gli ex-combattenti per poter svolgere attività lavorative nel settore, cercando sempre di restare nella loro "*comfort-zone*", relativa cioè al tema della sicurezza ma spostata in ambito informatico. Il secondo caso invece potrebbe portare all'adozione di attività che comportino l'eliminazione, tramite attività di consulenza, della glorificazione delle terribili atrocità condotte durante il conflitto[573].

Accanto alle attività DDR, compito del sub-dipartimento considerato sarebbe quello di proteggere e promuovere i diritti umani. La rilevanza di questo tema, come già studiato nel capitolo 2, si ottiene nel momento in cui un eventuale *cyber attack* finisca per comportare una violazione dei principali diritti umani, dato che, riprendendo la definizione fornita dalla *Rule 30* del Tallinn Manual, ha la possibilità di causare danni o addirittura morte a singoli individui. Le operazioni di protezione dei diritti umani si rivolgerebbero, con particolare vigore, alla tutela del diritto alla vita, del diritto alla privacy e del diritto ad esporre ma anche ricevere informazioni e pensieri tramite qualsiasi media[574]. Per quanto attiene al diritto alla vita, compito del CKP team sarebbe quello di proteggere qualsiasi computer network che possa subire un *cyber attack* in grado di cagionare la morte di persone. In questo senso, un aiuto a comprendere la tipologia di attacco considerata ci viene fornito dal Tallinn Manual stesso, nel quale viene esaminato il caso in cui un *cyber attack* manometta il corretto funzionamento del sistema di

[572] Subedi, D. B., & Jenkins, B. (2018). The Nexus between reintegration of ex-combatants and reconciliation in Nepal: A social capital approach. In *Reconciliation in Conflict-Affected Communities* (pp. 41-56). Springer, Singapore.

[573] Machakanja, P. (2014). Reintegration of child soldiers: A case of Southern Sudan. *Building Peace from Within*, 88-90.

[574] Almutawa, *op. cit*., p. 27. (Vedi pag. 17).

purificazione statale dell'acqua; la contaminazione potrebbe portare agli effetti considerati dalla regola[575]. Compito del sub-dipartimento sarebbe tutelare il diritto alla vita tramite l'identificazione dell'imminente *cyber attack* e tramite la sua neutralizzazione.

Per quanto riguarda invece la protezione del diritto di ricevere e fornire informazioni, l'esempio che può essere studiato è quello dell'attacco *Denial of Service,* in grado di manomettere la possibilità di effettuare un libero accesso ad Internet, come avvenuto in Estonia nel 2007[576]. In questo caso, il diritto considerato verrebbe violato. Per questo il sub-dipartimento avrebbe l'obbligo di proteggere i computer ed i sistemi informatici che potrebbero essere più facilmente scagliati contro i paesi che sono appena usciti da un conflitto e che si trovano ancora in una situazione di instabilità. Anche in questo caso le misure adottabili potrebbero comprendere la predisposizione di "*training courses*", in grado di spiegare le modalità possibili di risposta ad un attacco di quel tipo[577]. La promozione dei diritti umani potrebbe essere implementata tramite l'indizione di incontri, a cui sarebbero invitati i principali studiosi dei diritti umani, per rendere edotte le persone che vi partecipano dei loro diritti[578].

Infine, la promozione della ripresa e dello sviluppo economico e sociale potrebbe avvenire tramite attività di sviluppo dell'istruzione online e tramite la predisposizione di vantaggi volti a stimolare l'e-commerce.

---

[575] Schmitt, M. N. (Cur.). (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

[576] Ottis, R. (2008). Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare* (p. 163).

[577] Whitman, M. E., Mattord, H. J., & Green, A. (2013). *Principles of incident response and disaster recovery*. Nelson Education.

[578] Freedman, R. (2013). *The United Nations Human Rights Council: A Critique and Early Assessment*. Routledge.

4.2.6 Sub-dipartimento per gli affari e la sicurezza dello stato

L'ultimo sub-dipartimento dell'organo prospettato è quello che si occuperebbe degli affari dello stato e della sicurezza. Le attività che questo dipartimento andrebbe a svolgere sono quelle rimanenti e si articolano in attività di: facilitazione nella transizione verso un governo stabile basato su principi democratici, aiuto nella redazione di riforme del settore della sicurezza ed implementazione della certezza del diritto, rimozione di mine ed azioni anti-malware, assistenza nella redazione di un corretto sistema elettorale ed infine supporto nella ricostruzione dell'autorità dello stato che è appena uscito da un conflitto[579].

La facilitazione della transizione verso un governo stabile avverrebbe tramite tre misure distinte per supportare il nuovo governo legittimamente eletto. La prima di queste consisterebbe nella creazione di sistemi di formazione online, i quali sarebbero in grado di essere utilizzati per formare ufficiali governativi. Un governo stabile, per un corretto funzionamento, necessita di ufficiali governativi qualificati, che siano in grado di affrontare tutte le problematiche, anche e soprattutto quelle derivanti dal mondo cibernetico. Il lavoro in questo senso ricalcherebbe quello svolto dall'*United Nations Institute for Training and Research* (UNITAR), il quale ha più volte svolto corsi di formazione destinati ai soggetti degli stati che sono usciti da un conflitto[580]. La seconda attività riguarderebbe l'implementazione di una cultura cibernetica, diretta prevalentemente ai cittadini. La conoscenza del mondo online e dei diritti che sono riconosciuti all'interno dello stesso garantirebbe ai cittadini uno strumento ulteriore per far fronte alle attività statali ingiuste. In questo senso, il sub-dipartimento lavorerebbe cercando di espandere la possibilità di accesso alla

[579] Almutawa, *op. cit.*, p. 27. (Vedi pag. 20).

[580] United Nations Institute for Training and Research (UNITAR). (2021). *Official Website.* Consultato da https://unitar.org/

rete[581]. L'ultima attività, infine, consisterebbe nell'aumento della protezione del sistema di sicurezza di raccolta dei dati[582].

Per quanto invece riguarda l'aiuto nella redazione di riforme del settore della sicurezza, il sub-dipartimento potrebbe istituire percorsi formativi aggiunti per coloro che opereranno nel settore di sicurezza statale, per fornire agli stessi migliori strumenti di difesa e conoscenze amplificate. Questi processi di formazione risulterebbero particolarmente fruttuosi, dal momento che i *CPK operators* dovrebbero essere specializzati nello sviluppo cibernetico di paesi che sono ancora lontani dagli standard di sicurezza ritenuti necessari[583].

La terza attività del dipartimento comprenderebbe la rimozione di mine cibernetiche e di malware. Il tema delle mine rimaste inesplose, successivamente ad un conflitto, è stato oggetto di studio approfondito da parte dell'ONU, tanto che, da un punto di vista prettamente dinamico (per il momento), è stato istituito il "servizio di azione contro le mine" (UNMAS)[584]; quest'ultimo lavora per eliminare la minaccia delle mine rimaste inesplose e per distruggere i residui esplosivi di guerra. Il dipartimento considerato garantirebbe un maggiore supporto alle operazioni di UNMAS, soprattutto per quanto riguarda i servizi di consulenza per la sicurezza dei software che contengono le informazioni sulle mine[585]. Dall'altra parte, la rimozione di malware comprenderebbe il rilevamento e la neutralizzazione di quelli che si trovano dentro le reti informatiche degli stati che sono appena usciti da un conflitto. Allo stesso modo, il sub-dipartimento

[581] Yangyue, L. (2014). *Competitive political regime and Internet control: Case studies of Malaysia, Thailand and Indonesia*. Cambridge Scholars Publishing.

[582] Almutawa, *op. cit*., p. 27. (Vedi p. 22).

[583] Karake, Z., Shalhoub, R. A., & Ayas, H. (2019). *Enforcing Cybersecurity in Developing and Emerging Economies.* Institutions, Laws and Policies. Edward Elgar Publishing. Consultato da https://www.e-elgar.com/shop/gbp/enforcing-cybersecurity-in-developing-and-emerging-economies-9781785361326.html

[584] United Nations Mine Action Service (UNMAS). (n.d.). *Who we are.* Consultato da https://unmas.org/en/who-we-are

[585] Almutawa, *op. cit*., p. 27.

potrebbe fornire le indicazioni e gli strumenti necessari agli stati per prevenire la diffusione dei malware considerati e impedire danni incalcolabili[586].

Le attività di assistenza nello svolgimento dell'attività elettorale si basano sul diritto riconosciuto all'art.21 della "*Universal Declaration of Human Rights*", il quale garantisce il diritto a chiunque di partecipare al governo del proprio paese, sia direttamente che indirettamente[587]. Anche se la maggior parte delle elezioni vengono svolte tramite strumenti cartacei, il diritto può essere violato tramite una serie di attività cibernetiche. Come già evidenziato nel corso dell'elaborato, infatti, determinate operazioni cibernetiche possono andare ad alterare il corretto funzionamento del processo elettorale, come avvenuto negli Stati Uniti nel 2016, con la diffusione di *fake news* in grado di screditare il candidato democratico Hillary Clinton, a favore di Donald Trump[588]. L'operato demandato al dipartimento considerato sarebbe contraddistinto dal supporto nell'identificazione e nelle misure adottabili contro simili attività, ma anche nel sostegno della creazione di un sistema elettorale online, il quale andrebbe a ridurre notevolmente il costo delle spese elettorali, pur riscontrando una maggiore sfiducia dei cittadini[589].

Infine, l'ultima attività del dipartimento prevede il supporto nella ricostruzione dell'autorità dello stato che è appena uscito da un conflitto. Essendo la comunicazione uno degli elementi focali per permettere la ricostruzione dell'autorità dello stato, il sub-dipartimento potrebbe supportare i governi nella creazione di sistemi online per la comunicazione intra-governativa. La creazione di questi sistemi di e-governance permettono una migliore e maggiore

[586] *Ibid.*

[587] United Nations. (n.d.). *The Universal Declaration of Human Rights.* Consultato da https://www.un.org/en/universal-declaration-human-rights/

[588] Mueller, R. S. (2019). *The Mueller report: Report on the investigation into Russian interference in the 2016 presidential election*. WSBLD.

[589] Hartami, A., & Handayani, P. W. (2012, giugno). The critical success factors of e-voting implementation in Indonesian local elections: The case of Jembrana regency election. In *ECEG2012-Proceedings of the 12th European Conference on e-Government: ECEG* (p. 336). Academic Conferences Limited.

interazione con i cittadini che si sentono più sicuri, dal momento che gli stati possono creare determinati siti web di accesso pubblico che permettano il controllo dell'operato da parte degli individui[590]. Il dipartimento potrebbe altresì aiutare lo stato nella creazione di infrastrutture governative elettroniche che permettano ai cittadini di ottenere una visione generale e più ampia[591].

4.3 Principali problematiche

La realizzazione di operazioni di *cyber peacekeeping* risulta tutt'altro che facile. Le prime problematiche che derivano da una mancanza di uniformità di visioni che intercorrono tra i vari stati del mondo per quanto concerne l'attività cibernetica. In particolare, non avere una definizione universalmente accettata dei vari temi trattati in questo elaborato, come quello di *cyber defense*, *security* o *attack*, complica notevolmente il lavoro, dal momento che la maggior parte degli studi, come quello di Almutawa, devono avvenire su basi strettamente teoriche o, comunque sia, non vincolanti.

La prima critica che viene mossa all'istituzione di attività di CPK fa leva sul fatto che nessuno, ad oggi, degli stati membri delle Nazioni Unite ha richiesto lo svolgimento delle attività fino a questo momento considerate. Anche se ciò probabilmente deriva da una mancanza di chiarezza e di sicurezza relativa alla natura delle stesse, non è stata avvertita la necessità di avere simili operazioni, probabilmente sulla base del carattere assolutamente innovativo rappresentato da queste operazioni[592]. Accanto a ciò, è possibile analizzare cinque aspetti che costituiscono le principali critiche alla creazione di un organo abilitato a svolgere le anzidette attività.

---

[590] Kamal, M. M., Hackney, R., & Sarwar, K. (2013). Investigating factors inhibiting e-government adoption in developing countries: the context of Pakistan. *Journal of Global Information Management (JGIM), 21*(4), 77-102.

[591] Almutawa, *op. cit*., p. 27. (Vedi p. 25).

[592] Dorn, *op. cit*., p. 171.

La prima si riscontra nella mancanza di competenze ma soprattutto risorse[593]. Al giorno d'oggi le Nazioni Unite non dispongono della capacità e delle competenze che risultano necessarie per l'efficacia di dette operazioni; manca difatti una conoscenza approfondita e non approssimativa di temi che risultano fondamentali, come la conoscenza della struttura dei virus informatici più sofisticati, delle singole sfaccettature del dark web o delle capacità nazionali relative alla *cyber warfare*. Per colmare queste lacune, i singoli stati dovrebbero mettere a disposizione della collettività le rispettive competenze informatiche e le conoscenze dei propri esperti cibernetici, se non addirittura direttamente questi ultimi[594]. Inoltre, non tutti gli stati si contraddistinguono per un elevato numero e livello di esperti. Essendo questo l'unico modo per implementare la conoscenza degli operatori ONU, si potrebbe raggiungere anche un conflitto di interessi, dal momento che gli esperti potrebbero essere portatori di semplici interessi nazionali, non della collettività. Inoltre, la mancanza di un regime internazionale di sicurezza informatica non può durare in eterno dal momento che, in futuro, quest'ultimo sarà necessario per regolare la sempre maggiore attività degli stati nel *cyberspace*[595].

In aggiunta a ciò, sebbene l'attività di CPK sia stata identificata come una "futura area di ricerca" indicativamente agli inizi del XXI secolo, il concetto viene, nella maggior parte dei casi, visto come innovativo[596]. Gli stessi scarsi studi giuridici sul problema rilevano un altrettanto limitato dibattito. Questo avviene prevalentemente per il fatto che moltissimi stati si sono dimostrati totalmente lontani da quest'idea di visione collettiva dal momento che potrebbero emergere situazioni spiacevoli per gli stessi: il CPK team potrebbe infatti rivelare e

[593] Nabeel, *op. cit*., p. 174.

[594] *Ibid.*

[595] Dorn, A. W., & Webb, S. (2019). Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 9(1), 19-30.

[596] *Ibid.*

constatare l'esistenza di attività segrete adottate dai singoli stati nel cyber spazio che gli stessi cercano di mantenere segrete[597].

Inoltre, alcuni ritengono che la creazione di una forza per il mantenimento della pace da un punto di vista informatico possa essere una misura assolutamente ridondante, dal momento che i meccanismi di mantenimento di pace già esistenti dovrebbero essere in grado, autonomamente e senza implementazioni, di andare a ricoprire ed a fronteggiare anche tutti gli attacchi informatici, tramite l'esistente cooperazione intergovernativa[598]. In aggiunta, l'istituzione di un nuovo organo con funzioni, strumenti e dipendenti propri, presenterebbe costi elevati, seppur senza dubbio inferiori rispetto a quelli sostenuti per effettuare le dinamiche attività di *peacekeeping*[599].

Un ulteriore elemento di discussione è rappresentato dalle difficoltà che avrebbe un CPK team nel riuscire ad operare solo ed unicamente nel campo di battaglia virtuale, senza andare a svolgere attività all'interno del campo di battaglia fisico, già ampiamente tutelato dagli operatori di mantenimento della pace tradizionali[600]. Questo argomento si sviluppa partendo dalle difficoltà relative all'inesistenza di confini fisici predefiniti in cui operare, essendo il *cyberspace* un mondo privo di delimitazioni territoriali. Tuttavia, secondo alcuni studiosi, questa incertezza non impedirebbe lo svolgimento di attività di CPK, dal momento che la stessa natura della *cyber warfare* risulta non pienamente comprensibile[601].

L'inesistenza di un quadro giuridico unitario, tuttavia, è la problematica che maggiormente tocca il tema delle *CPK operations*; infatti, un numero elevato di questioni relative alla conduzione delle stesse ed al loro fondamento giuridico

[597] *Ibid.*

[598] Phneah, *op. cit.*, p. 174.

[599] *Ibid.*

[600] *Ibid.*

[601] Robinson, *op. cit*., p. 121.

sono state avanzate e continueranno ad essere proposte. È utile ricordare come, al giorno d'oggi, manchi un vero e proprio meccanismo univoco e universalmente accettato che sia in grado di determinare quando un attacco cibernetico possa costituire un atto di guerra[602]. Nel caso, inoltre, in cui venisse superata la soglia e si giungesse ad un conflitto armato, gli operatori di pace diventerebbero inevitabilmente parti del conflitto, con conseguenti dubbi relativi alla natura e durata del loro ruolo. Tuttavia, la maggior parte degli ostacoli giuridici potrebbe essere superata tramite una valutazione caso per caso, tenendo sempre in considerazione l'operatività e i limiti che verrebbero imposti tramite il mandato e tramite altri elementi rilevanti come le risoluzioni dei CdS, l'adozione di mandati specifici, la natura degli armamenti usati dai *cyber peacekeepers*[603].

Come abbiamo visto, l'attività dei *PK operators* dovrebbe essere subordinata al rispetto dei diritti umani, oltre che alla promozione ed alla protezione degli stessi. Nonostante questo, in diverse occasioni le truppe tradizionali di *peacekeeping* (i cosiddetti "caschi blu") si sono macchiate, nello svolgimento della propria attività, del compimento di una serie di violazione dei diritti umani, tra cui la realizzazione di abusi e di violenze sessuali, o ancora attività comprendenti la tortura o la detenzione arbitraria contro i locali[604]. Il numero di accuse è inoltre aumentato notevolmente nel corso degli ultimi anni, come rilevato dal Segretario Generale: il personale delle Nazioni Unite avrebbe infatti approfittato della situazione "vantaggiosa" derivante dagli effetti che il conflitto aveva creato, quali un'estrema povertà ed un aumento dello sfruttamento sessuale, in cui si trovava[605]. Inoltre, accanto a queste situazioni, gli operatori di pace potrebbero

[602] *Ibid.*

[603] Nabeel, *op. cit.*, p. 174. (Vedi p. 21).

[604] Dannenbaum, T. (2010). Translating the standard of effective control into a system of effective accountability: how liability should be apportioned for violations of human rights by member state troop contingents serving as United Nations peacekeepers. *Harv. Int'l LJ*, *51*, 113.

[605] United Nations General Assembly. (2017, 28 febbraio). *Special measures for protection from sexual exploitation and sexual abuse.* UN Doc A/70/729, 7. 2016 Report of the Secretary-General. Consultato da https://peacekeeping.un.org/sites/default/files/sg_report_a_71_818_special_measures_for_protection_from_sexual_exploitation_and_abuse.pdf

trovare una "forza maggiore" nel compimento di attività che comportano violazioni dei diritti umani, sulla base di quanto previsto espressamente dall'art. 105 della Carta delle Nazioni Unite[606]. L'art.105 statuisce che le Nazioni Unite godano di privilegi ma soprattutto di immunità nel territorio dei suoi stati membri, dal momento che queste previsioni risultano assolutamente necessarie per il perseguimento degli scopi dell'organizzazione internazionale. Accanto a questo, viene stabilito che i privilegi dovrebbero essere concessi a tutti i membri e ai funzionari delle Nazioni Unite, per dare la possibilità a questi ultimi di svolgere correttamente le funzioni che vengono loro attribuite. La previsione contenuta all'art.105 è stata implementata dalla Convenzione sulle Immunità, la quale statuisce che :

«*immunity shall be granted to the UN, its properties and funds*».[607]

In aggiunta a questa previsione, l'immunità dovrebbe essere garantita anche ai rappresentanti dell'ONU nel mondo, ai suoi ufficiali ed anche agli esperti che vengono autorizzati nelle missioni. Secondo l'ICJ, le disposizioni contenute nella Convenzione forniscono una piena immunità nei confronti di qualsiasi processo legale davanti a giudici nazionali per gli atti imputabili all'organizzazione[608]. Le immunità fino a qui considerate si estenderebbero, da un punto di vista teorico, anche alle *peacekeeping forces*[609]; è stato rilevato, tuttavia, come, da un punto di vista pratico, gli operatori godano di immunità assolute, sulla base della possibile stipulazione di accordi tra l'ONU e il paese ospitante le truppe stesse[610]. Quanto fino ad ora analizzato permette di capire come i problemi relativi alla

[606] United Nations, *op. cit.*, p. 189. Vedi art. 105.

[607] United Nations Treaty Collection. (2021). *Status of Treaties.* Consultato da https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-1&chapter=3&clang=_en

[608] International Court of Justice. (n.d.). *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (1998)*. Consultato da https://www.icj-cij.org/en/case/100

[609] Lewis, P. J. (2013). Who Pays for the United Nations' Torts: Immunity, Attribution, and Appropriate Modes of Settlement. *NCJ Int'l L. & Com. Reg., 39*, 259.

[610] Helmner, A. (2016). *Human Rights Violations of Peacekeeping Troops: Accountability of the UN and the Relationship to the ECHR*. (Vedi pag. 11).

creazione di un *CPK team* potrebbero insorgere anche in questo senso. In particolare, tenuto conto del lavoro online che verrebbe svolto da queste truppe cibernetiche, una difficoltà ulteriore potrebbe essere rappresentata da violazioni di diritti umani, i quali come già studiato vengono riconosciuti anche online; garantendo un ampio accesso alle reti informatiche del paese, gli operatori si potrebbero macchiare di plurime violazioni. I diritti umani potrebbero essere senza dubbio protetti, tutelati e promossi ma al tempo stesso potrebbero essere vittime di plurime violazioni, il diritto alla privacy fra tutti[611].

4.4 La responsabilità internazionale dello Stato per gli attacchi cibernetici

Il tema della responsabilità per le operazioni compiute dagli stati assume una particolare rilevanza nel diritto internazionale. Innanzitutto, la responsabilità statale internazionale sembra essere emersa, nel corso del tempo, su basi analogiche di responsabilità contenute all'interno del diritto privato statale[612]. Come rilevato dall'allora Permanente Corte di Giustizia Internazionale, nello studio del caso "*Factory at Chorzów"* [613], qualsiasi violazione di un determinato impegno, anche e soprattutto se assunto a livello internazionale, comporta l'obbligo di una riparazione. Il diritto contemporaneo che si occupa della responsabilità degli stati ha, come principale fonte di riferimento, gli articoli relativi alla responsabilità degli stati per atti illeciti a livello internazionale (ARS), adottati dalla "*International Law Commission*" (ILC) nel 2001[614]. Il testo non è un trattato; tuttavia, dal 2001 ad oggi è stato talmente tante volte ripreso dalle corti e dai tribunali internazionali da essere considerato come una

[611] Nabeel, *op. cit*., p. 174.

[612] Lauterpacht, H. (2002). *Private law sources and analogies of international law: with special reference to international arbitration*. The Lawbook Exchange, Ltd..

[613] Factory at Chorzow (Germ. v. Pol.), 1927 P.C.I.J. (ser. A) No. 9 (Luglio 26).

[614] International Law Commission (ILC). (2021). *Official Website*. Consultato da https://legal.un.org/ilc/

dichiarazione autorevole del diritto internazionale consuetudinario sulla responsabilità degli stati[615].

Come chiarito all'art.2, il punto cardine è il compimento di un atto illecito, il quale si articola nella constatazione di due elementi distinti ai fini della presenza di una responsabilità internazionale statale: il primo enfatizza il tema dell'attribuzione dell'atto illecito allo stato mentre il secondo si focalizza sulla violazione di un'obbligazione internazionale[616]. Il rafforzamento di questi due elementi si può riscontrare nel caso "*Phosphates in Morocco*"[617]. Per attribuzione si intende la possibilità di allegare un determinato atto o una determinata omissione ad uno stato; per eseguire detto collegamento è possibile rifarsi, in una prima battuta, all'identità delle persone naturali che hanno svolto l'attività considerata ma soprattutto alla loro relazione con uno stato in particolare[618]. Come infatti rilevato dai commentari sull'art.2, gli stati inevitabilmente saranno portati ad agire tramite persone fisiche o gruppi; di conseguenza il problema dell'attribuzione si "riduce" principalmente all'individuazione delle persone ed al tentativo di ricondurre l'attività degli stessi alle volontà statali[619]. Gli articoli considerati, pur essendo incentrati principalmente sull'individuazione dell'identità dell'individuo come criterio di attribuzione allo stato, non escludono la possibilità di ammettere la responsabilità dello stato per un atto o per un'omissione dei suoi cittadini che, si presume, siano sotto il controllo dello stesso[620]. Pertanto, sulla base dell'esistenza di diversi gli requisiti che saranno analizzati, si ha la responsabilità dello stato per atti od omissioni commessi da parte delle seguenti categorie di individui: si avrà una attribuzione per quei

---

615 Crawford, J. (2019). *Brownlie's principles of public international law*. Oxford University Press, USA.

616 United Nations. (2005). *Responsibility of States for Internationally Wrongful Acts*. Consultato da https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdff

617 Phosphates in Morocco (Italy v. Fr.), 1938 P.C.I.J. (ser. A/B) No. 74 (giugno 14).

618 Ibid., (p. 127).

619 United Nations. (2008). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Consultato da https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

620 Tsagourias, *op. cit*., p. 61. (Vedi p. 59).

soggetti che *de jure* sono agenti dello stato o per gli organi statali, indipendentemente dalla loro posizione gerarchica all'interno dell'apparato dello stato o della sua struttura (Art.4)[621], mentre si avrà un'attribuzione allo stato nel caso di attività od omissioni compiute da quei soggetti, quali attori non statali o varie entità che, essendo sotto la direzione e la dipendenza assoluta dello stato, sono stati elevati ad organi statali *de facto*[622].

Il secondo requisito invece si concretizza nella violazione di un obbligo derivante dal diritto internazionale, la quale può consistere nel compimento di un atto o in un'omissione che è imposta o da una norma di diritto consuetudinario o da un trattato, in grado di imporre un obbligo per lo stato considerato[623]. La responsabilità di uno stato per violazione di un obbligo può insorgere sia sulla base del compimento di un atto singolo sia nel caso in cui una singola violazione si verifichi in un'attività continuata.[624]

4.4.1 La responsabilità statale nel *cyberspace*

Non vi è, al giorno d'oggi, motivo per negare l'applicabilità della disciplina qui considerata anche al regime del *cyberspace*[625]. L'importanza del regime della responsabilità statale generale viene presa in considerazione per riuscire a determinare la responsabilità di uno stato per le operazioni che lo stesso compie nello spazio cibernetico. Come rilevato più volte nel corso del lavoro, il cyber spazio solleva problemi molto più pressanti per il requisito dell'attribuzione di una condotta. Infatti, l'identificazione di singoli individui o enti che utilizzano Internet è contraddistinta da notevoli difficoltà, derivante ciò dal fatto che l'anonimato e la possibilità di negare il compimento delle operazioni o depistarne

[621] United Nations (2008)., *op. cit.*, p. 196.

[622] *Ibid.*

[623] United Nations (2008)., *op. cit.*, p. 196. (Vedi art. 12-13).

[624] United Nations (2008)., *op. cit.*, p. 196. (Vedi art. 14-15).

[625] Tsagourias, *op. cit.*, p. 61. (Vedi p. 62).

la ricerca risulta relativamente semplice[626]. Così, quasi sempre, risulta impossibile andare a determinare, con assoluta certezza, la persona o l'entità che agisce utilizzando un *personal computer*. L'attribuzione, che non per forza fornirà l'indicazione della persona che ha oggettivamente causato la violazione di un obbligo internazionale per lo stato, può solo avvenire tramite la ricostruzione ed il ricollegamento dell'indirizzo IP del computer, il quale fornirà unicamente una precisa geolocalizzazione. Pertanto, un atto illecito a livello internazionale sembra essere attribuito solo ad uno o più computer particolari, mentre l'identità della persona che agisce potrà, successivamente, essere conosciuta tramite presunzioni o sulla base di informazioni interne possedute dagli agenti governativi dello stato che è sospettato della violazione di un obbligo internazionale[627]. Partendo da quanto fin qui analizzato, la localizzazione di un computer all'interno di uno stato, con conseguente scoperta della natura di "*government computer*" dal quale è stato diffuso un malware o un attacco *denial of service*, potrebbe portare all'attribuzione dell'attività allo stato stesso. Questa presunzione sembra essere possibile indipendentemente dall'identità dell'operatore che ha effettivamente lanciato l'attacco o diffuso il malware, presumendo altresì che lo stesso sia un agente governativo o che, comunque sia, vi fosse per lo stato un obbligo effettivo di controllo sull'operato dei computer governativi[628].

Dopo aver fornito questa visione generale, è necessario passare all'analisi di quanto sottolineato nel Tallinn Manual in tema di responsabilità statale nel *cyberspace*, con particolare riferimento alle *Rule 6, 7*, e *8*.

La *Rule 6* sottolinea quanto segue:

---

[626] *Ibid.*

[627] Aljazeera America. (2013). *Timeline of Edward Snowden's revelations. Guardian announces leak of classified NSA documents.* Consultato da http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

[628] Tsagourias, *op. cit.*, p. 61. (Vedi p. 62).

«A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation».[629]

Nello stesso modo previsto per le operazioni dinamiche, anche le operazioni cibernetiche saranno regolate dalla disciplina prevista in tema di responsabilità statale dalle ARS. Ai fini della verificazione della responsabilità sarà necessario valutare sia la questione dell'attribuzione della condotta ad uno stato e della violazione di un obbligo internazionale. Nel regime del *cyberspace*, una violazione del diritto internazionale può consistere nella rottura di un obbligo derivante da una delle previsioni contenute nella Carta delle Nazioni Unite o dalle obbligazioni previste dalla normativa sui conflitti armati. Allo stesso modo, una violazione cibernetica di regole che non riguardano il conflitto, come ad esempio una violazione del principio di non intervento e della legge del mare, possono costituire violazioni del diritto internazionale che fanno insorgere una responsabilità[630]. Come è facilmente intuibile, la disciplina applicabile per determinare quando uno stato incorra nella responsabilità internazionale si ha nel caso in cui l'atto o l'omissione comporti una violazione del diritto internazionale mentre non verrà attribuita nel caso in cui quelle attività siano permesse o non siano regolate dal diritto internazionale stesso[631]. Un esempio che viene riportato è quello dello spionaggio cibernetico; dal momento che il *cyber espionage* non è regolato dal diritto internazionale, l'attuazione dell'attività da parte di uno stato non fa insorgere una responsabilità dello stesso in sé e per sé, sempre che particolari aspetti dello spionaggio non vadano a violare specifiche proibizioni internazionali (come nel caso di spionaggio di agenti diplomatici)[632]. In linea di

[629] Schmitt, M. N. (Cur.). (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

[630] *Ibid*., (p. 36).

[631] Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, I.C.J. Reports 2010, p. 403.

[632] *Rule 84* Tallinn Manual.

massima, la presenza di un danno non è considerata una condizione preliminare per poter qualificare un'operazione informatica come un illecito internazionale dal quale deriva una responsabilità statale[633]. Tuttavia, la regola in questione potrebbe arrivare a considerarlo come necessario.

Per costituire la violazione di un'obbligazione internazionale, l'atto o l'omissione considerata, anche nel mondo cibernetico, deve risultare attribuibile ad uno stato. In particolare, come precedentemente evidenziato, in questo senso tutti gli atti compiuti da organi dello stato nell'esercizio delle loro attività sono attribuibili allo stato automaticamente. Tutte quelle attività cibernetiche effettuate dal corpo militare, dalle agenzie di intelligence, dagli organi di sicurezza interna comporteranno una responsabilità dello stato, qualora le stesse causino una violazione di un obbligo giuridico internazionale applicabile a quello stato[634]. Se gli atti vengono inoltre compiuti dagli organi in questione, ai fini dell'attribuzione della responsabilità allo stato, risulta del tutto irrilevante che il compimento degli stessi sia avvenuto in conformità o meno delle istruzioni impartite; la responsabilità dello stato si avrà anche nel caso in cui nessuna informazione sia stata fornita. Nel caso in cui vengano posti in essere atti *ultra vires* dagli organi fino a questo momento considerati, insorgerà una responsabilità uguale dello stato, qualora l'organo considerato abbia agito, anche solo apparentemente, nell'esercizio delle sue facoltà[635]. Allo stesso modo, quei soggetti che, pur non essendo considerati operatori di organi dello stato, si vedono attribuita un'autorità governativa sono equiparati ad organi statali e, quando agiscono spendendo detta autorità, provocano l'assegnazione delle condotte direttamente allo stato[636].

[633] United Nations (2008), *op. cit.*, p. 196.

[634] Schmitt, *op. cit.*, p. 19.

[635] United Nations (2008), *op. cit.*, p. 196. (Vedi p. 36).

[636] *Ibid.*

In determinate circostante, si ha la possibilità di far rientrare l'attività di attori non statali all'interno di quegli atti che fanno insorgere una responsabilità internazionale per lo stato stesso. L'art.8 dell'ARS, infatti, sottolinea come "il comportamento di una persona o di un gruppo di persone è considerato un atto di uno stato ai sensi del diritto internazionale se la persona, o il gruppo, hanno agito sulla base di istruzioni o sotto la direzione o il controllo dello stato"[637]. Questa norma risulta particolarmente rilevante dal momento che molto spesso gli stati, per evitare diretti collegamenti alla propria volontà, si sono rivolti a privati cittadini o ad esperti per sviluppare strategie ed operazioni cibernetiche contro altri stati[638]. Chiaramente, queste situazioni sono totalmente diverse dal caso in cui i privati cittadini, di loro propria iniziativa, conducano cyber operazioni. Infatti, se mancassero istruzioni, direzione o controllo risulterebbe troppo gravoso far emergere una responsabilità dello stato; inoltre è stato rilevato come incoraggiare o esprimere supporto, da parte dello stato, per il compimento di atti indipendenti da parte di attori non statali non superi la soglia che comporta l'applicabilità dell'art.8[639].

Inoltre, nell'ambito delle operazioni militari, uno stato viene considerato responsabile, sulla base di quanto asserito dalla Corte Internazionale di Giustizia, anche per le azioni compiute da attori non statali se, nei loro confronti, godeva della possibilità di avere un "controllo effettivo"[640], anche se questo aspetto sarà meglio trattato nel paragrafo conclusivo, relativo agli obblighi di *due diligence.*

Il compimento di operazioni cibernetiche risulta ampiamente fuorviante per quanto riguarda il luogo dove le stesse vengono attuate e la capacità di nascondere, in questo modo, il reale soggetto che compie l'attività. Per questo motivo, è stato previsto che il luogo in cui viene svolta l'operazione cibernetica,

---

[637] *Ibid.*, (p. 47).

[638] Schmitt, *op. cit.*, p. 19. (Vedi p. 37).

[639] *Ibid.*

[640] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984. (Vedi p. 392).

che comporta una violazione di un'obbligazione internazionale, risulta, ai fini dell'attribuzione della responsabilità, non direttamente rilevante. Un esempio riportato dal gruppo di esperti che ha redatto il Tallinn Manual può essere illuminante[641]. Il caso concerne un gruppo di operatori informatici che risiedono nello stato A, i quali riescono ad insediarsi nel sistema di computer dello stato B e, su indicazione dello stato C, sovraccaricano i sistemi informatici di uno stato D. In questo caso, non si può presumere una responsabilità internazionale da parte di A per il solo fatto che l'attività cibernetica è effettivamente partita dentro il suo territorio; allo stesso modo, essendo l'attacco scagliato dai computer dello stato B indirettamente, B non può essere ritenuto responsabile. Solo lo stato D, per le informazioni e le indicazioni fornite, può essere ritenuto responsabile di una violazione del diritto internazionale.

Quest'ultimo elemento viene ripreso dalla *Rule 7*, la quale evidenzia come il semplice fatto che un'operazione cibernetica sia stata avviata o abbia comunque origine da qualche infrastruttura governativa non è di per sé una prova sufficiente per attribuire l'operazione ad uno stato ma indica semplicemente che lo stato in questione è associato con l'operazione[642]. Questo articolo fa riferimento solo alle operazioni avviate e non riguarda le operazioni che semplicemente passano tramite tali infrastrutture, cui è dedicata la *Rule 8*. Inoltre, risulta del tutto indifferente se la proprietà delle infrastrutture sia dello stato o dei privati cittadini. In sé e per sé l'articolo non costituisce una base giuridica per intraprendere un'azione volta ad accertare la responsabilità dello stato o per ritenerlo responsabile degli atti in questione[643]. Mentre l'approccio tradizionale infatti prevedeva una maggiore facilità nel ritenere responsabile uno stato sulla base dell'utilizzo di risorse governative, soprattutto militari, a causa dell'improbabilità del loro utilizzo da parte di individui o gruppi non autorizzati

[641] *Ibid.*

[642] Schmitt, *op. cit.*, p. 19. (Vedi p. 39).

[643] *Ibid.*

dal governo a ciò, con l'avvento delle operazioni cibernetiche la situazione si è completamente ribaltata, dal momento che un'infrastruttura informatica del governo potrebbe essere soggetta essa stessa ad un attacco da parte di privati che cercano di utilizzare le sue funzionalità[644].

Per concludere, mentre la *Rule 7* si riferisce ad attività iniziata o effettuata tramite le infrastrutture cibernetiche governative, la *Rule 8*, dall'altra parte, esplica che l'attività di semplice attraversamento dei sistemi informatici delle infrastrutture governative da parte di una *cyber operation* non sia sintomo sufficiente per attribuire l'operazione allo stato[645]. Le caratteristiche e la natura del cyberspazio permettono spostamenti di attività, operazioni e dati in millesimi di secondo e la mancanza di delimitazioni territoriali rafforza la velocità delle operazioni stesse. Di conseguenza, uno stato non potrà incorrere in una responsabilità internazionale in questo caso, dal momento che molto spesso l'attività considerata è del tutto imprevedibile e lo stato non presenta nessun grado di coinvolgimento nell'operazione, essendo lo stesso spesso vittima di un'intrusione[646].

Tuttavia, queste ultime due *Rules* hanno presentato determinate difficoltà dal momento che la *Rule 5* fa riferimento ad un tema di particolare importanza: il rispetto del principio di "*due diligence*" da parte degli stati[647]. Il Manuale di Tallinn del 2013 è focalizzato prevalentemente sulla normativa applicabile in tempo di guerra e non in tempo di pace[648]. Per questo, le operazioni di *due diligence* sono solo trattate in maniera limitata. L'ampliamento dello studio della seguente obbligazione è stato oggetto di un ampio dibattito nella redazione del

[644] *Ibid.*

[645] *Ibid.*

[646] *Ibid.*

[647] *Ibid.*

[648] Schmitt, M. N. (2015-2016). In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum, 125*, 68-81.

Tallinn Manual 2.0, il quale dedica al tema un paragrafo intero del primo capitolo, composto dalla *Rule 6* e *7* [649], le quali meritano una trattazione separata.

4.4.2 La responsabilità delle organizzazioni internazionali applicabile alle operazioni di pace

Prima di passare all'analisi finale riguardante il concetto dell'applicabilità del principio di *due diligence* nel cyberspazio in un'ottica di attribuzione della responsabilità, è necessario esaminare, quantomeno sommariamente, le difficoltà e le problematiche che incontra il tema di attribuzione della responsabilità alle varie organizzazioni internazionali, concentrandosi, in particolare, su un riparto di responsabilità possibile tra ONU e stati membri per le operazioni compiute dal *CPK team* sopra delineato. Le varie organizzazioni internazionali operano, a tutti gli effetti, all'interno del mondo reale, tramite operazioni che possono comportare una responsabilità internazionale, così come delineata nel paragrafo precedente[650]. Accanto al *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* (DARS), nel 2011 è stato adottato anche il *Draft Articles on the Responsibility of International Organizations* (DARIO)[651]. Il contenuto di questi due documenti risulta molto simile, al punto che, molto spesso, le regole contenute all'interno dell'ultimo riprendono, anche solo con parziali modificazioni, quelle contenute nel primo[652]. Ciò che è rilevante per il seguente elaborato fa leva sulle difficoltà di accertamento della responsabilità per le operazioni poste in essere dai *CPK operators*, tema che può essere rinvenuto

[649] Schmitt, M. (2017). Due diligence. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 30-50). Cambridge: Cambridge University Press. doi:10.1017/9781316822524.008

[650] Hirsch, M. (1995). *The responsibility of international organizations toward third parties: some basic principles* (Vol. 20). Martinus Nijhoff Publishers.

[651] United Nations General Assembly. (2012). *Responsibility of the International Organization*. A/RES/66/100. Consultato da https://undocs.org/en/A/RES/66/100.

[652] Pustorino, P. (2015). The Control Criterion between Responsibility of States and Responsibility of International Organizations. In *Evolutions in the Law of International Organizations* (pp. 406-422). Brill Nijhoff.

analogicamente tramite la spiegazione delle difficoltà di attribuzione della responsabilità per le condotte adottate dagli operatori "tradizionali" di mantenimento della pace. Allo scopo di illustrare come ciò potrebbe avvenire sulla base del rispetto dei requisiti stabiliti dal criterio del controllo effettivo[653], prima è necessario sottolineare nuovamente come le Nazioni Unite non abbiano a propria disposizione un vero e proprio esercito, essendo un'organizzazione internazionale. Le attività di mantenimento della pace vengono infatti svolte dai cosiddetti "caschi blu", ovvero militari messi a disposizione dell'ONU da parte dei vari stati membri, che dovranno operare sulla base delle indicazioni e di un controllo dell'ONU, anche se, nella realtà dei fatti, molto spesso si trovano ad operare seguendo indicazioni statali; ed è proprio qui che sorgono i maggiori problemi. Il criterio del controllo effettivo serve a stabilire se e quando le operazioni adottate dai vari *PK operators* rientrino sotto il controllo effettivo delle Nazioni Unite oppure nell'insieme delle operazioni effettuate sulla base di indicazioni dei vari stati. In merito a questo tema, particolar valore viene assunto dall'art. 7 dei *Draft Articles*, commentato tramite il report della "*International Law Commission*" del 2011[654]. Come spiegato nei commenti, questa previsione è quella più rilevante in termini di attribuibilità della responsabilità per le condotte adottate dagli *UN operators*[655]. Nello specifico, l'art. 7 stabilisce i principi che regolano e disciplinano l'attribuzione della condotta, che comprende atti ed omissioni, da parte di quegli organi messi a disposizione per l'Organizzazione da parte di uno stato[656]. In questo senso, i *Peacekeeper operators*, essendo formalmente forze militari dei vari stati, rientrano nella definizione di organi dello stato che però sono messi a disposizione delle Nazioni Unite. Viene infatti

[653] Okada, Y. (2019). Effective control test at the interface between the law of international responsibility and the law of international organizations: Managing concerns over the attribution of UN peacekeepers' conduct to troop-contributing nations. *Leiden Journal of International Law*, *32*(2), 275-291.

[654] International Law Commission (ILC). (2011). *Report of the International Law Commission Fifty-Sixth Session*. UN Doc A/66/10 (2011) 99. Consultato da https://legal.un.org/ilc/reports/2011/

[655] United Nations. (2011). *Draft articles on the responsibility of international organizations, with commentaries (2011).* Consultato da https://legal.un.org/ilc/texts/instruments/english/commentaries/9_11_2011.pdf

[656] *Ibid.*

stabilito, all'art. 7, che la condotta di un organo di uno stato o di un organo o agente di un OI messo a disposizione di un'altra OI sarà considerata, ai sensi del diritto internazionale applicabile, un atto di quest'ultima, nel caso in cui la stessa eserciti un controllo effettivo su tale condotta[657]. Come chiarito nel commentario dalla *International Law Commission*, il test per verificare il controllo effettivo non deve essere svolto su tutto l'operato generale dell'organo ma viene svolto su ogni specifico atto illecito, per verificare se l'atto è stato compiuto sotto il controllo dell'OI oppure sotto il controllo dello stato mandante. Nel caso in cui l'atto illecito sia stato compiuto a seguito di istruzioni di quest'ultimo, la condotta dovrebbe essere attribuita allo stato; viceversa, qualora lo stato non abbia fornito nessuna istruzione e l'attività di controllo è stato svolta dall'OI, si dovrebbe ritenere quest'ultima responsabile[658].

Il criterio del controllo effettivo, per l'attribuzione della condotta considerata, è stato più volte affermato da diversi tribunali internazionali, tra i quali la stessa ICJ, nel "*case concerning military and paramilitary activities in and against Nicaragua"*[659] e nel "*case concerning application of the convention on the prevention and punishment of the crime of genocide*"[660]. In linea di massima, le Nazioni Unite si sono, quasi sempre, assunte la responsabilità per le attività effettuate dalla *PK forces*[661]. L'ONU riconosce infatti la sua responsabilità internazionale sulla base della sua personalità giuridica internazionale e della sua capacità di essere titolare di diritti e obblighi; inoltre, è ampiamente accettato il principio stante il quale, a seguito di una violazione del diritto internazionale,

[657] *Ibid.*

[658] *Ibid.*

[659] Vedi nota 166.

[660] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina, Serbia and Montenegro), Judgment, I.C.J. Reports 2007. (Vedi p. 43).

[661] Leck, C. (2009). International responsibility in united nations peacekeeping operations: Command and control arrangements and the attribution of conduct. *Melbourne Journal of International Law*, 10(1), 346-364.

segue l'obbligo, anche per l'ONU, di una compensazione[662]. La posizione assunta dall'ILC all'art. 7 è interessante se presa in considerazione con la posizione espressa dal segretariato dell'ONU sullo status giuridico delle forze di pace. Il segretariato ha infatti dichiarato, nel 2004, che le forze di pace istituite dal SC saranno considerate organi sussidiari delle Nazioni Unite[663]. Inoltre, il segretariato si è espresso nel seguente modo*:*

> *«As a subsidiary organ of the United Nations, an act of a peacekeeping force is, in principle, imputable to the Organization, and if committed in violation of an international obligation entails the international responsibility of the Organization and its liability in compensation»*[664].

Tuttavia, la possibilità di attribuire la condotta del *PK team* allo stato che invia gli operatori è la conseguenza del mantenimento di alcuni poteri dello stato stesso sui suoi "contingenti nazionali" e su un controllo che quest'ultimo esercita sugli stessi[665]. Ciò rende possibile, almeno in principio, la doppia attribuzione delle condotte poste in essere dai *peacekeepers* sia all'Organizzazione sia allo Stato d'invio del contingente nazionale autore della condotta.[666] È stato evidenziato, inoltre, come in alcuni casi i comandanti dei contingenti nazionali abbiano cercato istruzioni dai rispettivi governi, prima di eseguire gli ordini impartiti dalle Nazioni Unite, il che dimostra come gli stati continuino a

---

662 United Nations General Assembly. (1996). *Financing of the United Nations Protection Force, the United Nations Confidence Restoration Operation in Croatia, the United Nations Preventive Deployment Force and the United Nations Peace Forces headquarters. Administrative and budgetary aspects of the financing of the United Nations peacekeeping operations: financing of the United Nations peacekeeping operations.* UN Doc. A/51/389. Consultato da https://documents-dds-ny.un.org/doc/UNDOC/GEN/N96/249/39/PDF/N9624939.pdf?OpenElement

663 United Nations Secretariat. (2004). *Responsibility of International Organizations. Comments and Observations Received from International Organizations*, 56 th sess, UN Doc A/CN.4/545. Consultato da https://legal.un.org/ilc/documentation/english/a_cn4_545.pdf

664 *Ibid.*

665 International Law Commission (ILC), *op. cit.*, p. 205.

666 Court of Appeal of The Hague, 5 July 2011 and 26 June 2012, ECLI:NL:GHSGR:2011:BR0132/ ECLI:NL:GHSGR:2012:BW9014 and ECLI:NL:GHSGR:2011:BR0133/ ECLI:NL:GHSGR:2012:BW9015 (the Appeal was dealt with in two stages); Supreme Court, 6 September 2013, ECLI:NL:HR:2013:BZ9228 and ECLI:NL:HR:2013:BZ9225.

mantenere un certo controllo sulle truppe "prestate". A tal proposito, il segretariato dell'ONU ha chiarito come l'attribuibilità della condotta dei *PKO*, con conseguente responsabilità per la OI, sia condizionata obbligatoriamente al presupposto che l'atto considerato sia eseguito sotto il suo comando e controllo esclusivo. Nella prassi, l'esercizio di tali poteri da parte dello Stato d'invio ha portato talvolta sino alla "rottura" della catena di comando internazionale, determinando l'attribuzione allo Stato del fatto illecito commesso dal proprio contingente.[667] In altri casi, l'accertamento da parte delle corti interne di circostanze straordinarie, tali per cui la missione di *peacekeeping* poteva ritenersi entrata in una "fase di transizione" finalizzata al ritiro dei contingenti in cui le decisioni erano assunte dallo Stato d'invio, ha costituito il presupposto fattuale e giuridico per l'attribuzione a quest'ultimo delle condotte del proprio contingente.[668] La prova dell'avvenuto "recupero" del controllo effettivo da parte dello Stato d'invio sulle condotte del proprio contingente è tuttavia particolarmente ardua da produrre,[669] il che si traduce, possibilmente, nell'attribuzione delle condotte dei *peacekeepers* alle Nazioni Unite ogni qual volta non si siano potute accertare circostanze straordinarie che abbiano prodotto un'interruzione della catena di comando internazionale. In tal senso, l'applicazione del criterio del controllo effettivo sembra risolversi in una presunzione di imputabilità all'ONU delle condotte poste in essere durante un'operazione di *peacekeeping.*

Partendo di conseguenza dalle difficoltà dell'attribuibilità della responsabilità nel mondo dinamico per gli operatori di pace, tramite la creazione di un *CPK team* come quello considerato le problematiche non farebbero altro che aumentare. Il

[667] Mukeshimana-Ngulinzira et al., v. Belgian State, Court of First Instance of Brussels, *Judgment of 8 December 2010*, Case nos 04/4807/A and 07/15547/A.

[668] V. i casi citati alla *nota 666*, e Stichting Mothers of Srebrenica et al v the State of the Netherlands and the United Nations, The Hague Court of Appeal, Judgment of 27 June 2017, Case nos 200.158.313/01 and 200.160.317/ 01.

[669] Mukeshimana-Ngulinzira et al., v. Belgian State, Court of Appeal of Brussels, *Judgment of 8 June 2018*, Case nos 2011/AR/292 and 2011/AR/294.

team considerato sarebbe, allo stesso modo di quanto avviene per i *Peacekeeper operators* tradizionali, composto da *cyber* esperti forniti da vari stati membri[670], la maggior parte dei quali sarebbe scelta tra i paesi più sviluppati, i quali hanno migliorato le loro capacità informatiche ed hanno esperti da "inviare". Gli operatori considerati, essendo di conseguenza esperti nazionali, potrebbero svolgere la propria attività seguendo direttive o istruzioni dei rispettivi stati, esattamente come può avvenire nelle operazioni dinamiche. Sulla base di ciò le difficoltà di attribuzione della responsabilità che si hanno per le forze delle Nazioni Unite impegnate nel mantenimento della pace non solo sarebbero presenti anche nel contesto di un *CPK team* ma risulterebbero forse amplificate[671]. Un esempio può essere riportato sulla base di quanto rilevato nel corso della trattazione: l'attribuibilità delle condotte effettuate nel *cyberspace* anche da un *CPK operator* sarebbe ancora più complicata da raggiungere, sulla base delle difficoltà attributive delle condotte cibernetiche. Tuttavia, il tema della responsabilità per le operazioni di un eventuale *CPK team* può essere solo accennato ed ipotizzato, dal momento che mancano studi specifici sullo stesso e che quei pochi presenti, al giorno d'oggi, preferiscono focalizzarsi solo sulla creazione dello stesso, senza, per il momento, esaminare i profili di un eventuale riparto della responsabilità.

4.4.3 Applicabilità del principio di due diligence nel cyberspace: le maggiori difficoltà.

Il principio di *due diligence* si riscontra la prima volta nel 1872[672], ma due sono i casi che, da un punto di vista internazionale, assumono particolare rilevanza su questo tema. Il primo tra questi si concretizza nell'arbitrato "*Trail Smelter*", il

[670] Nabeel, *op cit.*, p. 174.

[671] Robinson, *op. cit*., p. 121.

[672] United Nations. (2012). *Arbitral Tribunal, Alabama Claims of the United States of America against Great Britain. Reports of International Arbitral Awards (1871, 8 May).* Consultato da https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf

quale prevedeva l'impossibilità per gli stati, non soltanto di utilizzare le risorse del proprio territorio per causare lesioni a proprietà o persone di altri stati, ma anche l'obbligo di evitare che le proprie risorse venissero utilizzate per gli scopi sopra delineati[673]. Lo stesso principio veniva ripreso nel *Corfu Channel case*[674] e successivamente nel principio 21 della Dichiarazione di Stoccolma del 1972[675] e della Dichiarazione di Rio del 1992[676]. Il principio si basa su due elementi: l'obbligo di prevenire e l'obbligo di evitare che venga causato un danno[677]. Questi obblighi prevedono una serie di attività che gli stati dovranno attuare per prevenire che venga causato un danno ad un altro stato tramite le proprie risorse o che, in generale, provenga da operazioni sul proprio territorio; le maggiori problematiche derivano dalla mancata esaustività delle indicazioni relative alle attività che uno stato deve adottare, per evitare di incorrere in una responsabilità internazionale. In particolare, l'obbligo di non causare un danno agli altri stati prevede che lo stato attui una serie di accortezze e di attività di controllo per prevenire il danno considerato[678]. Qualora venga accertato che, a seguito del mancato rispetto dell'obbligo di *due diligence*, si sia verificata un'operazione in grado di causare un danno che poteva essere evitata dallo stato semplicemente

[673] United Nations. (2006). *Arbitral Tribunal, Trail Smelter Arbitration (United States v Canada). Reports of International Arbitral Awards (1938, 16 April and 1941, 11 March),* vedi p. 1905. Consultato da https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf

[674] International Court of Justice (ICJ). (1949, 9 aprile). *Corfu Channel (U.K. v. Alb.). Judgment of 9 April 1949*, 6, 35. Consultato da https://www.icj-cij.org/en/case/1

[675] United Nations. (1972, 16 giugno). *Declaration of the United Nations Conference on the Human Environment. UN Doc A/RES/2994 (Stockholm Declaration).* Consultato da https://legal.un.org/avl/ha/dunche/dunche.html

[676] United Nations. (1992, 14 giugno). *Declaration on Environment and Development. UN Doc A/CONF.151/26 (Rio Declaration).* Consultato da https://legal.un.org/avl/ha/dunche/dunche.html

[677] Okwori, E. O. (2019). The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States. In *Ethiopian Yearbook of International Law 2018* (pp. 205-242). Springer, Cham.

[678] International Court of Justice (ICJ). (2010). *Pulp Mills on the River Uruguay (Argentina v Uruguay).* Judgement (2010) ICJ Rep 79, para. 197 (Pulp Mills Case). Consultato da https://www.icj-cij.org/en/case/135/judgments

adottato tutte le misure necessarie, lo stato si macchierà di una violazione di un'obbligazione internazionale e per questo motivo sarà ritenuto responsabile[679].

Il principio di due diligence viene spesso considerato alla stregua di standard che devono essere rispettati[680]. Il problema di questi standard minimi è che la loro interpretazione e valenza risulta assolutamente variabile, dal momento che determinati standard che vengono considerati eccessivi da alcuni stati possono essere considerati come basilari da parte di altri[681]. Le tipologie di attività che possono comportare una violazione del principio di due diligence possono essere omissive o commissive. Nel primo caso si ha una violazione del principio considerato qualora uno stato non abbia effettuato una corretta e adeguata vigilanza ed abbia omesso lo svolgimento di qualsiasi attività; non utilizzando le risorse a sua disposizione, ha fallito nel prevenire la causazione di un danno proveniente dal proprio territorio[682]. Allo stesso modo, il compimento delle attività considerate può far insorgere, nei confronti dello stato, una violazione del principio di due diligence, qualora le misure attuate risultino inadeguate o inefficaci: infatti, tramite la predisposizione di misure differenti si sarebbe, senza eccessivi problemi, potuto evitare il significante danno causato[683].

Il principio di due diligence è ampiamente riconosciuto dagli stati come parte fondamentali dei relativi sistemi giuridici nazionali. La possibilità che un principio di diritto internazionale di questa rilevanza venga applicato deve essere subordinata alla presenza di determinati requisiti. In primis, deve essere specificatamente importante per la teoria e la pratica del diritto internazionale.

[679] United Nations (2012), *op. cit*., p. 208.

[680] Rao, P. S. (Cur.). (1999, 5 maggio). *International liability for injurious consequences arising out of acts not prohibited by international law (Prevention of Transboundary Damage from Hazardous Activities. Second Report of the Special Rapporteur for the ILC on the topic of International Liability*. UN Doc A/CN.4/501. Consultato da https://legal.un.org/ilc/documentation/english/a_cn4_501.pdf

[681] Barnidge, R. (2006). The due diligence principle under international law. *International Community Law Review*, *8*(1), 81-121.

[682] Bastin, L. (2017). *State responsibility for omissions: establishing a breach of the full protection and security obligation by omissions* (Doctoral dissertation, University of Oxford).

[683] Pisillo-Mazzeschi, R. (1992). The due diligence rule and the nature of the international responsibility of states. *German YB Int'l L.*, *35*, 9. (Vedi p. 20).

Deve inoltre garantire una coesistenza con le altre varie regole del diritto internazionale e deve essere accettato nella sua totalità[684]. Il principio di due diligence rispecchia una necessità fondamentale nei rapporti internazionali, dal momento che assicura la possibilità di avere una responsabilità statale subordinata ad eventuali mancanze da parte degli stati stessi nel controllo dell'attività che viene svolta all'interno del proprio territorio ed è stato indubbiamente accettato come un principio di diritto internazionale[685].

Per la parte che interessa il seguente elaborato, nel momento in cui si forma un principio generale di diritto internazionale, quale quello di *due diligence*, pur essendosi originato per specifici aspetti del ramo internazionale, dovrebbe essere possibile applicarlo anche a situazioni simili, indipendentemente dalla prassi degli stati nel ritenerlo possibile[686]. L'invasività di internet nello svolgimento di operazioni statali ha portato a considerare la possibilità di estendere il principio considerato anche al mondo cibernetico; importare il principio di due diligence per evitare che si materializzi un danno consistente tramite una serie di attività di prevenzione che devono essere adottate dai vari stati appare senza dubbio plausibile[687]. In particolare, viene imposto un obbligo di due diligence a tutti gli stati, obbligando gli stessi a garantire che non verranno compiute attività che siano in grado di causare un danno agli altri stati; accanto a questo, gli obblighi impongono la predisposizione di attività di prevenzione e controllo per evitare che dalle proprie infrastrutture e dagli hardware situati nel territorio vengano lanciate le stesse operazioni[688]. Ciascuno stato avrà il compito di adottare tutte le

[684] Kulesza, J. (2016). *Due diligence in international law*. Brill.

[685] United Nations General Assembly. (1992) ICJ, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania), Judgment (1949) ICJ Rep 1, p. 22; ICJ, Armed Activities on the Territory of the Congo (DRC V Uganda), Merits (2005) ICJ Rep 168, para. 162 (Armed Activities Case); UNGA (1970), principle 1.

[686] Khanna, P. (2018). State sovereignty and self-defence in cyberspace. *BRICS LJ*, 5, 139.

[687] Ziolkowski, K. (2013). *Peacetime regime for state activities in cyberspace*. Tallinn: NATO CCD COE Publications.

[688] Ney, M., & Zimmermann, A. (2015). Cyber-security beyond the military perspective: international law, 'cyberspace' and the concept of due diligence. *German Yearbook of International Law*, 51-66.

misure che ritenga necessarie ed efficaci per impedire che venga causato un danno e l'inottemperanza di detto obbligo, derivato dalla mancata adozione delle misure considerate o dalla loro inefficacia, sarà ritenuto responsabile da un punto di vista internazionale[689]. I due distinti reports del 2013[690] e del 2015[691], redatti dal UNGGE ed affermati tramite risoluzione dell'Assemblea Generale, hanno confermato detta visione, evidenziando come le obbligazioni derivanti dal principio di due diligence dovrebbero ritenersi applicabili anche nel *cyberspace*. L'applicabilità del principio di due diligence nel cyber spazio viene inoltre sottolineata tramite due *Rules* del Manuale di Tallinn. La *Rule 6* evidenzia come ciascuno stato abbia il compito di non permettere che il proprio territorio o le proprie infrastrutture che sottostanno ad un controllo governativo siano utilizzate per compiere operazioni cibernetiche che colpiscano i diritti o causino serie conseguenze per altri stati[692]. La *Rule 7* invece, richiede che tutti gli stati adottino le misure che sono necessarie per far terminare un attacco cibernetico che produca gli effetti anzidetti[693].

Le caratteristiche necessarie per valutare la violazione delle obbligazioni derivanti dal principio di due diligence sono particolarmente importanti. Le prime due da considerate, anche da un punto di vista cibernetico, sono la conoscenza e la prevedibilità. Il principio di due diligence impone allo stato che è a conoscenza di un danno imminente o di un attacco dannoso nei confronti di un altro stato di adottare tutte le misure per evitarlo[694]. Mentre per gli attacchi armati la conoscenza dello stato è "facilmente" dimostrabile, maggiori difficoltà sono rappresentate dalla conoscenza degli attacchi cibernetici, soprattutto nel caso di

[689] Schmitt, *op. cit.*, p. 19. (Vedi p. 213).

[690] United Nations General Assembly. (2013, 24 giugno). *Developments in the field of information and telecommunications in the context of international security*, UN *Doc A/68/98.*

[691] United Nations General Assembly. (2015, 22 luglio). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN Doc. A/70/174, para. 26. Consultato da http://undocs.org/A/70/174

[692] Schmitt, *op. cit.*, p. 19. (Vedi p.30).

[693] *Ibid*., (p. 43).

[694] Kulesza, *op. cit*., p. 210.

arretratezza dello stato che manca della capacità informatiche per determinare, in tempo, quando un'operazione sia in procinto di essere scagliata, il che comporta un ritardo nell'adozione delle misure necessarie. Allo stesso modo, la prevedibilità del danno è analoga alla conoscenza dell'operazione; come avviene nel diritto ambientale internazionale, per ottemperare alle varie obbligazioni viene richiesto agli stati di dotarsi di misure preventive in grado di individuare le varie attività alla stregua delle capacità degli stati[695].

Un ulteriore elemento necessario è la scoperta del luogo d'origine da cui l'attacco viene scagliato. Questo punto risulta chiaramente complicato poiché, dal momento che gli attacchi possono essere scagliati da vari e plurime ubicazioni distinte, prevedere un regime di controllo con conseguente applicazione della responsabilità nei confronti di determinati stati per violazione degli obblighi di due diligence diviene complicato. Tuttavia, la capacità statale di tracciare la localizzazione dei vari computer risulta necessaria per poter ottemperare agli obblighi derivanti dal principio di due diligence[696]. Proprio quest'ultimo punto deve essere considerato come un elemento su cui intervenire, anche tramite una maggiore cooperazione internazionale. Infatti, la capacità di controllare le varie operazioni cibernetiche all'interno del proprio territorio, con la possibilità di intervenire qualora venga ravvisata un'attività che potrebbe causare un danno ad un altro stato, è subordinata alle capacità tecnologiche tecniche, intellettuali, finanziarie di uno stato[697]. Una soluzione in grado di ottemperare a dette lacune ed in grado di concedere una maggiore stabilità nel panorama di difesa cibernetica internazionale, con la quale verrebbe garantita una prevenzione maggiore delle varie attività cibernetiche, potrebbe essere quella di prevedere la possibilità di ricevere assistenza tecnologica da altri stati

[695] Okwori, *op. cit*., p. 209. (Vedi p. 216).

[696] Couzigou, I. (2018). Securing cyber space: the obligation of States to prevent harmful international cyber operations. *International Review of Law, Computers & Technology*, *32*(1), 37-57.

[697] Buchan, R. (2016). Cyberspace, non-state actors and the obligation to prevent transboundary harm. *Journal of Conflict and Security Law*, *21*(3), 429-453.

digitalmente più avanzati e finanziariamente più stabili. In questo modo, tramite il raggiungimento di standard conoscitivi comuni a livello tecnologico, anche gli stati che non sono dotati di capacità eccellenti nell'ambito informatico possono evitare che operazione informatiche contro altri stati vengano eseguite dal proprio territorio. Tuttavia, in questo momento non è presente alcuna obbligazione in capo agli altri stati relativa alla fornitura di assistenza per prevenire, all'interno di altri stati, condotte dannose[698].

Un caso concreto che può aiutare a comprendere le difficoltà dell'applicabilità materiale del principio qui considerato è rappresentato da *Wannacry*, già analizzato nel corso dell'elaborato. In particolare, ci si potrebbe chiedere se la Corea del Nord abbia violato il principio considerato, presupponendo un'inottemperanza degli obblighi di prevenzione e repressione delle attività eseguite all'interno del proprio stato[699]. In questo caso, veniva valutata la responsabilità della Corea per non aver effettuato un controllo capillare della rete. Tuttavia, quello che si può rilevare è come, nel cyber spazio, una serie di elementi dovranno essere presi in considerazione: tra questi il diritto alla privacy. Richiedere una sorveglianza capillare del cyberspace ad uno stato può comportare concrete violazioni del diritto alla privacy degli individui[700]. Per questo motivo, non potendo richiedere una diligenza che vada oltre la valutazione e la conoscenza di situazioni anomale, non si può ritenere responsabile la Corea per l'attacco *Wannacry.*[701]

Per concludere, ammettendo l'applicabilità del principio di due diligence ne cyber spazio, le sfide che vengono prospettate necessitano, per ottenere una maggiore efficacia, della predisposizione di un approccio meglio definito[702]. Vi è infatti la necessità di forzare l'applicazione di misure legislative ed

[698] Couzigou., *op. cit.*, p. 213. (Vedi p. 13).

[699] Mandrioli, *op. cit.*, p. 32.

[700] *Ibid.*

[701] *Ibid.*

[702] Okwori, *op. cit.*, p. 209. (Vedi p. 235).

amministrative a livello statale che garantiscano una conforme visione del principio. In questo modo si potrebbe creare un'obbligazione di risultato e non di mezzi, assicurandosi di conseguenza che gli stati possano effettuare grandi passi avanti nella ricerca degli strumenti per prevenire gli attacchi cibernetici[703]. Sulla base dello sviluppo dei principi di mutua assistenza e di leale cooperazione tra gli stati, potrebbe essere garantita la copertura delle mancanze in tema di rispetto dell'obbligo di due diligence anche per quelli più arretrati. Se l'obbligo di controllare le infrastrutture e le reti informatiche per gli stati risulta più accentuato, migliori dovrebbero essere le misure preventive adottate dai vari stati; il riconoscimento sarebbe in grado di creare una disciplina minima ma efficace per la determinazione dello standard di accortezza richiesto agli stati[704].

[703] *Ibid.*

[704] *Ibid*., (p. 236).

Conclusioni

Le innovazioni tecnologiche hanno portato tutti gli stati del mondo a relazionarsi con cambiamenti sempre più rapidi e frequenti. Negli ultimi due decenni abbiamo assistito, con particolare irruenza, all'ingresso nella vita di tutti i giorni di strumenti informatici che neanche lontanamente potevano essere immaginati. Con la presente tesi, accanto agli innumerevoli vantaggi che il cambiamento tecnologico ha portato, si sono volute analizzare nel dettaglio una serie di problematiche, relative al mondo cibernetico, che sono sorte da un punto di vista strettamente giuridico.

I pericoli non sono solo aumentati ma si sono evoluti. La connessione rapida che viene garantita a ciascun cittadino tramite lo sfruttamento di una rete mondiale, quale internet, presenta, subito di fianco ai vantaggi, una serie indistinta di possibili minacce; tali minacce potrebbero travolgere non solo la vita di un singolo, come nel caso di spionaggio cibernetico con conseguente furto di dati, ma anche i meccanismi quotidiani della società. La forza e l'invasività di quelli che, nel corso dell'elaborato, sono stati definiti come attacchi cibernetici vengono riscontrate sulla base di una digitalizzazione che è arrivata, al giorno d'oggi, ad intaccare ogni ramo della realtà. È sufficiente pensare a come lo svolgimento delle attività delle infrastrutture statali, anche di quelle più "banali", si basi su un sistema quasi interamente digitalizzato. Accanto all'aumento della velocità e della sistematicità dello svolgimento dell'attività, deve essere considerato un ulteriore elemento: qualora venisse colpita un'infrastruttura critica tramite un attacco informatico, l'infrastruttura entrerebbe in balia della volontà di coloro che attaccano, con la possibilità di andare a causare danni inimmaginabili allo stato vittima.

Le difficoltà maggiori riscontrate su questa materia fanno prevalentemente riferimento sia ad una mancanza di una normativa unitaria, a livello internazionale, in grado di disciplinare i singoli aspetti delle operazioni statali in termini di *cyberspace*, sia all'impossibilità di ottenere, per il momento, anche

solo una visione definitoria comune sui macro-temi considerati. La riluttanza dei singoli stati a fornire le proprie esplicite opinioni, relativamente ad una serie di temi e operazioni che potrebbero essere considerate illecite, rappresenta solo uno dei punti maggiori di dette difficoltà. Come rilevato all'interno del capitolo IV, gli stati cercano molto spesso di nascondere le proprie attività, tramite l'utilizzo di gruppi di soggetti che non sono direttamente ricollegabili agli stessi. Dette difficoltà, inoltre, si esplicano alla stregua del fatto che le operazioni cibernetiche sono molto più facili da nascondere; in questo modo, i singoli stati hanno la possibilità, non esistendo una vera e propria normativa globalmente applicabile, di svolgere la propria attività senza dover renderne conto ad altri soggetti di diritto internazionale. Il tema della responsabilità internazionale degli stati per le operazioni cibernetiche ha rappresentato un elemento di particolare rilevanza per l'elaborato. Creare confini definiti per l'applicabilità del principio di responsabilità internazionale nel mondo cibernetico, risulta uno degli elementi chiave per poter permettere una maggiore stabilità. Anche qui, tuttavia, le problematiche non si sono fatte attendere: l'attribuibilità delle operazioni cibernetiche è quella più pressante. Uno strumento utile prospettato nel lavoro è rappresentato da un miglioramento della cooperazione tra stati nello scambio di informazioni sulle innovazioni tecnologiche, in grado di permettere a tutti di individuare anticipatamente le minacce cibernetiche. Strettamente correlato al concetto di responsabilità è il rispetto del principio di *due diligence*, che prevede l'obbligo per ciascuno stato di evitare che dal suo territorio o tramite le sue infrastrutture vengano lanciati attacchi cibernetici.

Grandi passi avanti sono stati fatti per implementare il regime di sicurezza cibernetica nel panorama globale. Nello specifico, accanto al dibattito relativo all'applicabilità del diritto internazionale al *cyberspace* – tema oggi per lo più superato tramite le singole dichiarazioni statali che hanno confermato detta visione – i problemi principali sono sorti relativamente alle singole modalità di applicazione della normativa internazionale considerata. I principi e le norme del

diritto internazionale sono stati espressamente pensati per avere una rilevanza da un punto di vista strettamente dinamico e le nuove sfide che si prospettano comprenderanno la necessità di effettuare un'interpretazione evolutiva delle norme e della prassi degli stati, al fine di includere anche le attività cibernetiche e le rispettive singole sfaccettature. Queste ultime, di fatto, possiedono contorni ancora oggi contraddistinti da un ampio grado di nebulosità e dubbia chiarezza.

Il primo passo, accanto alle dichiarazioni statali, che è stato attuato per far fronte a dette difficoltà, è rappresentato dalla redazione del Tallinn Manual (2013) e del Tallinn Manual 2.0 (2017). La rilevanza e l'importanza che avranno negli anni avvenire le organizzazioni internazionali si riscontra già all'interno dei due manuali, dal momento che la prima redazione risale al lontano 2013, ed è stata promossa dalla NATO. La promozione di questa prima redazione è stata effettuata dal *NATO Cooperative Cyber Defence Centre of Excellence*; tuttavia, è opportuno ricordare che il Manuale non costituisce un documento vincolante, ma si concretizza come un tentativo da parte del gruppo di esperti che l'ha redatto di individuare la normativa applicabile al contesto cibernetico. Questo centro costituisce uno dei primi tentativi di creare un organo in seno ad un'organizzazione internazionale con compiti specifici relativi allo studio dei fenomeni cibernetici.

I due manuali rappresentano un connubio di opinioni degli esperti, dal momento che il lavoro non prevede solo l'indicazione della *Rule* che la maggioranza ritiene applicabile ma prevede l'inserimento, come commenti al lavoro, di tutte le opinioni che hanno contraddistinto il dibattito. Lo scopo dei due manuali, infatti, non è quello di stabilire una normativa vincolante. Partendo dal presupposto che gli esperti non avrebbero in ogni caso una tale autorità, una delle funzioni primarie dei manuali è rendere consci sia i singoli cittadini che i vari stati dell'importanza che il mondo cibernetico avrà nei prossimi anni e fornire una base per lavori futuri. Inoltre, rappresenta un tentativo di ampliare e aumentare la possibilità di dialogo tra i vari stati.

Come è stato riscontrato, il mondo cibernetico è privo di delimitazioni geografiche, fisiche e territoriali ed è proprio per questo motivo che l'unico modo prospettabile per avere uno standard di sicurezza cibernetica unitario è fornito tramite una necessaria cooperazione tra gli stati. Lo sviluppo di nuove tecnologie ed armi cibernetiche, come avviene d'altronde nel mondo fisico, può aumentare la sicurezza ma può anche creare una situazione di paura, specialmente per gli stati non così avanzati. La creazione di uno standard di sicurezza collettivo, basato su definizioni unitarie e una normativa applicabile a tutti gli stati, pur rappresentando un'ipotesi lontana, si configura come uno dei migliori strumenti per poter far fronte comune ai pericoli e alle minacce che circondano il *cyberspace*.

Per raggiungere i risultati prefissati, un compito sicuramente fondamentale sarà devoluto alle varie organizzazioni internazionali presenti nel mondo. Il fondamento dell'elaborato mette in luce il fatto che questo compito non viene devoluto solo a macro-organizzazioni internazionali come l'ONU, ma può e deve essere perseguito anche dalle più piccole organizzazioni internazionali, che avranno un compito fondamentale a livello regionale. La discussione e la diffusione di notizie relative a questo mondo, infatti, non farà altro che implementare la consapevolezza dei vari stati e dei singoli individui dell'importanza di ottenere un sistema che renda più sicuro il mondo *online*.

Pertanto, accanto all'individuazione del panorama attuale, l' obiettivo della tesi è stato quello di cercare di evidenziare vantaggi e problematiche che potrebbero sorgere in seguito alla creazione di un organo in grado di svolgere attività di mantenimento della pace all'interno del mondo cibernetico. La legale base giuridica per l'implementazione di un organo, ad oggi solo prospettato, di questo tipo deriva direttamente dalla legittimità, fornita tramite la Carta, per il Consiglio di Sicurezza delle Nazioni Unite di adottare misure che comprendono attività di *peacekeeping* o *peace enforcement*, la cui distinzione è stata tracciata nel quarto capitolo. I vantaggi che potrebbe portare un organo come quello analizzato

sarebbero molteplici. Essendo il panorama cibernetico stato definito più e più volte come il quinto dominio ed il luogo principale di possibili guerre future, un tale organo porterebbe, senza dubbio, ad una maggiore sicurezza e stabilità nel panorama internazionale. Le attività che un *cyber peacekeeping* andrebbe a svolgere potrebbero contribuire alla prevenzione di un eventuale scoppio di un conflitto o alla stabilizzazione della situazione successiva allo stesso. Le operazioni risulterebbero fondamentali per la tutela dei cittadini e comporterebbero l'implementazione di una maggiore e più sicura cultura del mondo cibernetico. Quest'ultimo tema potrebbe essere particolarmente rilevante alla stregua di duplici aspetti. La creazione di una cultura del mondo cibernetico, con conseguente realizzazione dei corsi di formazione tanto prospettati, non solo porterebbe ad una maggiore consapevolezza, per chiunque, delle potenzialità e delle minacce che sono presenti ma avrebbe un riscontro positivo anche nell'economia dei vari paesi. Tramite questi corsi, difatti, verrebbe favorita la possibile creazione di innumerevoli posti di lavoro innovativi e più sicuri; da una parte verrebbe garantita la facoltà di avere nuovi "*cyber* combattenti" e dall'altra si avrebbe un ragionevole smantellamento di situazioni dinamiche, potenzialmente più pericolose. Infine, l'organo prospettato andrebbe ad assumere compiti fondamentali nel rispetto e nella promozione di tutti i diritti umani che vengono riconosciuti nel *cyberspace*. Tra questi, oltre alla protezione del diritto alla vita, i più importanti, che sono stati analizzati nell'elaborato, riguardano la tutela del diritto alla *privacy*, che, come visto, può essere oggetto di numerose violazioni soprattutto in tema di *cyber espionage*, e il diritto ad ottenere e fornire informazioni.

Nonostante l'impellente e pressante sviluppo dei vari attacchi cibernetici che possono causare morte e danni a persone e oggetti, la problematica principale attiene al fatto che, ad oggi, il Consiglio di Sicurezza delle Nazioni Unite non sia stato ancora riunito in incontro formale per discutere del tema. Quest'ultimo è stato oggetto ampio di dibattito all'interno dell'Assemblea Generale, la quale si è

tuttavia limitata a adottare risoluzioni, che non sono vincolanti, per lo più riguardanti il tema della *cyber security*. Il CdS ha invece discusso, solo in due occasioni informali, le problematiche considerate. Non essendosi, di conseguenza, mai riunito formalmente, ad oggi non solo non è possibile riscontrare una constatazione che comporti un'equiparazione di un attacco cibernetico ad un attacco in grado di minacciare e violare la pace internazionale, ma nemmeno un primordio di discussione può essere rinvenuto. L'unico caso in cui detta equiparazione è stata prospettata deriva da un discorso tenuto dal Segretario Generale Antònio Guterres.

In conclusione, la necessità di avere al più presto un quadro definitorio generale ed un sistema comune di difesa per far fronte agli attacchi cibernetici si sviluppa partendo dalla considerazione che gli stessi stanno aumentando progressivamente. Dal primo attacco cibernetico di una certa rilevanza, il *Denial of Service* scagliato contro l'Estonia nel 2007, se ne sono sviluppati una serie in continuo aumento. Il ruolo che verrà svolto dalle organizzazioni internazionali sarà, in questo senso, incentrato *in primis* sull'implementazione della cooperazione e sullo scambio di informazioni tra i vari stati ma si dovrà sviluppare andando oltre, cercando cioè di creare un panorama cibernetico contraddistinto da definizioni comuni ed un sistema di difesa globale collettivo.

Bibliografia

Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, I.C.J. Reports 2010.

Akatyev, N., & James, J. (2017, giugno). United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping. In *European Conference on Cyber Warfare and Security* (pp. 8-16). Academic Conferences International Limited.

Akatyev, N., & James, J. I. (2015). Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. *Revised Selected Papers, ch. Cyber Peacekeeping*, 126– 139. Springer International Publishing. http://dspace.conacyt.gov.py/xmlui/handle/123456789/15838

Akatyev, N., & James, J. I. (2015, ottobre). Cyber peacekeeping. In *International Conference on Digital Forensics and Cyber Crime* (pp. 126-139). Springer, Cham.

Akatyev, N., & James, J. I. (2017, giugno). United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping. In *European Conference on Cyber Warfare and Security* (pp. 8-16). Academic Conferences International Limited. Consultato da https://arxiv.org/abs/1711.04502

Aljazeera America. (2013). *Timeline of Edward Snowden's revelations. Guardian announces leak of classified NSA documents.* Consultato da http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

Almutawa, A. (2020). Designing the Organisational Structure of the UN Cyber Peacekeeping Team. *Journal of Conflict and Security Law*, *25*(1), 117-147. Consultato da https://academic.oup.com/jcsl/article-abstract/25/1/117/5603655

Alvarez, J. E. (1997). Rush to closure: lessons of the Tadic judgment. *Mich. L. Rev.*, 96(7), 2031-2112. doi:10.2307/1290059

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina, Serbia and Montenegro), Judgment, I.C.J. Reports 2007.

Arai-Takahashi, Y. (2002). Shifting Boundaries of the Right of Self-Defence-Appraising the Impact of the September 11 Attacks on Fus Ad Bellum. In *Int'l L.*, 36.

Arquilla, J., & Ronfeldt, D. (1993). *Cyberwar is coming!.* Santa Monica, CA: RAND Corporation. Consultato da http://www.rand.org/pubs/reprints/RP223.html

Association of Southeast Asian Nations (ASEAN). (n.d.). *About ASEAN*. Consultato da https://asean.org/asean/about-asean/

Association of Southeast Asian Nations. (2012). *2012 Asean Regional Forum Statement By The Ministers Of Foreign Affairs On Cooperation In Ensuring Cyber Security*. Consultato da https://aseanregionalforum.asean.org/wp-content/uploads/2019/01/ARF-Statement-on-Cooperation-in-Ensuring-Cyber-Security.pdf

Awan, I. (2017, 15 marzo). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, 54, 138–149. https://doi.org/10.1007/s12115-017-0114-0

Bakir, V., & McStay, A. (2018). Fake News and The Economy of Emotions. *Digital Journalism*, 6(2), 154-175. Consultato da https://doi.org/10.1080/21670811.2017.1345645

Barkham, J. (2001). Information warfare and international law on the use of force. *NYUJ Int'l L. & Pol.*, *34*, 57.

Barnidge, R. (2006). The Due Diligence Principle Under International Law. *International Community Law Review, 8*(1), 81-121. doi: https://doi.org/10.1163/187197306779173194

Bastin, L. (2017). *State responsibility for omissions: establishing a breach of the full protection and security obligation by omissions* (Doctoral dissertation, University of Oxford).

Bellamy, A. J., & Williams, P. D. (Cur.). (2013). *Providing peacekeepers: the politics, challenges, and future of United Nations peacekeeping contributions*. OUP Oxford.

Benedetto, C., & Carlo, F. (2000). *Le Nazioni Unite*. Padova: Cedam.

BOE. Jefatura del Estado. (2002, 7 maggio). *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.* https://www.boe.es/eli/es/l/2002/05/06/11/con

BOE. Legislación Consolidada. (2002, 7 maggio). *Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.* https://www.boe.es/buscar/pdf/2002/BOE-A-2002-8628-consolidado.pdf

Bohr, S. (1993). Sanctions by the united nations security council and the European community. *European Journal of International Law, 4(2),* 256-268.

Botero, J. C., Janse, R., Muller, S., & Pratt, C. (Cur.). (2012, 24 settembre). *Innovations in Rule of Law. A Compilation of Concise Essays*. HiiL and The World Justice Project. Consultato da https://worldjusticeproject.org/our-work/publications/edited-volumes/innovations-rule-law-compilation-concise-essays

Bovet, A., & Makse, H. A. (2019, 2 gennaio). Influence of fake news in Twitter during the 2016 US presidential election. Nature Communications, 10(7). Da https://doi.org/10.1038/s41467-018-07761-2

Bowett, D. (1972, gennaio). Reprisals involving recourse to armed force. *Am. J. Int'l L.*, 66(1), 1-36.

Brandom, R. (2017). UK hospitals hit with massive ransomware attack. *The Verge*, *12*.

Brenner, S. W. (2007). At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology, 97(2).* Consultato da https://scholarlycommons.law.northwestern.edu/jclc/vol97/iss2/2/

Bruce, G. (2013). Definition of terrorism social and political effects. *Journal of Military and Veterans Health, 21*(2), 26. https://jmvh.org/article/definitionof-terrorism-social-and-political-effects/

Brun, L., & Bellanova, R. (2020). *The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity*. Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain.

Buchan, R. (2016). Cyberspace, non-state actors and the obligation to prevent transboundary harm. *Journal of Conflict and Security Law*, *21*(3), 429-453.

Burk, D. L. (1995). Trademarks Along the Infobahn: A First Look at the Emerging Law of Cybermark. *Law School Journal,* 1(1). Consultato da https://scholarship.richmond.edu/jolt/vol1/iss1/4/

Cahill, T. P., Rozinov, K., & Mule, C. (2003). Cyber warfare peacekeeping. *IEEE Systems, Man and Cybernetics Society Information Assurance Workshop,* 100-106. West Point, NY, USA. doi: 10.1109/SMCSIA.2003.1232407.

Cannizzaro, E. (2012). *Diritto internazionale*. Giappichelli: Torino.

Carr, J. (2012). *Inside cyber warfare: Mapping the cyber underworld*. " O'Reilly Media, Inc.".

CECC (Congressional-Executive Commission on China). (2015, 18 settembre). *Urging China's President Xi Jinping to Stop State-Sponsored Human Rights Abuses.* Statement by Xiao Qiang. https://www.cecc.gov/sites/chinacommission.house.gov/files/CECC%20Hearing%20-%20Human%20Rights%20Abuses%20-%2018Sept15%20-%20Xiao%20Qiang.pdf

Cerf, V. G., & Kahn, R. E. (1974, maggio). A Protocol for Packet Network Interconnection. *IEEE Transactions on Communications*, 22(5), 637–48. https://www.cs.princeton.edu/courses/archive/fall06/cos561/papers/cerf74.pdf

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American Society for Information Science and Technology*, 59(8), 1347–1359. Doi: 10.1002/asi.20838

Chen, Q., & Bridges, R. A. (2017, December). Automated behavioral analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE.

Chivers, K. (2019, 28 agosto). *Zero-day vulnerability: What it is and how it works.* Consultato da Security Center https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Choucri, N., Madnick, S., & Koepke, P. (2016, agosto). *Institutions for Cyber Security: International Responses and Data Sharing Initiatives.* Cambridge, MA: Sloan School of Management, Cybersecurity Interdisciplinary Systems Laboratory (CISL). Consultato da http://web.mit.edu/smadnick/www/wp/2016-10.pdf

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Springer.

Christou, G. (2019). The collective securitization of cyberspace in the European Union. *West European Politics*, *42*(2), 278-301.

CIA (Central Intelligence Agency). (2020, 6 ottobre). *About CIA: History of the CIA.* Consultato da https://www.cia.gov/about-cia/history-of-the-cia

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.

Cohen-Amagor, R. (2015, giugno). *Confronting the internet's dark side moral and social responsibility on the free highway*. Cambridge: Cambridge University Press. doi: 10.1017/CBO9781316226391.

Colonna Vilasi, A. (2014). *Storia della CIA*. Sovera Edizioni.

Comandini, V. V. (2018, 25 giugno). Le *fake news* sui social network: un'analisi economica. *Saggi – Fake news, pluralismo informativo e responsabilità di rete*, 183-212. http://www.medialaws.eu/wp-content/uploads/2018/06/Visco-Comandini.pdf

Commissione Europea. (2017, 4 ottobre). *Comunicazione Della Commissione Al Parlamento Europeo E Al Consiglio Sfruttare al meglio le reti e i sistemi informativi – verso l'efficace attuazione della direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*. Consultato da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017DC0476&from=IT

Committee On Formation Of Customary (General) International Law. (2000). *Statement of Principles Applicable to the Formation of General Customary International Law*, in

International Law Association (ILA), Report of the Sixty-Ninth Conference, pp. 1-66. London Conference. Consultato da http://www.law.umich.edu/facultyhome/drwcasebook/Documents/Documents/ILA%20Report%20on%20Formation%20of%20Customary%20International%20Law.pdf

Condron, S. M. (2007). Getting it right: Protecting American critical infrastructure in cyberspace. *Harvard Journal of Law & Technology, 20(2)*, 403-422. Consultato da https://jolt.law.harvard.edu/assets/articlePDFs/v20/20HarvJLTech403.pdf

Conforti, B., & Focarelli, C. (2017). *Le Nazioni Unite* (11. ed.). Cedam.

Conforti, B., & Iovane, M. (1997). *Diritto internazionale*. Editoriale scientifica.

Council of Europe. (2001, 23 novembre). *Convention on Cybercrime*. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of Europe. (2020). *Lista completa dei trattati del Consiglio d'Europa.* Consultato da https://www.coe.int/it/web/conventions/full-list/-/conventions/rms/0900001680078b37 art.6

Council of Europe. (n.d.). *European Convention for the Protection of Human Rights and Fundamental Freedoms*, modificata dai Protocolli No. 11 and 14, 4 Novembre 1950, ETS 5, Consultato da https://www.refworld.org/docid/3ae6b3b04.html

Council of Europe. European Court of Human Rights. (2010). *Convenzione Europea dei diritti dell'uomo.* Consultato da https://www.echr.coe.int/documents/convention_ita.pdf

Couzigou, I. (2018). Securing cyber space: the obligation of States to prevent harmful international cyber operations. *International Review of Law, Computers & Technology*, *32*(1), 37-57.

Crawford, J. (2019). *Brownlie's principles of public international law*. Oxford University Press, USA.

Dannenbaum, T. (2010). Translating the standard of effective control into a system of effective accountability: how liability should be apportioned for violations of human rights by member state troop contingents serving as United Nations peacekeepers. *Harv. Int'l LJ*, *51*, 113.

Davis, B. R. (2006). *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance.* 15 CommLaw Conspectus 119. Consultato da https://scholarship.law.edu/commlaw/vol15/iss1/7

De Coning, C., Aoi, C., & Karlsrud, J. (Cur.). (2017, 3 febbraio). *UN Peacekeeping doctrine in a new era.* Routledge. Consultato da https://cedricdeconing.net/2017/02/03/un-peacekeeping-doctrine-in-a-new-era/

Del Vecchio, A. (2012). *Diritto delle organizzazioni internazionali*. (pp. 22-231). Edizioni Scientifiche Italiane.

Delegation to UN General Assembly (PRC). (2013, ottobre). *Statement by the Chinese Delegation on Information and Cyber Security at the Thematic Debate at the First Committee of the 68th Session UNGA.* (New York: United Nations).

Delupis, I. (1984). Foreign Warships and Immunity for Espionage. *American Journal of International Law*, *78*(1), 53-75. doi:10.2307/2202342

Demarest, G. B. (1996). Espionage in International Law. *24 Denv. J. Int'l L. & Pol'Y,* 24(2), 321-348. Consultato da https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1657&context=djilp

Democratic National Committee. (n.d.). *Official Website*. Consultato da https://democrats.org/who-we-are/

Denning, D. E. (2013). Framework and Principles for Active Cyber Defense. *Computers & security*, 40. DOI: 10.1016/j.cose.2013.11.004.

Dev, P. R. (2015). Use of force and armed attack thresholds in cyber conflict: The looming definitional gaps and the growing need for formal U.N. response. *Texas International Law Journal, 50(2-3)*, 381-402. Consultato da https://texashistory.unt.edu/ark:/67531/metapth838918/

Dobrzeniecki, K. (2005). How should we deal with human rights in cyberspace? Some remarks. *International Review of Law, Computers & Technology*, 19:3, 253-258 Consultato da https://doi.org/10.1080/13600860500348036

Dominioni, S. (2019, 2 dicembre). *Cybersecurity: l'architettura della difesa italiana*. Istituto per gli studi di politica internazionale. Consultato da https://www.ispionline.it/it/pubblicazione/cybersecurity-larchitettura-della-difesa-italiana-24546

Dorn, A. W., & Webb, S. (2019). Cyberpeacekeeping: New Ways to Prevent and Manage Cyberattacks. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 9(1), 19-30.

Dorn, W. (2017). Cyberpeacekeeping: A New Role for the United Nations? *Georgetown Journal of International Affairs*, 18(3), 138-146. Consultato da https://walterdorn.net/257

Duignan, P. (2000). *NATO: Its Past, Present, Future*. Hoover Press.

Egan, B. J. (2017). International Law and Stability in Cybershpace. *Berkeley J. Int'l L., 35*, 169.

Egan, M. (2019, 25 settembre). *What is the Dark Web, What's on it & How to Access it.* Tech Advisor. https://www.techadvisor.co.uk/how-to/internet/dark-web-3593569/ (visitato il 28 ottobre 2020).

ENISA. (2012, 8 maggio). *National Cyber Security Strategies: setting the course for national efforts to strengthen security in cyberspace.* Consultato da https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

ENISA. (2016). *German National Cyber Security Strategy*. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

ENISA. (2020). *About ENISA - The European Union Agency for Cybersecurity: Towards a Trusted and Cyber Secure Europe.* Consultato da https://www.enisa.europa.eu/about-enisa

ENISA. (2020, giugno). *A Trusted And Cyber Secure Europe. ENISA Strategy*. Consultato da https://www.enisa.europa.eu/publications/corporate-documents/a-trusted-and-cyber-secure-europe-enisa-strategy

EUR-lex. (2004, 13 marzo). *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance).* Consultato da https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004R0460

EUR-lex. (2019, 17 aprile). *Regulation (Eu) 2019/881 Of The European Parliament And Of The Council Of 17 April 2019.* Consultato da https://eur-lex.europa.eu/eli/reg/2019/881/oj/

European Commission. (2013, 7 febbraio). *EU Cyber security strategy: An Open, Safe and Secure Cyberspace.*

European Defence Agency. (2020). *Mission.* Consultato da https://www.eda.europa.eu/Aboutus/Missionandfunctions

European Defence Agency. (2020, 7 agosto). *Cyber Defence*. https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence

Factory at Chorzow (Germ. v. Pol.), 1927 P.C.I.J. (ser. A) No. 9 (Luglio 26).

FBI (Federal Bureau of Investigation). (n.d.). *Official Website*. Consultato da https://www.fbi.gov/

Federal Ministry of the Interior. (2005). *National Plan for Information Infrastructure Protection*. Consultato da https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/EN/BSI/Kritis/National_Plan_for_Information_Infrastructure_Protection.pdf?__blob=publicationFile

Finnish Government, Ministry of Foreign Affairs. (2020, 15 ottobre). *Finland published its positions on public international law in cyberspace*. Consultato da https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace

Flammini, F. (2012). *Critical infrastructure security: assessment, prevention, detection, response*. WIT Press.

Focarelli, C. (2015). *Diritto internazionale*. Vicenza: Wolters Kluwer.

Franzese, P. W. (2009). Sovereignty in cyberspace: Can it exist? *Air Force Law Review, 64(1),* 1-42.

Freedman, R. (2013). *The United Nations Human Rights Council: A Critique and Early Assessment*. Routledge.

Gallotti, C. (2019). *Information security: Risk assessment; information security management systems; the ISO/IEC 27001 standard*. Cesare Gallotti.

Ghosh, S., & Turrini, E. (Cur.). (2010). *Cybercrimes: a multidisciplinary analysis*. Springer Science & Business Media.

Gibbs, D. N. (2000). The United Nations, international peacekeeping and the question of 'impartiality': revisiting the Congo operation of 1960. *The Journal of Modern African Studies*, *38*(3), 359–382. Consultato da http://doi.org/10.1017/S0022278X0000338

Gioia, A. (2013). *Diritto internazionale: manuale breve*. Giuffrè Editore.

Goodrich, L. M., Simons, A. P., & Hambro, E. I. (1969). *Charter of the United Nations: Commentary and Documents. 3d and rev. ed*. Columbia University Press.

Government of Canada, Public Safety Canada. (2020). *National Cyber Security Action Plan (2019-2024).* Consultato da https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx#a02

Government of Netherlands. (2019, 5 luglio). *Letter to the parliament on the international legal order in cyberspac*e. Consultato da https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace

Governo italiano. (2012, 17 settembre). *La posizione italiana sui principi fondamentali di Internet*.

Green, J. A. (2006). Docking the Caroline: Understanding the relevance of the formula in contemporary customary international law concerning self-defense. *Cardozo Journal of International and Comparative Law, 14(2),* 429-480.

Grosswald, L. (2011). Cyberattack attribution matters under article 51 of the U.N. Charter. *Brooklyn Journal of International Law*, 36(3), 1151-1182. Consultato da https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1124&context=bji

Guymon, C. D. (ed). (2012). *Digest of United States Practice in International Law.*

Halawi, R. A. S. (2020). Cybercrime and cybersecurity: The need for International Cybersecurity Law. Consultato da Leiden Law Blog https://leidenlawblog.nl/articles/cybercrime-and-cybersecurity-the-need-for-international-cybersecurity-law

Harries, D. (2017). Narrative Mapping of Cyberspace. Context and Consequences. In J. Martín Ramírez Luis & A. García-Segura (Cur.), *Cyberspace Risks and Benefits for Society, Security and Development* (pp. 23-40). Berlino: Springer.

Hartami, A., & Handayani, P. W. (2012, giugno). The critical success factors of e-voting implementation in Indonesian local elections: The case of Jembrana regency election. In *ECEG2012-Proceedings of the 12th European Conference on e-Government: ECEG*. Academic Conferences Limited.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The Law of Cyber-Attack. *California Law Review, 100*(4), 817–885.

Heintschel von Heinegg, W. (2013). Territorial sovereignty and neutrality in cyberspace. *International Law Studies, 89*(1), 17.

Helmner, A. (2016). *Human Rights Violations of Peacekeeping Troops: Accountability of the UN and the Relationship to the ECHR.*

Herrera, G. L. (2006). Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In M. D. Cavelty, & V. Mauer (Cur.), *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace* (Cap. 4).

Hilderbrand, R. C. (2001). *Dumbarton Oaks: the origins of the United Nations and the search for postwar security*. UNC Press Books.

Hirsch, M. (1995). *The responsibility of international organizations toward third parties: some basic principles* (Vol. 20). Martinus Nijhoff Publishers.

Hoisington, M. (2009). Cyberwarfare and the use of force giving rise to the right of self-defense. *BC Int'l & Comp. L. Rev., 32*, 439. Consultato da https://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16/

Hongju Koh, H. (2012). International Law in Cyberspace. *Harvard International Law Journal*, 54, 1-12. Consul. da https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5858&context=fss_papers

Hsu, K., & Murray, C. (2014). *China and international law in cyberspace*. US-China Economic and Security Review Commission.

Hughes, A. Deputy Assistant Secretary of Defense. (2016). Statement on *Digital Acts of War: Evolving the Cybersecurity Conversation, Before the H. Comm. on Oversight and*

Government Reform Subcomms. on Information Security and National Security, 114th Cong. 1.

Hughes, R. (2009). NATO and Cyber Defence. *Atlantisch Perspectief*, 33. Consultato da https://scholar.google.com/citations?user=ORnkIVgAAAAJ&hl=en

Human Rights Council. (2015, 22 maggio). *U.N. Doc. A/HRC/29/3*: *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye.*

Il Consiglio federale. Il portale del Governo svizzero. (2020, 14 settembre). *Convenzione sulla cibercriminalità*. Consultato da https://www.admin.ch/opc/it/classified-compilation/20100537/index.html

INCIBE. (n.d.). *Cómo trabajamos.* Consultato da https://www.incibe.es/que-es-incibe/como-trabajamos

INCIBE. (n.d.). *Qué hacemos*. Consultato da https://www.incibe.es/que-es-incibe/que-hacemos#actividad

International Committee of the Red Cross (ICRC). (n.d.). Treaties, States Parties and Commentaries. *Project of an International Declaration concerning the Laws and Customs of War. Brussels, 27 August 1874*. Consultato da https://ihl-databases.icrc.org/ihl/INTRO/135

International Court of Justice (ICJ), Official Website. (2020). *Legality of the Threat of Nuclear Weapons, Advisory Opinion,* (1996, 8 luglio). 22, 39. Consultato da https://www.icj-cij.org/en/case/95

International Court of Justice (ICJ). (1949). *Reparation for injuries suffered in the service of the United Nations, Advisory Opinion: I.C.J.* Reports 1949.

International Court of Justice (ICJ). (1949, 9 aprile). *Corfu Channel (U.K. v. Alb.). Judgment of 9 April 1949*, 6, 35. Consultato da https://www.icj-cij.org/en/case/1

International Court of Justice (ICJ). (1984, 26 novembre). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984.* Consultato da https://www.icj-cij.org/en/case/70/judgments

International Court of Justice (ICJ). (2010). *Pulp Mills on the River Uruguay (Argentina v Uruguay).* Judgement (2010) ICJ Rep 79, para. 197 (Pulp Mills Case). Consultato da https://www.icj-cij.org/en/case/135/judgments

International Court of Justice (ICJ). (n.d.). *Legality of the Threat or Use of Nuclear Weapons*. Consultato da https://www.icj-cij.org/en/case/95

International Court of Justice. (n.d.). *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (1998)*. Consultato da https://www.icj-cij.org/en/case/100

International Law Commission (ILC). (2011). *Report of the International Law Commission Fifty-Sixth Session*. UN Doc A/66/10 (2011) 99. Consultato da https://legal.un.org/ilc/reports/2011/

International Law Commission (ILC). (2021). *Official Website*. Consultato da https://legal.un.org/ilc/

Iovane, G. (2008). *Cyberwarfare e Cyberspace: Aspetti Concettuali, Fasi ed Applicazione allo Scenario Nazionale ed all'ambito Militare* [Tesi di dottorato, DIMA Università degli Studi di Salerno]. Cons. da

http://www.difesa.it/SMD_/CASD/IM/CeMISS/Pubblicazioni/Documents/46644_ricerca_2pdf.pdf

Jackson, S. (1979). Prologue to the Marshall plan: the origins of the American commitment for a European recovery program. *The Journal of American History*, *65*(4), 1043-1068. Oxford University Press.

Jackson, S. (2016). NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Aggression Qualifies as an Armed Attack. *The CIP Report*. Consultato da https://cip.gmu.edu/2016/08/16/nato-article-5-cyber-warfare-natos-ambiguous-outdated-procedure-determining-cyber-aggression-qualifies-armed-attack/

Jensen, E. (2017). The Tallinn manual 2.0: Highlights and insights. *Georgetown Journal of International Law*, 48(3), 735-778.

Jensen, E. T. (2016). The Tallinn Manual 2.0: Highlights and Insights. *Geo. J. Int'l L.*, *48*, 735.

Jian, S. (2014). An International Code of Conduct for Information Security: China's perspective on building a peaceful, secure, open and cooperative cyberspace'. In *Cyber Stability Seminar*.

Jinks, D. (2003). State responsibility for the acts of private armed groups. *Chi. J. Int'l L.*, 4(1). Consultato da https://chicagounbound.uchicago.edu/cjil/vol4/iss1/8/

Johnson, D., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review, 48*(5), 1367-1402. doi:10.2307/1229390

Kamal, A. (2005). *The Law of Cyber-Space: An invitation to the table of negotiations*. United Nations Institute of Training and Research.

Kamal, M. M., Hackney, R., & Sarwar, K. (2013). Investigating factors inhibiting e-government adoption in developing countries: the context of Pakistan. *Journal of Global Information Management (JGIM)*, *21*(4), 77-102.

Karake, Z., Shalhoub, R. A., & Ayas, H. (2019). *Enforcing Cybersecurity in Developing and Emerging Economies.* Institutions, Laws and Policies. Edward Elgar Publishing. Consultato da https://www.e-elgar.com/shop/gbp/enforcing-cybersecurity-in-developing-and-emerging-economies-9781785361326.html

Kavanagh, C. (2017). *The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century.* United Nations Institute for Disarmament Research.

Kavanagh, C. (2018). IT and Cyber Capabilities as a Force Multiplier for Transnational Crime. In *Organized Crime and Illicit Trade* (pp. 37-77). Palgrave Macmillan, Cham.

Kavanagh, C., Maurer, T., & Tikk-Ringas, E. (2014). *Baseline Review: ICT-related Processes & Events: Implications for International and Regional Security (2011-2013)*. ICT4Peace Foundation. Consultato da https://ict4peace.org/wp-content/uploads/2017/11/Baseline-Review-2014-ICT-Processes-colprint.pdf

Kelsen, H. (2000). *The law of the United Nations: a critical analysis of its fundamental problems: with supplement* (Vol. 11). The Lawbook Exchange, Ltd.

Khanna, P. (2018). State sovereignty and self-defence in cyberspace. *BRICS LJ*, 5, 139.

Kittichaisaree, K. (2017). *Public international law of cyberspace (Vol. 32).* Cham: Springer.

Kleffner, J. K., & Harrison Dinniss, H. A. (2013). Keeping the cyber peace: international legal aspects of cyber activities in peace operations. *International Law Studies*, *89*(1), 4. Consultato da https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1039&context=ils

Koh, H. (2012). Remarks as Prepared for Delivery By Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, Sept 18, 2012. *Harvard International Law Journal (Online)*, *54*, 1-12.

Koh, H. (2018). *International law in cyberspace*. (Discorso tenuto presso *the USCYBERCOM Inter-Agency Legal Conference*, 18 settembre 2012) in Carrie Lyn D. Guymon (Cur.), Digest of United States Practice in International Law (United States Department of State 2012) 593, 594–595.

Kostrzewa-Zorbas, G. (2014). NATO in the new strategic environment: Cyberattacks now Covered by article 5 of the north atlantic Treaty. *Studia Bezpieczeństwa Narodowego*, *4(6), 397-418.* Consultato da http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-a3e2b0d5-a7ae-4a61-993e-5e05997253b4

Kulesza, J. (2016). *Due diligence in international law*. Brill.

Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. *Computer Law & Security Rev. 25*, 307, 308–309.

Kunz, J. L. (1947). Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations. *American Journal of International Law*, *41*(4), 872–879. http://doi.org/10.2307/2193095

Lam, C. (2018, giugno). A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election. *59 Boston College Law Review,* 2167-2201.

Lamberti, C. (2014). Gli strumenti di contrasto al terrorismo e al cyber-terrorismo nel contesto europeo. *Rivista di Criminologia, Vittimologia e Sicurezza*, 8(2), 138-161. Consultato da http://eprints.bice.rm.cnr.it/9847/1/articolo_lamberti_2014-02.pdf

Lange, C. (1972). *Nobel Lecture, Peace 1901-1925*. NobelPrize.org. Nobel Media AB 2020. https://www.nobelprize.org/prizes/peace/1921/lange/lecture/_Editore Frederick W. Haberman, Amsterdam: Elsevier Publishing Company. (Traduzione inglese dell'originale del 1921).

Lauterpacht, H. (2002). *Private law sources and analogies of international law: with special reference to international arbitration*. The Lawbook Exchange, Ltd..

Leck, C. (2009). International responsibility in united nations peacekeeping operations: Command and control arrangements and the attribution of conduct. *Melbourne Journal of International Law,* 10(1), 346-364.

Legal Information Institute. (n.d.). *U.S. Constitution, amend. IV*. Consultato da https://www.law.cornell.edu/constitution/fourth_amendment

Lewis, J., & Vignard, K. (2016). *Report of the International Security Cyber Issues Workshop Series.* United Nations Institute for Disarmament Research (UNIDIR), Center for Strategic & International Studies (CSIS). Consultato da https://www.google.com/search?client=firefox-b-d&q=Report+of+the+International+Security+Cyber+Issues+Workshop+Series%E2%80%9D%2C+pp.+4%E2%80%937%2C

Lewis, P. J. (2013). Who Pays for the United Nations' Torts: Immunity, Attribution, and Appropriate Modes of Settlement. *NCJ Int'l L. & Com. Reg.*, *39*, 259.

Lewis, T. G., Darken, R. P., Mackin, T., & Dudenhoeffer, D. (2012). Model-based risk analysis for critical infrastructures. *WIT Transactions on State-of-the-Art in Science and Engineering, 54*.

Liaropoulos, A., & Ryan, J. (2011). War and ethics in cyberspace: cyber-conflict and just war theory. *Leading Issues in Information Warfare & Security Research, 1*(2).

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND *Corporation*.

Liivoja, R., & McCormack, T. (2014). Law in the Virtual Battlespace: The Tallinn Manual and the *Jus in Bello*. In: Gill T., Geiß R., Heinsch R., McCormack T., Paulussen C., & Dorsey J. (Cur.), *Yearbook of International Humanitarian Law Volume 15* (2012). T.M.C. Asser Press, The Hague. Consultato da https://doi.org/10.1007/978-90-6704-924-5_3

Loffredo, F. (2010). *Le persone giuridiche e le organizzazioni senza personalità giuridica. Manuale e applicazioni pratiche dalle lezioni di Guido Capozzi*. Terza edizione. Giuffrè Editore.

Lovato, G. (2017). *Private Military and Security contractors Origini, problematiche e continuità con il passato*. [Tesi, Università Ca'Foscari Venezia].

Lucchi, N. (2014). Internet content governance and human rights. *Vanderbilt Journal of Entertainment and Technology Law*, 16(4), 809-856.

Machakanja, P. (2014). Reintegration of child soldiers: A case of Southern Sudan. *Building Peace from Within*, 88-90.

MacQueen, N. (1999). *The United Nations Since 1945: Peacekeeping and the Cold War*. Addison-Wesley Longman.

Mandrioli, D. (2018). *Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati*. La comunità internazionale, (3)2018, 473-492. Consultato da https://scholar.google.com/scholar?hl=it&as_sdt=0%2C5&q=++Mandrioli%2C+D.+%282018%29.+Il+caso+WannaCry%3A+il+fenomeno+dei+cyber+attacks+nel+contesto+della+responsabilit%C3%A0+internazionale+degli+Stati.+Il+caso+WannaCry%3A+il+fenomeno+dei+cyber+attacks+nel+contesto+della+responsabilit%C3%A0+internazionale+degli+Stati%2C+473-492&btnG=

Martino, L. (2013). La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace ei rischi di guerra cibernetica. *Centro Interdipartimentale di Studi Strategici Internazionali e Imprenditoriali (CSSII), Florence*.

Maurer, T. (2011, settembre). Cyber norm emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security. *Discussion Paper, 2011-11, Science, Technology, and Public Policy Program.* Cambridge, MA: Belfer Center for Science and International Affairs. Consultato da https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security

Miao, W. M., & Lei, W. (2016). Policy review: The Cyberspace Administration of China. *Global Media and Communication*, 12(3), 337-340. 10.1177/1742766516680879

Mik, C., & Człowieka, Z. P. (1992). *Collective Human Rights*. Wydawnictwo UMK, Torun.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984.

Miller, A. (1993). Universal Soldiers: U.N. Standing Armies and the Legal Alternatives, *81 GEO. L.J.*, 773, 779-83. Consultato da https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles

Ministère Des Armes. (2019, 9 settembre). *Droit International Appliqué Aux Opérations Dans Le Cyberespace*. Consultato da https://www.google.com/search?client=firefox-b-d&q=Droit+International+appliqu%C3%A9+aux+op%C3%A9rations+dans+lecyberspace

Ministry of Defence. (2008). *National Cyber Security Strategy: Cyber Security Strategy Committee of Estonia*. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

Ministry of Economic Affairs and Communications. (2019). Cybersecurity Strategy 2019-2022: Republic of Estonia. Consultato da https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

Mix, C. (2014). Internet Communication Blackout: Attack Under Non-International Armed Conflict?. *Journal of Law & Cyber Warfare*, *3*(1), 70-102.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5).

Mueller, R. S. (2019). *The Mueller report: Report on the investigation into Russian interference in the 2016 presidential election*. WSBLD.

Muggah, R. (2010). Innovations in disarmament, demobilization and reintegration policy and research. Reflections on the last decade. *NUPI Working Papers*. Oslo: The Norwegian Institute for International Affairs. Consultato da https://www.files.ethz.ch/isn/119784/WP-774-Muggah.pdf

Mukeshimana-Ngulinzira et al., v. Belgian State, Court of Appeal of Brussels, *Judgment of 8 June 2018*, Case nos 2011/AR/292 and 2011/AR/294.

Mukeshimana-Ngulinzira et al., v. Belgian State, Court of First Instance of Brussels, *Judgment of 8 December 2010*, Case nos 04/4807/A and 07/15547/A.

Nabeel, F. (2019). Establishment of UN Cyber Peacekeeping Force: Prospects and Challenges. *NUST Journal of International Peace and Stability*, *2*(2).

Nabeel, F. (2020). Cyber Peacekeeping: Critical Evaluation of Digital Blue Helmets Program. *NUST Journal of International Peace and Stability*, 3(2), 17-27. Consultato da https://www.researchgate.net/publication/343224548_Cyber_Peacekeeping_Critical_Evaluation_of_Digital_Blue_Helmets_Program

National Institute of Standards and Technology (NIST). U.S. Department of Commerce. (n.d.). *Official Website Homepage*. Consultato da https://www.nist.gov/

National Research Council. (2009). *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press. Consultato da https://www.nap.edu/read/12651/chapter/1

National Security Council (U.S.), & United States. Executive Office of the President. (2011). *International strategy for cyberspace: Prosperity, security, and openness in a networked world*. [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council.

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

National Security Council (U.S.), & United States. Executive Office of the President. (2018). *National Cyber Strategy of the United States of America.* [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council. Consultato da https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

NATO CCDCOE Group of Experts. (Schmitt, M. N., cur). *Tallinn Manual on the International Law Applicable to cyber Warfare*. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Association of Southeast Asian Nations.* Consultato da https://ccdcoe.org/organisations/asean/

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Shanghai Cooperation Organisation*. Consultato da https://ccdcoe.org/organisations/sco/

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *United Nations.* Consultato da https://ccdcoe.org/organisations/un/

NATO Heads of State and Government. (2010, 19-20 novembre). *Strategic Concept of the Defence and Security of the Members of the North Atlantic Treaty Organization.* Consultato da https://www.nato.int/nato_static/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO Official Website. (2020). *A short history of NATO*. Consultato da https://www.nato.int/cps/en/natohq/declassified_139339.htm

NATO Sito ufficiale. (2020). *Che cos'è la NATO?* Consultato da https://www.nato.int/nato-welcome/index_it.html

NATO. (2015, 19 maggio). *Keynote Speech by NATO Secretary General Jens Stoltenberg at the Opening of the NATO Transformation Seminar*. Consultato da http://www.nato.int/cps/en/natohq/opinions_118435.htm.

NATO. (2016, 8-9 luglio). *NATO Summit Guide.* Consultato da https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf

NATO. (2018, 30 agosto). *Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.* Consultato da https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2019, 25 novembre). *Collective defence – Article 5*. Consultato da https://www.nato.int/cps/en/natohq/topics_110496.htm

NATO. (2020, 23 ottobre). *Allied Command Operations (ACO).* Consultato da https://www.nato.int/cps/en/natolive/topics_52091.htm.

NATO. (2020, 3 novembre). *Centres of Excellence.* Consultato da https://www.nato.int/cps/en/natohq/topics_68372.htm.

NATO. Supreme Allied Commander Transformation (NATO's ACT). (n.d.). *Official site.* Consultato da https://www.act.nato.int/

Ney, M., & Zimmermann, A. (2015). Cyber-security beyond the military perspective: international law, 'cyberspace' and the concept of due diligence. *German Yearbook of International Law*, 51-66.

NSA (National Security Agency). (n.d.). *Understanding the threat.* Consultato da https://www.nsa.gov/what-we-do/understanding-the-threat/

Office of Information and Communication Technology. (n.d.). *Digital Blue Helmets*. Consultato da https://unite.un.org/digitalbluehelmets/sites/unite.un.org.digitalbluehelmets/files/docs/digitalbluehelmets_brochure_final.pdf

Official Journal of the European Community. (2002). *Consolidated Versions of the Treaty on European Union and of the Treaty Establishing the European Community*, Brussels. C 325/1, Articolo 95. Consultato da https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12002E/TXT&from=FR

Official Journal of the European Union. (2012). *Consolidated version of the Treaty on the Functioning of the European Union*, Brussels. C 115/47, Articolo 114. Consultato da https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF

OHCHR. (n.d.). *Mr. David Kay, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Consultato da https://www.ohchr.org/en/issues/freedomopinion/pages/davidkaye.aspx

Okada, Y. (2019). Effective control test at the interface between the law of international responsibility and the law of international organizations: Managing concerns over the attribution of UN peacekeepers' conduct to troop-contributing nations. *Leiden Journal of International Law*, *32*(2), 275-291.

Okwori, E. O. (2019). The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap Between Universal and Differential Approaches for States. In *Ethiopian Yearbook of International Law 2018* (pp. 205-242). Springer, Cham.

Opensource. (n.d.). *Official Website.* Consultato da https://opensource.com/

Organization of American States (OAS). (2021). *CICTE's Cybersecurity program.* Consultato da http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

Organization of American States (OAS). (2021). *Cyber Security.* Consultato da https://www.oas.org/en/topics/cyber_security.asp

Organization of American States (OAS). (2021). *Who we are.* Consultato da http://www.oas.org/en/about/who_we_are.asp

O'Sullivan, M., Goldsmith, J., & Wu, T. (2006). Who Controls the Internet? Illusions of a Borderless World. *NUCB journal of language culture and communication*, *8*(1), 143-144.

Ottis, R. (2008). Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective. In *Proceedings of the 7th European Conference on Information Warfare*.

Oyez. LII Supreme Court Resources. (n.d.). *Griswold v. Connecticut*. Consultato da https://www.oyez.org/cases/1964/496

Oyez. LII Supreme Court Resources. (n.d.). *Katz v. United States*. Consultato da https://www.oyez.org/cases/1967/35

Painter, C. (2014, 4 marzo). *Remarks at Georgetown University Institute for Law Science and Global Security's 2014 International Engagement on Cyber Conference.* (Washington, DC). Consultato da http://www.state.gov/s/cyberissues/releasesandremarks/223075.htm.

Phneah, E. (2012, 6 febbraio). *Idea of Cyber Peacekeepers Premature, "Redundant"*. ZDNet News. Consultato da http://www.zdnet.com/idea-of-cyber-peacekeepers-prematureredundant-2062303742/

Phosphates in Morocco (Italy v. Fr.), 1938 P.C.I.J. (ser. A/B) No. 74 (giugno 14).

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2014, July). A cyber-attack evaluation methodology. In *Proc. of the 13th European Conference on Cyber Warfare and Security*.

Pisillo-Mazzeschi, R. (1992). The due diligence rule and the nature of the international responsibility of states. *German YB Int'l L., 35*, 9.

Post, D. G. (1996). Governing cyberspace. *Wayne Law Review, 43(1)*, 155-172.

Powles, A., Partow, N., & Nelson, M. N. (Cur.). (2015). *United Nations Peacekeeping Challenge: The Importance of the Integrated Approach*. Ashgate Publishing, Ltd..

Presidency of the Council of Ministers. (2013). *National Strategic Framework for Cyberspace Security*. Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

Presidency of The Council of Ministers. (2017). *The Italian Cybersecurity Action Plan*. Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

Prochko, V. (2018, 30 marzo). *The International Legal View of Espionage*. E-International Relations. [The University of St, Andrews], 1-10. Consultato da https://www.e-ir.info/pdf/73350

Project of an International Declaration Concerning the Laws and Customs of War, Adopted by the Conference of Brussels, August 27, 1874. (2017, 4 maggio). *The American Journal of International Law*, 1(2), 96–103. doi:10.2307/2212371 (pubblicato da Cambridge University Press, originale datato aprile 1907).

Proulx, V. J. (2006). Babysitting terrorists: Should states be strictly liable for failing to prevent transborder attacks. *Berkeley J. Int'l L., 23*.

Pubblicazioni Centro Studi per la Pace. (1999, 20 giugno). *Trattato del Nord Atlantico 1949.* Consultato da http://www.studiperlapace.it/documentazione/natotreaty.html#FN1

Pustorino, P. (2012). *Lo status di membro delle organizzazioni internazionali*. In Diritto delle organizzazioni internazionali (pp. 141-204). Napoli: Edizioni scientifiche italiane.

Pustorino, P. (2015). The Control Criterion between Responsibility of States and Responsibility of International Organizations. In *Evolutions in the Law of International Organizations* (pp. 406-422). Brill Nijhoff.

Pustorino, P. (2019). *Lezioni di tutela internazionale dei diritti umani* (pp. 1-232). Cacucci Editore.

Radsan, A. J. (2007). The Unresolved Equation of Espionage and International Law. *Michigan Journal of International Law*, 28(3), 596-623. Consultato da https://repository.law.umich.edu/mjil/vol28/iss3/5

Rao, P. S. (Cur.). (1999, 5 maggio). *International liability for injurious consequences arising out of acts not prohibited by international law (Prevention of Transboundary Damage from Hazardous Activities. Second Report of the Special Rapporteur for the ILC on the topic of International Liability*. UN Doc A/CN.4/501. Consultato da https://legal.un.org/ilc/documentation/english/a_cn4_501.pdf

Read, D. (2013). Heather Harrison Dinniss, cyber warfare and the laws of war. *Nordic Journal of Human Rights, 31(2),* 284-[ii].

Regno Unito. Parlamento e Consiglio. (2006, 2 maggio). *SENTENZA DELLA CORTE (Grande Sezione).* Consult. da https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62004CJ0217&from=EN

Roberts, A. (2008, 3 marzo). The crisis in UN peacekeeping. *Survival*, 36(3), 93–120. Consulta. da https://www.tandfonline.com/doi/abs/10.1080/00396339408442752

Robinson, M., Jones, K., & Janicke, H. (2015, marzo). Cyber warfare: Issues and challenges. *Comput. & Secur*. 49(2015), 70–94. DOI: 10.1016/j.cose.2014.11.007

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018, aprile). An introduction to cyber peacekeeping. *Journal of Network and Computer Applications 114,* 70-87. https://www.researchgate.net/publication/324704165_An_Introduction_to_Cyber_Peacekeeping

Rolston, B. (2007). Demobilization and reintegration of ex-combatants: The Irish case in international perspective. *Social & Legal Studies*, *16*(2), 259-280.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Ruotolo, G. M. (2014). Internet (Diritto Internazionale)(Internet (International Law)). *RUOTOLO GM*, in *Enciclopedia del diritto–Annali, Milano, 2104*, 545.

Sarti, E. (2019, 1 ottobre). *La visione francese sul diritto internazionale nel cyberspace. Center for Cyber Security and International Relations Studies.* Consultato da https://www.cssii.unifi.it/upload/sub/Francia_DirInt_Cyberspace.pdf

Saul, B. (2008). *Defining Terrorism in International Law*. Oxford: Oxford University Press.

Schindler, D., & Toman, J. (1988). *The Laws of Armed Conflicts.* Martinus Nijhoff Publishers, 22-34.

Schmidt, A. (2013). The Estonian cyberattacks. In Jason Healey (Cur.), *The Fierce Domain – Conflicts in Cyberspace 1986-2012* (pp. 174-193). Washington, D.C.: Atlantic Council.

Schmitt, M. (2017). Due diligence. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 30-50). Cambridge: Cambridge University Press. doi:10.1017/9781316822524.008

Schmitt, M. (Cur.). (2016, 15 novembre). *US Transparency regarding International Law in Cyberspace.* Consultato da Just Security https://www.justsecurity.org/34465/transparency-international-law-cyberspace/

Schmitt, M. N. & Vihul, Liis. (2014, 1 dicembre). The Nature of International Law Cyber Norms. *Tallinn Papers No. 5 (NATO Cooperative Cyber Defence Centre of Excellence, Dec. 2014)*. Consultato da SSRN: https://ssrn.com/abstract=2543520

Schmitt, M. N. (2011). Cyber Operations and the Jud Ad Bellum Revisited. *Vill. L. Rev.*, *56(3),* 569-606. Consultato da https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?article=1019&context=vlr

Schmitt, M. N. (2015-2016). In Defense of Due Diligence in Cyberspace. *Yale Law Journal Forum, 125*, 68-81.

Schmitt, M. N. (Cur.). (2013). *The Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. Consultato da https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf.

Schmitt, M. N. (Cur.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schmitt, N. M. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*, 37, 1-41, pag 921. Consultato da https://apps.dtic.mil/dtic/tr/fulltext/u2/a471993.pdf

Security Council Report. (2019, 23 dicembre). *In Hindsight: The Security Council and Cyber Threats.* Consultato da https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php

Security Council Report. (2020, 16 dicembre). *Arria-Formula Meetings*. Consultato da https://www.securitycouncilreport.org/un-security-council-working-methods/arria-formula-meetings.php

Security Council Report. (2020, gennaio). *Monthly Forecast.* Consultato da https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/2020_01_forecast.pdf

Servizio Europeo per l'Azione Esterna (SEAE). (n.d.). Consultato da Unione Europea sito ufficiale https://europa.eu/european-union/about-eu/institutions-bodies/eeas_it

Sharp, W. G. (1999). *Cyberspace and the Use of Force*. Aegis Research Corporation

Shea, J. (2017). How is NATO meeting the challenge of cyberspace?. *Prism*, *7*(2), 18-29. Consultato da https://cco.ndu.edu/News/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/

Sistema di informazione per la sicurezza della Repubblica. (n.d.). *DIS: Chi siamo.* Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html

Sistema di informazione per la sicurezza della Repubblica. (n.d.). *AISI: Chi siamo*. Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aisi.html

Sistema di informazione per la sicurezza della Repubblica. (n.d.). *AISE: Chi siamo.* Consultato da https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html

Sjursen, H. (2004). On the identity of NATO. *International Affairs*, 80(4), 687–703, Consultato da https://doi.org/10.1111/j.1468-2346.2004.00411.

Sklerov, M. J. (2009). Solving the dilemma of sate responses to cyberattacks: A justification for the use of active defenses against states who neglect their duty to prevent. *Mil. L. Rev.*, *201*, 1.

Smith, A., & Stewart, D. (1963). *An Inquiry into the Nature and Causes of the Wealth of Nations* (Vol. 1). Homewood, Ill: Irwin.

Staff Writers. (2008, 14 maggio). *NATO launches cyber defence centre in Estonia.* Consultato da Space War, https://www.spacewar.com/reports/NATO_launches_cyber_defence_centre_in_Estonia_999.html

Stato. (2015, 24 febbraio). Traduzione de *Convenzione di Vienna sul diritto dei trattati (1969).* Consultato da https://www.admin.ch/opc/it/classifiedcompilation/19450070/201201250000/0.193.501.pdf

Stilz, A. (2019). *Territorial sovereignty: A philosophical exploration*. Oxford University Press.

Subedi, D. B., & Jenkins, B. (2018). The Nexus between reintegration of ex-combatants and reconciliation in Nepal: A social capital approach. In *Reconciliation in Conflict-Affected Communities* (pp. 41-56). Springer, Singapore.

Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 russian-georgian cyber conflict. *Loyola of Los Angeles International and Comparative Law Review, 32(2),* 303-334. Consultato da https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1010&context=il

Taddeo, M. (2012). An analysis for a just cyber warfare. *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1-10.

Tavani, T. H., & Grodzinsky, F. S. (2014, settembre). Trust, betrayal, and whistleblowing: reflections on the Edward Snowden case. *SIGCAS Comput. Soc.*, 44(3), 8–13. Consultato da https://doi.org/10.1145/2684097.268410

Teti, A. (2018). *Cyber Espionage e Cyber Counterintelligence: spionaggio e controspionaggio cibernetico.* Rubettino Editore.

Tharoor, S. (1995). The changing face of peacekeeping and peace-enforcement. *Fordham Int'l LJ*, *19*, 408.

The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *About us*. Consultato da https://ccdcoe.org/about-us/

The NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Official Website*. Consultato da https://ccdcoe.org/

The North Atlantic Treaty. (1949, 4 aprile). *Art. V*. Consultato da https://www.nato.int/cps/en/natolive/official_texts_17120.htm

The Russian Ministry of Defense. (2011, settembre). *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*.

Tikk-Ringas, E. (Cur.). (2012). *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*. ICT4Peace Foundation. Consultato da https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

Todd, G. H. (2009). Armed attack in cyberspace: Deterring asymmetric warfare with an asymmetric definition. *Air Force Law Review, 64(1),* 65-102. Consultato da https://www.afjag.af.mil/Portals/77/documents/AFD-091026-024.pdf

Treccani. (2020). *Backup.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/backup/

Treccani. (2020). *Cloud computing.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/cloud-computing

Treccani. (2020). *Commutazione di pacchetto*. Enciclopedie on line, Istituto della Enciclopedia Italiana. Consul. da https://www.treccani.it/enciclopedia/commutazione-di-pacchetto_%28Lessico-del-XXI-Secolo%29/#:~:text=commutazi%C3%B3ne%20di%20pacch%C3%A9tto%20s.%20f.%20%E2%80%93%20Tecnica,o%20le%20applicazioni%20da%20interconnettere.

Treccani. (2020). *Denial of service.* Enciclopedie on line, Istituto della Enciclopedia Italiana: “attacco informatico consistente nell’occupare tutte le risorse di un sistema, impedendogli il corretto funzionamento.

Treccani. (2020). *E-commerce*. Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/e-commerce

Treccani. (2020). *E-health.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/e-health_%28Lessico-del-XXI-Secolo%29/

Treccani. (2020). *Formattazione.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/formattazione/

Treccani. (2020). *Instradamento*. Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/instradamento/

Treccani. (2020). *Malware*. Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/vocabolario/malware_%28Neologismi%29/

Treccani. (2020). *Scrambling.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/vocabolario/scrambling_%28Neologismi%29/

Treccani. (2020). *Screening.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/vocabolario/screening/

Treccani. (2020). *Scrolling.* Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/scrolling/

Treccani. (2020). *Steganografia.* Enciclopedie on line, Istituto della Enciclopedia Italiana. https://www.treccani.it/enciclopedia/steganografia_%28Enciclopedia-della-Matematica%29/

Treccani. (2020). *Trojan horse*. Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/enciclopedia/trojan-horse/

Treccani. (2020). *Worm*. Enciclopedie on line, Istituto della Enciclopedia Italiana. Consultato da https://www.treccani.it/vocabolario/worm/

Tsagourias, N., & Buchan, R. (Cur.). (2015). *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.

Turrini, P. (2012). *L'interpretazione evolutiva nella giurisprudenza internazionale*. [Tesi di dottorato, Università degli Studi di Firenze]. Consultato da https://flore.unifi.it/retrieve/handle/2158/826147/27268/Tesi%20completa%20%28Paolo%20Turrini%29%20-%2014-01-2013.pd

Twitter. *Twitter Usage Statistic.* Visitato il 9 dicembre 2020. Consultato da https://www.internetlivestats.com/twitter-statistics/

U.S. CYBER COMMAND. (n.d.). *Official site.* Consultato da https://www.cybercom.mil/

U.S. Department of State. (Archivio 2001-2009). *Chairman's Statement: The First ASEAN Regional Forum Ministerial Meeting, Bangkok, Thailand, 25 July 1994.* Consultato da https://www.google.com/search?client=firefox-b-d&q=first+arf+statement+1994

Unione Europea. (2020). *Agenzia europea per la difesa (AED).* Consultato da https://europa.eu/european-union/about-eu/agencies/eda_it

United Nations CISA. (2003). *National Strategy to Secure Cyberspace*. Consultato da https://www.cisa.gov/national-strategy-secure-cyberspace

United Nations Digital Blue Helmets. (2020). *Activities.* Consultato da https://unite.un.org/digitalbluehelmets/activities

United Nations General Assembly and Security Council. (2000, 21 agosto). *Comprehensive Review of the Whole Question of Peacekeeping Operations in All Their Aspects A/55/305.* Consultato da *https://www.un.org/ruleoflaw/files/brahimi%20report%20peacekeeping.pdf*

United Nations General Assembly. (1974). *Res. 3314, U.N. GAOR, 29th Sess., art. 1 (Dec. 14, 1974)*. Consultato da https://research.un.org/en/docs/ga/quick/regular/29

United Nations General Assembly. (1974). *Resolution 3314 (XXIX). Definition of aggression*. United Nations, New York. Consultato da athttp://www.un.org/documents/ga/res/29/ares29.htm.

United Nations General Assembly. (1996). *Financing of the United Nations Protection Force, the United Nations Confidence Restoration Operation in Croatia, the United Nations Preventive Deployment Force and the United Nations Peace Forces headquarters. Administrative and budgetary aspects of the financing of the United Nations peacekeeping operations: financing of the United Nations peacekeeping operations.* UN Doc. A/51/389. Consultato da https://documents-dds-ny.un.org/doc/UNDOC/GEN/N96/249/39/PDF/N9624939.pdf?OpenElement

United Nations General Assembly. (1999, 4 gennaio). *Developments in the field of information and telecommunications in the context of international security, UN Doc.* A/RES/53/70. Consultato da https://digitallibrary.un.org/record/265311#record-files-collapse-header

United Nations General Assembly. (2001, 22 gennaio). *Combating the criminal misuse of information technologies, UN Doc.* A/RES/55/63. Consultato da https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

United Nations General Assembly. (2002, 23 gennaio). *Combating the criminal misuse of information technologies*", UN Doc. A/RES/56/121. Consultato da https://digitallibrary.un.org/record/454952

United Nations General Assembly. (2002, 31 gennaio). *A/RES/56/183. Resolution 56/183 World Summit on the Information Society*. Consultato da https://undocs.org/pdf?symbol=en/A/RES/56/183

United Nations General Assembly. (2003, 31 gennaio). *Creation of a global culture of cybersecurity,* UN Doc. A/RES/57/239.Da http://www.itu.int./ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

United Nations General Assembly. (2004, 20 Novembre) *Creation of a global culture of cybersecurity and the protection of critical information infrastructures,* UN Doc. A/RES/58/199. Consultato da https://undocs.org/pdf?symbol=en/A/RES/64/211

United Nations General Assembly. (2010, 17 marzo). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures,* UN Doc. A/RES/64/211.1. Consultato da https://digitallibrary.un.org/record/672141

United Nations General Assembly. (2010, 30 luglio). *Report on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN Doc. A/65/201. Consultato da https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

United Nations General Assembly. (2012). *Responsibility of the International Organization*. A/RES/66/100. Consultato da https://undocs.org/en/A/RES/66/100.

United Nations General Assembly. (2012, 29 giugno). *Doc. A/HRC/20/L.13: The promotion, protection and enjoyment of human rights on the Internet.* Consultato da

https://documents-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf?OpenElement

United Nations General Assembly. (2013, 24 giugno). *Developments in the field of information*

United Nations General Assembly. (2015, 22 luglio). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174. Consultato da https://undocs.org/pdf?symbol=en/a/70/174

United Nations General Assembly. (2017, 28 febbraio). *Special measures for protection from sexual exploitation and sexual abuse.* UN Doc A/70/729, 7. 2016 Report of the Secretary-General. Consultato da https://peacekeeping.un.org/sites/default/files/sg_report_a_71_818_special_measures_for_protection_from_sexual_exploitation_and_abuse.pdf

United Nations General Assembly. (2018, 11 dicembre). *Developments in the field of information and telecommunications in the context of international security,* UN Doc. A/RES/73/27. Consultato da https://undocs.org/pdf?symbol=en/A/RES/73/27

United Nations General Assembly. (2019, 2 gennaio). *A/RES/73/266 Resolution adopted by the General Assembly on 22 December 2018: Advancing responsible State behaviour in cyberspace in the context of international security*. Consultato da https://undocs.org/A/RES/73/266

United Nations General Assembly. (n.d.). *Disarmament and International Security (First Committee).* Consultato da https://www.un.org/en/ga/first/index.shtml

United Nations General Assembly. (n.d.). *Economic and Financial Committee (Second Committee).* Consultato da https://www.un.org/en/ga/second/index.shtml

United Nations General Assembly. (n.d.). *Social, Humanitarian & Cultural Issues (Third Committee).* Consultato da https://www.un.org/en/ga/third/index.shtml

United Nations General Assembly. GGE. (2013). *Report A/68/98: para. 20*.

United Nations Human Rights Committee (HRC). (1988, 8 aprile). *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*. Consultato da https://www.refworld.org/docid/453883f922.html

United Nations Human Rights Committee (HRC). (2004, 26 maggio). *General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, CCPR/C/21/Rev.1/Add.13.* Consultato da https://www.refworld.org/docid/478b26ae2.html

United Nations Human Rights Committee (HRC). *General comment, supra note 9, 7*: *Art. 2 requires that States Parties adopt legislative, judicial, administrative, educative and other appropriate measures in order to fulfill their legal obligations.").*

United Nations Institute for Disarmament Research (UNIDIR). (2017). *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century.* Consultato da https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

United Nations Institute for Training and Research (UNITAR). (2021). *Official Website.* Consultato da https://unitar.org/

United Nations Mine Action Service (UNMAS). (n.d.). *Who we are.* Consultato da https://unmas.org/en/who-we-are

United Nations Office for Disarmament Affairs. (n.d.). *Group of Governmental Experts*. Consultato da https://www.un.org/disarmament/group-of-governmental-experts/

United Nations Office on Drugs and Crime. (2021). *Official Website*. Consultato da https://www.unodc.org/unodc/en/commissions/CCPCJ/index.html

United Nations Official site. (n.d.). *Group of Governmental Experts*. Consultato da https://www.un.org/disarmament/group-of-governmental-experts/

United Nations SCOR. (200, 28 settembre). *Resolution 1373 Doc. S/RES/1373 (2001).* Consultato da https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf

United Nations Secretariat. (2004). *Responsibility of International Organizations. Comments and Observations Received from International Organizations*, 56 th sess, UN Doc A/CN.4/545. Consultato da https://legal.un.org/ilc/documentation/english/a_cn4_545.pdf

United Nations Security Council. (2018, 3 maggio). *Letter dated 30 April 2018 from the Permanent Representative of Finland to the United Nations addressed to the President of the Security Council*, UN doc. S/2018/404. Consultato da https://undocs.org/S/2018/404.

United Nations Treaty Collection. (2021). *Status of Treaties.* Consultato da https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-1&chapter=3&clang=_en

United Nations. (1972, 16 giugno). *Declaration of the United Nations Conference on the Human Environment. UN Doc A/RES/2994 (Stockholm Declaration).* Consultato da https://legal.un.org/avl/ha/dunche/dunche.html

United Nations. (1992, 14 giugno). *Declaration on Environment and Development. UN Doc A/CONF.151/26 (Rio Declaration).* Consultato da https://legal.un.org/avl/ha/dunche/dunche.html

United Nations. (2005). *Responsibility of States for Internationally Wrongful Acts*. Consultato da https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdff

United Nations. (2006). *Arbitral Tribunal, Trail Smelter Arbitration (United States v Canada). Reports of International Arbitral Awards (1938, 16 April and 1941, 11 March)* Consultato da https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf

United Nations. (2006, 24 ottobre). *Charter of the United Nations and Statute of the International Court of Justice*. (Traduz. Italiana). (Originariamente pubblicato nel 1945). Consultato da https://www.admin.ch/opc/it/classified-compilation/20012770/200609120000/0.120.pdf

United Nations. (2008). *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Da https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

United Nations. (2008). *United Nations Peacekeeping Operations: Principles and Guidelines ("The Capstone Doctrine")*. (United Nations Department of Peacekeeping Operations and the United Nations Department of Field Support 2008) 97. Consultato da https://www.un.org/ruleoflaw/blog/document/united-nations-peacekeeping-operations-principles-and-guidelines-the-capstone-doctrine/.

United Nations. (2008, gennaio). *United Nations Peacekeeping Operations: Capstone Doctrine*. Consulta. da http://pbpu.unlb.org/pbps/library/capstonedoctrineeNg.pdf

United Nations. (2011). *Draft articles on the responsibility of international organizations*. Consultato da https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf

United Nations. (2011). *Draft articles on the responsibility of international organizations, with commentaries (2011).* Consultato da https://legal.un.org/ilc/texts/instruments/english/commentaries/9_11_2011.pdf

United Nations. (2012). *Arbitral Tribunal, Alabama Claims of the United States of America against Great Britain. Reports of International Arbitral Awards (1871, 8 May).* Consultato da https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf

United Nations. (2012, 8 giugno). *UN condemns deadly attack on peacekeepers in Côte d'Ivoire*. Consultato da https://news.un.org/en/story/2012/06/412772-un-condemns-deadly-attack-peacekeepers-cote-divoire

United Nations. (2014). *Operational Guide to the Integrated Disarmament, Demobilization and Reintegration Standards.* Consultato da https://www.google.com/search?client=firefox-b-d&q=United+Nations%2C+%E2%80%98Operational+Guide+to+the+Integrated+Disarmament%2C+Demobilizationand+Reintegration+Standards%E2%80%99+%28United+Nations%2C+2014%29

United Nations. (2020). *1944-1945: Dumbarton Oaks and Yalta.* Consultato da https://www.un.org/en/sections/history-united-nations-charter/1944-1945-dumbarton-oaks-and-yalta/index.html

United Nations. (2020). *Charter of the United Nations. Chapter I: Purposes and Principles.* Consultato da https://www.un.org/en/sections/un-charter/chapter-i/index.html

United Nations. (2020). *Office of legal affairs. OLA.* Consultato da https://legal.un.org/repertory/art41.shtml

United Nations. (n. d.). *Group of Governmental Experts*. Consultato da https://www.un.org/disarmament/group-of-governmental-experts/

United Nations. (n.d.). *Cyber Risk.* Consultato da https://unite.un.org/digitalbluehelmets/cyberrisk

United Nations. (n.d.). *Official Website.* Consultato da https://www.un.org/en/

United Nations. (n.d.). *Open-ended Working Group*. Consultato da https://www.un.org/disarmament/open-ended-working-group/

United Nations. (n.d.). *The Universal Declaration of Human Rights*. Consultato da https://www.un.org/en/universal-declaration-human-rights/

United Nations. *Charter Art. II, para. 3 & para 4.* Consultato da https://www.un.org/en/sections/un-charter/chapter-i/index.html

UNSCR. (n.d.). *Resolution 660 Iraq-Kuwait (2 August).* Consultato da http://unscr.com/en/resolutions/doc/660

US Presidential Policy Directive/PPD–20. (2012, ottobre). *US Cyber Operations Policy*. Consultato il 14 gennaio 2021 da https://fas.org/irp/offdocs/ppd/ppd-20.pdf

Verble, J. (2014, settembre). The NSA and Edward Snowden: surveillance in the 21st century. *SIGCAS Comput. Soc.*, 44(3), 14-20. Consultato da https://doi.org/10.1145/2684097.2684101

Virzo, R. (2012). *Gli atti delle organizzazioni internazionali. Diritto delle organizzazioni internazionali*. Edizioni Scientifiche Italiane.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004.

Wallander, C. A. (2000). Institutional assets and adaptability: NATO after the Cold War. *International organization*, 705-735. The IO Foundation and the Massachusetts Institute of Technology.

Waterman, H., Zagorcheva, D., & Reiter, D. (2002). NATO and Democracy. *International Security*, *26*(3), 221-235. Consultato da https://www.researchgate.net/publication/249564772_NATO_and_democracy

Weissbrodt, D. (2013). *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage.* University of Minnesota Law School, 347-387. Consultato da https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1227&context=faculty_articles

Whitman, M. E., Mattord, H. J., & Green, A. (2013). *Principles of incident response and disaster recovery*. Nelson Education.

Wikileaks. (2015, 3 novembre). *What is WikiLeaks.* Definizione tradotta: «WikiLeaks è un organizzazione internazionale la quale, senza scopo di lucro, riceve, analizza e pubblica documenti ufficiali ristretti, riguardanti guerre, spionaggio e corruzione». Consultato da: https://wikileaks.org/What-is-WikiLeaks.html

Wikipedia. (2020). *Federal Security Service.* Consultato da https://en.wikipedia.org/wiki/Federal_Security_Service

Wood, M. (2013). International Law and the Use of Force: What Happens in Practice?. *Indian journal of international law*, *53*, 345-367. Consultato da https://legal.un.org/avl/pdf/ls/Wood_article.pdf

Wortham, A. (2012). Should cyber exploitation ever constitute demonstration of hostile intent that may violate un charter provisions prohibiting the threat or use of force. *Federal Communications Law Journal*, *64(3)*, 643-660. https://www.repository.law.indiana.edu/fclj/vol64/iss3/8

Yangyue, L. (2014). *Competitive political regime and Internet control: Case studies of Malaysia, Thailand and Indonesia*. Cambridge Scholars Publishing.

YouTube. *YouTube About: Statistics 2020.* Visitato il 9 dicembre 2020. Consultato da https://www.youtube.com/intl/en-GB/about/press/

ZeroUno. (2020, 28 settembre). *Che cosa sono i file log e perché non c'è sicurezza senza log management*. Consultato da https://www.zerounoweb.it/techtarget/searchsecurity/che-cosa-sono-i-file-log-e-perche-non-c-e-sicurezza-senza-log-management/.

Ziolkowski, K. (2013). *Peacetime regime for state activities in cyberspace*. Tallinn: NATO CCDCOE Publications.

Ringraziamenti

Al Professor Pustorino, per avermi permesso di esplorare un tema così delicato e per avermi trasmesso la sua passione per questa materia. Un ringraziamento particolare va, inoltre, al Dott. Insolia, per la pazienza e la disponibilità dimostrata durante la stesura.

Ai miei genitori, fonti inesauribili e risacche d'amore. A mamma Ester, per avermi spinto ad intraprendere questa meravigliosa avventura lontano da casa, per essermi stata vicina ogni secondo, per avermi dimostrato che, insieme, tutti i limiti e gli ostacoli possono essere abbattuti e per essere la donna più forte che abbia mai conosciuto. A papà Andrea, migliore amico e confidente dei giorni più difficili, per avermi dimostrato che, con pazienza e gentilezza, si possono raggiungere i traguardi più lontani e per essere il modello di uomo che voglio diventare. Sono al mondo per rendervi orgogliosi di me.

A Giulia, àncora e ancora, compagna di vita nelle sfide di tutti i giorni in questi dieci anni meravigliosi. Il grazie più grande è per aver trasformato il limite della distanza in un'incredibile possibilità, dimostrandomi come sia facile restare uniti anche se lontani. Mi hai spronato tutti i giorni a far emergere la parte migliore di me, confidando nelle mie capacità e non buttandomi mai giù, porgendomi la mano tutte le volte in cui ho vacillato. Non so davvero che cosa abbia fatto in una vita precedente per meritare una persona speciale come te al mio fianco.

Agli amici di casa e a quelli del mare, per non essersi fatti spaventare dai 400 chilometri di distanza e per avermi dimostrato come la vera amicizia vada oltre il vedersi tutti i giorni. In particolare, un grazie di cuore a Tommaso, amico di sempre che mai mi ha fatto sentire solo quando tornavo.

Infine, il grazie più grande va agli amici di Roma. Quando sono partito, cinque anni fa, mai avrei immaginato di trovarmi qui a scrivere qualcosa del genere. Siete stati la mia forza e il mio scudo quando tutto sembrava crollare, quando mi venivano chieste le prefazioni dei libri in numeri romani e non sapevo dove sbattere la testa (resto ancora dell'idea che manco l'autore sappia che ci sta scritto) . Quando non riuscivo a capire neanche una parola di napoletano, quando mi mancava casa e non sapevo come fare, quando facevamo i tornei e venivamo

sempre eliminati dall'Everton, c'era sempre una sola costante: voi. Quello che mi porterò a casa da questi cinque anni è molto più di un "semplice" foglio di carta, perché, usando un'espressione (mia) del lontano 2015, siete stati e sarete per me, semplicemente, più di una famiglia.

Un grazie particolare va a Yaselli, fratelli da madri e regioni diverse. Non so neanche descrivere quello che avete rappresentato per me, avete riempito casa con colori che neanche pensavo esistessero. Ogni volta facciamo i conti di tutto quello che avete "scroccato" in questi cinque anni, ma la verità è che, per quello che mi avete dato, sarò per sempre in debito con voi. Che sia solo l'inizio.

Infine, l'ultimo ringraziamento va a quella psicopatica di Rosita; almeno una soddisfazione nella vita bisognerà concedergliela. Insieme dal giorno uno, quando sei venuta in avanscoperta per far fare amicizia a quel palo di Lorenzo, fino all'ultimo giorno, dalle nottate a Pola ai pranzi fuori: auguro davvero a chiunque di poter avere una migliore amica come te.