LUISS Guido Carli
LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

DIPARTIMENTO DI SCIENZE POLITICHE

Cattedra di Diritto Internazionale

"CYBER DIPLOMACY, UNA NUOVA FRONTIERA PER LE RELAZIONI INTERNAZIONALI"

RELATORE

Chiar.mo Prof.

Pietro Pustorino

CANDIDATO

Matteo Politano

098972

INDICE

INTRODUZIONE

Prima di entrare nel merito dell'analisi approfondita contenuta nel presente elaborato, è doveroso sottolineare come questo lavoro rappresenti il risultato di un interesse maturato nel corso del mio percorso triennale di studi, in particolare il corso di diritto internazionale, e durante la partecipazione al Corso di Alta Formazione in Cyber Diplomacy presso Sole24OreFormazione.

L'impostazione e lo sviluppo di questo studio si ispirano in modo significativo agli insegnamenti ricevuti dai dottori Pierluigi Paganini, Davide Lo Prete e Gianluigi Plini, docenti della prima edizione di detto corso. Nonostante la sua breve durata, tale percorso formativo ha costituito un'esperienza intellettuale e professionale di grande stimolo, fornendo una solida base teorica e pratica essenziale per affrontare le complesse e dinamiche sfide del settore della cybersicurezza e della diplomazia digitale.

Il presente elaborato si propone di esplorare un ambito strategico di cruciale importanza nell'attuale scenario internazionale: la *cyberwarfare* e la *cyber diplomacy*. Si tratta di un campo caratterizzato da dinamiche estremamente articolate, che coinvolgono attori statali e non statali, interessi geopolitici, normative ancora incomplete e una continua evoluzione tecnologica.

La complessità di tali tematiche è accentuata dalla natura intrinsecamente sfuggente e asimmetrica del cyberspazio, dove i confini tradizionali di guerra e pace si fanno progressivamente più sfumati, e dove la definizione stessa di vittoria e sconfitta assume nuove connotazioni.

L'analisi si concentrerà sulle difficoltà tecniche, politiche e giuridiche che caratterizzano la gestione delle minacce informatiche, in particolare quelle riconducibili a conflitti di natura ibrida e asimmetrica. Particolare attenzione sarà riservata al ruolo crescente della cooperazione internazionale, della governance multilivello e dell'interazione tra attori pubblici e privati, nonché alla necessità di sviluppare strategie efficaci di deterrenza e resilienza.

Si discuterà inoltre dell'importanza di definire con chiarezza responsabilità e attribuzioni, imprescindibili per la costruzione di un quadro normativo credibile e operativo.

In un contesto globale segnato da tensioni geopolitiche sempre più accentuate e da un continuo aumento delle minacce cibernetiche, la comprensione approfondita di questi temi risulta imprescindibile per delineare politiche di sicurezza adeguate e promuovere un dialogo costruttivo a livello internazionale.

L'elaborato intende pertanto fornire un contributo didascalico e analitico, con l'obiettivo di evidenziare le sfide attuali e le possibili traiettorie di sviluppo della *cyber diplomacy* e della *cyberwarfare* nel XXI secolo.

CAPITOLO I

La Cyber Diplomacy nel contesto odierno: scorci sulla multivettorialità della tematica

1.1 Definizione e contesto storico

Il cyberspazio rappresenta oggi una dimensione imprescindibile della società contemporanea, tanto da essere considerato un vero e proprio dominio strategico, al pari dei quattro domini tradizionali: terra, mare, aria e spazio.

Tuttavia, la sua definizione risulta tutt'altro che semplice. La natura complessa e in continua evoluzione del cyberspazio, caratterizzata da un'estrema interconnessione tra fattori tecnologici, politici ed economici, genera spesso ambiguità, sia nella narrativa comune, sia nelle analisi specialistiche. Gli sviluppi tecnologici, le dinamiche geopolitiche e le trasformazioni economiche si influenzano reciprocamente, creando scenari difficili da interpretare senza un'analisi approfondita e interdisciplinare. Questa complessità si manifesta non solo nella diffusione delle tecnologie digitali, ma anche nella crescente dipendenza dai sistemi informatici, che oggi permeano ogni aspetto della vita sociale, economica e politica. Tali sistemi diventano strumenti, al tempo stesso, di progresso e innovazione, ma anche di vulnerabilità e rischio.

La narrazione legata al concetto di cyberspazio è quindi spesso imprecisa e condizionata da semplificazioni, che tendono a ridurre la complessità di un ambiente nato come realtà tecnica e scientifica, ma rapidamente divenuto centrale nei rapporti internazionali e nella quotidianità globale.

La genesi del cyberspazio risale agli anni Settanta, in particolare al 1969, quando la *DARPA* (*Defense Advanced Research Projects Agency*) degli Stati Uniti sviluppò *ARPANET*, la prima rete informatica in grado di connettere centri universitari e di ricerca[1]. Il progetto, concepito nel contesto della Guerra Fredda, mirava a garantire la continuità delle comunicazioni in caso di attacco nucleare. Ciò che nacque come infrastruttura tecnico-militare, pensata per la resilienza e la sicurezza dello scambio informativo, si trasformò ben presto in un ecosistema globale. La vera svolta arrivò nel 1989 con la creazione del *World Wide Web* da parte di Tim Berners-Lee, che aprì la rete alla dimensione civile e commerciale, favorendo l'accesso su scala mondiale a informazioni, beni e servizi[2].

Negli anni Novanta, la diffusione dei *personal computer* e dei primi *browser* rese Internet accessibile a milioni di persone. Nei primi anni Duemila, la comparsa degli *smartphone* e la nascita dei *social media* segnarono un ulteriore punto di svolta, ridefinendo profondamente la natura e l'utilizzo del cyberspazio.

[1] https://www.darpa.mil ; Sulle prospettive future dell'Agenzia cfr: D. Theresa, "*Liberty Lifter: How Cold War tech inspired DARPA's next-gen transport*" in https://interestingengineering.com/military/liberty-lifter-darpa-transport
[2] Cfr: "*The birth of the Web*", in *Cern Resources*, https://home.cern/science/computing/birth-we

Oggi, oltre cinque miliardi di utenti sono connessi, e l'*Internet of Things* ha ulteriormente ampliato i confini del cyberspazio, integrando nelle reti digitali dispositivi della vita quotidiana, dalle automobili agli elettrodomestici[3].

La conseguenza inevitabile di questa evoluzione è stata la moltiplicazione delle vulnerabilità: ogni oggetto connesso rappresenta una possibile porta d'accesso per attacchi esterni, aumentando esponenzialmente la superficie d'attacco.

L'interconnessione, se da un lato ha migliorato la qualità della vita e reso più efficienti i processi economici e sociali, dall'altro ha introdotto nuove forme di fragilità, spesso difficili da eliminare. I primi segnali di rischio emersero già in epoca pionieristica: negli anni Settanta, alcune agenzie governative statunitensi avevano previsto che l'espansione delle reti digitali avrebbe comportato notevoli rischi di compromissione.

Nel 1988, il *worm* della Cornell University — uno dei primi esempi di *malware* — si diffuse involontariamente attraverso *ARPANET*, paralizzando circa il 10% delle macchine collegate. Questo episodio dimostrò per la prima volta come un codice malevolo potesse propagarsi rapidamente e avere effetti sistemici. Negli anni Novanta, eventi come *Solar Sunrise* evidenziarono la vulnerabilità delle reti militari, mentre nel 2007 il test *Aurora Generator* mostrò come un attacco informatico potesse danneggiare fisicamente infrastrutture critiche, rendendo inutilizzabile un generatore elettrico.

Due anni dopo, il caso *Stuxnet* rappresentò un vero spartiacque. Questo *malware*, introdotto tramite una semplice chiavetta USB in un sistema isolato dalla rete, riuscì a compromettere l'impianto nucleare iraniano di Natanz, rallentando le centrifughe e danneggiandole fisicamente. Per la prima volta si constatò che un'operazione informatica poteva produrre effetti tangibili e devastanti nel mondo reale, influenzando gli equilibri geopolitici senza ricorrere a un attacco convenzionale.

Per comprendere con maggiore precisione cosa si intenda con il termine *cyberspazio*, è necessario analizzarne la struttura, articolata in diversi livelli. Il cyberspazio, infatti, non è un'entità uniforme, ma si compone di più strati.

Solo una piccola parte dei contenuti digitali è visibile attraverso i comuni motori di ricerca: la grande maggioranza, circa il 90%, è custodita nel *deep web*, che comprende archivi istituzionali, dati bancari, sanitari o giudiziari non accessibili al pubblico. Ancora più nascosto è il *dark web*, nato per garantire anonimato e libertà di espressione — soprattutto in contesti autoritari — ma oggi prevalentemente utilizzato per attività illecite, come lo scambio di armi, droga, dati rubati e strumenti per attacchi informatici[4].

[3] https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption
[4] https://www.varutra.com/the-hidden-internet-exploring-the-secrets-of-the-dark-web/

Proprio in questo spazio agiscono molte organizzazioni criminali, che pubblicano campioni di dati trafugati per costringere le vittime a pagare un riscatto, sotto la minaccia di diffondere l'intero archivio. Tali dinamiche sono alla base delle moderne campagne *ransomware*, che dimostrano come il cyberspazio abbia favorito la nascita di nuove economie illegali globalizzate.

Oltre alla distinzione tra *web* visibile, *deep web* e *dark web*, il cyberspazio è composto da tre livelli principali: lo strato fisico, lo strato logico e lo strato umano, quest'ultimo definito anche come *cyber-persona*.

Il livello fisico del cyberspazio è rappresentato dalle infrastrutture materiali: *server*, *computer*, *data center* e, soprattutto, cavi sottomarini, attraverso i quali transita oltre il 95% del traffico mondiale di dati[5]. La loro rilevanza strategica è tale che alcuni Stati hanno sviluppato navi militari in grado di intercettarli o danneggiarli. Episodi come il danneggiamento accidentale di un cavo in Armenia nel 2011, che causò un *blackout* digitale a livello nazionale, o le recenti minacce di sabotaggi nei pressi del Mar Rosso, dimostrano come la dimensione fisica del cyberspazio sia vulnerabile tanto quanto quella digitale.

Il livello logico include *software*, *firmware* e protocolli che permettono il funzionamento delle infrastrutture e la comunicazione tra gli utenti. È in questo livello che si verifica la maggior parte degli attacchi informatici, i quali sfruttano vulnerabilità del codice per trasformare strumenti legittimi in *malware* o *ransomware*. Questi ultimi, cifrando i dati e rendendoli inaccessibili, rappresentano una delle minacce più redditizie per i criminali, capaci di paralizzare intere aziende e ottenere riscatti milionari[6].

Infine, il terzo livello è quello umano, che riguarda direttamente gli utenti. Essi costituiscono spesso l'anello più debole della catena di sicurezza. Tecniche di *social engineering*, come *phishing* e *smishing*, si basano sull'inganno e sulla manipolazione psicologica piuttosto che su complesse vulnerabilità tecniche[7]. Le minacce possono derivare da errori di progettazione, configurazioni errate o falle non ancora note, denominate *zero-day vulnerabilities*.

I metodi di attacco comprendono un ampio ventaglio di strumenti: *malware* di vario tipo, *ransomware*, attacchi *DDoS* (*Distributed Denial-of-Service*) e compromissioni della *supply chain*. Quest'ultima risulta particolarmente insidiosa: colpendo un fornitore, un attacco può propagarsi lungo l'intera catena di clienti, anche se questi dispongono di avanzati sistemi di difesa.

Le conseguenze economiche del *cybercrime* sono imponenti: secondo stime recenti, i danni globali superano i tremila miliardi di dollari all'anno, cifra destinata a raddoppiare nel prossimo

[5] https://submarine-cable-map-2024.telegeography.com/
[6] Dati del 2023, disponibili su: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023
[7] Cfr: C. Hadnagy, *Social Engineering: The Science of Human Hacking, chapter 3, Wiley Editor*, 2018.

decennio. L'Agenzia europea per la cybersicurezza (*ENISA*) monitora costantemente l'evoluzione delle minacce attraverso il rapporto annuale *Threat Landscape*. Questo documento classifica gli strumenti e le tecniche più diffuse, offrendo una panoramica dettagliata dello scenario attuale.

Tuttavia, per comprendere appieno il contesto *cyber* odierno, è necessario sottolineare la crescente interconnessione tra cyberattacchi e dinamiche geopolitiche. In questo senso, l'invasione russa dell'Ucraina ha rappresentato un punto di svolta: accanto alle operazioni militari convenzionali, si è verificata un'intensificazione degli attacchi informatici, volti a sabotare infrastrutture critiche, bloccare sistemi di pagamento e diffondere disinformazione.

Inoltre, il conflitto ha confermato un aspetto già ampiamente discusso nel settore: il ruolo sempre più centrale degli attori privati, tema che sarà approfondito nei prossimi capitoli. Di fatto, molte imprese — anche non direttamente coinvolte nel conflitto — si sono viste costrette a investire ingenti risorse per rafforzare la propria resilienza cibernetica[8].

1.2 Attori coinvolti

Gli attori che operano nel *cyberspace* sono molteplici e profondamente eterogenei. In primo piano vi sono ovviamente gli Stati, i quali, attraverso unità dedicate, conducono operazioni di *cyber espionage* su vasta scala. Tali attività non si rivolgono esclusivamente contro avversari dichiarati, ma anche verso Paesi formalmente alleati, allo scopo di ottenere vantaggi tecnologici, militari o diplomatici. Emblematico è il caso del Vaticano, bersaglio di campagne di spionaggio informatico attribuite ad attori cinesi in concomitanza con delicate trattative sulla nomina dei vescovi. Questo dimostra come nessun attore, nemmeno religioso, sia immune da tali pratiche.

Accanto agli Stati, operano gruppi di *cybercrime* mossi da finalità economiche. Questi sfruttano il modello del *cybercrime-as-a-service*, offrendo nel *dark web* pacchetti preconfigurati e servizi di assistenza tecnica. Questa industrializzazione dell'attività illecita abbassa significativamente la soglia di ingresso, consentendo anche a soggetti con competenze tecniche limitate di condurre attacchi complessi. Spesso, tali gruppi agiscono come *proxy* per Stati desiderosi di mantenere una plausibile negazione (*plausible deniability*) delle proprie responsabilità.

In questo contesto, la difficoltà di attribuzione rappresenta una delle sfide più critiche del dominio cibernetico, poiché ostacola le risposte diplomatiche e legali.

[8] Cfr: B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, *Oxford University Press*, 2016, p. 209-223.

Un altro attore rilevante è rappresentato dai cosiddetti *hacktivist*, gruppi di individui motivati da ideali politici o sociali, che nel corso degli anni hanno condotto azioni eclatanti. Tra i più noti vi è il collettivo *Anonymous*, autore di numerose operazioni, tra cui quella contro obiettivi russi dopo l'invasione dell'Ucraina nel 2022. Tuttavia, lo stesso collettivo aveva già colpito in passato infrastrutture italiane, evidenziando l'imprevedibilità delle loro azioni e la difficoltà di incasellarli in una dicotomia rigida tra "buoni" e "cattivi".

Le organizzazioni terroristiche, invece, utilizzano il *cyberspace* prevalentemente come piattaforma di propaganda, reclutamento e coordinamento, sfruttando la capacità della rete di amplificare messaggi ideologici e radicalizzare individui.

Altri attori rilevanti includono i *thrill-seekers*, spinti dal desiderio di sperimentare e dimostrare le proprie capacità, e le minacce interne (*insider threat*), ovvero soggetti appartenenti alle organizzazioni stesse che, per frustrazione o interesse economico, contribuiscono alla compromissione dei sistemi.

La molteplicità e l'eterogeneità di questi attori, uniti alla natura fluida e transnazionale del dominio cibernetico, hanno contribuito al riconoscimento del *cyberspace* come quinto dominio della conflittualità, accanto a terra, mare, aria e spazio[9].

1.3 Il cyberpower e la competizione geopolitica nel cyberspazio

Il concetto di *cyberpower* sintetizza la capacità di un attore di esercitare influenza strategica attraverso strumenti digitali. Secondo la definizione proposta da Joseph Nye, il politologo statunitense noto per aver coniato il concetto di *soft power*, la *cyberpower* si articola nella possibilità di costringere un avversario ad assumere comportamenti indesiderati, di limitarne le opzioni o di modificarne le preferenze. La misurazione di questa capacità è complessa, e diversi studi hanno prodotto classifiche differenti.

Il *National Cyber Power Index* del *Belfer Center* colloca gli Stati Uniti al vertice, seguiti da Cina, Russia e altri Paesi dotati di forti capacità tecnologiche. Anche Israele, Francia, Germania e Regno Unito figurano tra le potenze di rilievo, ciascuna con specifiche aree di eccellenza. L'asimmetria che caratterizza i conflitti tradizionali risulta attenuata nel *cyberspace*, poiché anche Stati minori, o persino attori non statali, possono acquisire capacità offensive significative con investimenti relativamente modesti.

[9] Cfr: T. Rid, "*Cyber War Will Not Take Place*", in *Journal of Strategic Studies,* 2012, pp.5-32.

Le *Advanced Persistent Threats (APT)* mostrano come gruppi sponsorizzati da governi possano infiltrarsi nei sistemi avversari e rimanere indisturbati per anni, raccogliendo informazioni sensibili o predisponendo azioni distruttive. L'anonimato, garantito da strumenti come *Tor*, *VPN* e *botnet*, e l'uso di *false flag*, complicano ulteriormente il quadro, lasciando tracce ingannevoli che deviano l'attribuzione verso soggetti estranei.

Il problema dell'attribuzione rappresenta uno degli aspetti più complessi della *cyber diplomacy*. Non si tratta più soltanto di individuare l'autore tecnico di un attacco, ma di stabilire chi ne sia politicamente responsabile. Le responsabilità statali possono variare, passando dalla completa estraneità, con collaborazione per fermare gli attacchi, fino all'integrazione diretta di unità *cyber* nelle strutture militari e governative.

L'attribuzione può essere di tre tipologie: può essere resa pubblica, utilizzata in modo selettivo con gli alleati o mantenuta privata. Ogni opzione comporta vantaggi e rischi: una dichiarazione pubblica serve a screditare l'avversario, ma può innescare escalation indesiderate; un'attribuzione selettiva rafforza la cooperazione tra partner; una comunicazione privata agisce da deterrente, ma senza produrre effetti visibili. La scelta dipende dal contesto, dalla gravità dell'attacco e dagli obiettivi strategici perseguiti.

Il *cyberspace*, dunque, non è solo un'infrastruttura tecnologica ma un'arena geopolitica, economica e diplomatica. La sua peculiarità consiste nella commistione di attori statali e non statali, nell'asimmetria delle capacità e nell'anonimato, che complica le relazioni di causa ed effetto. La necessità di una diplomazia specifica nasce proprio da queste caratteristiche: la *cyber diplomacy* rappresenta la risposta istituzionale e strategica a un dominio che sfida le categorie tradizionali delle relazioni internazionali.

Essa non riguarda più soltanto gli Stati, ma include imprese, organizzazioni internazionali, gruppi criminali e individui dotati di strumenti dirompenti. La definizione di norme condivise, la costruzione di meccanismi di cooperazione e la gestione del rischio di *escalation* sono le sfide centrali di questa nuova diplomazia digitale, destinata a incidere in maniera crescente sugli equilibri futuri della comunità internazionale[10].

1.4 Sfide principali: attacchi cyber, cyberwar e cyber espionage

[10] Cfr: D. Van Puyvelde – A.F. Brantly, *Cybersecurity: politics, governance and conflict in cyberspace*, *Polity Press*, 2019, pp.35-65.

La riflessione sul concetto di guerra nel dominio cibernetico ha rappresentato negli ultimi decenni un terreno fertile di dibattito tra studiosi, decisori politici e strateghi militari, poiché la natura stessa delle operazioni digitali sfugge alle categorie tradizionali della conflittualità. La difficoltà maggiore risiede in una semplice constatazione: la maggior parte delle attività malevole condotte attraverso strumenti informatici, a differenza di quanto accade negli altri domini, si colloca al di sotto della soglia convenzionalmente definita come guerra.

Queste attività ostili si svolgono infatti in quella che viene definita *"grey zone",* un'area di ambiguità in cui è difficile stabilire se un'azione debba essere qualificata come semplice disturbo o ostilità, *cyber espionage*, sabotaggio oppure vero e proprio *cyberwarfare*. La distinzione tra queste operazioni resta tutt'altro che chiara, poiché il *cyberspace* si caratterizza per estrema fluidità e per la compresenza di molteplici attori, che agiscono con strumenti e obiettivi differenti[11].

Non solo: anche la definizione stessa di *cyberwarfare* risulta problematica. Diversi autori ed esperti hanno espresso nel tempo opinioni divergenti: negli anni Ottanta e Novanta, quando si cercava di inquadrare queste nuove minacce, alcuni studiosi affermarono che la guerra cibernetica non potesse essere considerata guerra vera e propria, poiché priva delle caratteristiche tradizionali individuate dal generale Clausewitz, come la violenza fisica, l'intenzionalità politica e la capacità di costringere l'avversario. Sostenevano quindi che, allora come oggi, non si potesse parlare di guerra in senso stretto.

Al contrario, altri esperti, fin dai primi anni Novanta, hanno sostenuto esplicitamente la teoria opposta, prevedendo l'imminente inizio dell'era della guerra cibernetica. Torneremo a breve sulla componente storica e sul dibattito riguardo la definizione di *cyberwarfare*, ma prima è importante riflettere sulle ragioni per cui questo quadro risulta così poco definito, sia giuridicamente che politicamente.

Tra i fattori rilevanti in tal senso figurano la difficoltà di attribuzione, l'asimmetria tra attaccanti e difensori e la rapidità con cui si propagano le offensive digitali. Questi elementi contribuiscono a rendere arduo stabilire quando un'azione debba essere qualificata come atto di guerra.

Il dibattito teorico si è arricchito grazie a episodi concreti, storicamente, militarmente e politicamente rilevanti, che hanno dimostrato come le operazioni digitali possano avere impatti reali. Il caso più noto è quello di *Stuxnet*, che nel 2010 ha dimostrato come un malware potesse danneggiare

[11] M. Schmitt, "*Grey Zones in the International Law of Cyberspace*", in *Yale Journal of International Law*, 2017, p. 42 ss.

fisicamente un'infrastruttura critica, compromettendo le centrifughe di un impianto nucleare iraniano e segnando uno spartiacque concettuale.

Ma già nel 2007, con gli attacchi all'Estonia, si era evidenziata la capacità di campagne informatiche coordinate di paralizzare servizi essenziali di uno Stato. Nel 2008, durante il conflitto in Georgia, le offensive cibernetiche hanno accompagnato le operazioni militari russe, integrandosi con esse e aprendo la strada a una nuova concezione della guerra ibrida.

Questi eventi, insieme ad altri come gli attacchi alle centrali elettriche ucraine del 2015 e 2016, hanno segnato una transizione: si è passati da una fase di semplice consapevolezza a una vera e propria militarizzazione del dominio digitale. La comunità internazionale ha riconosciuto ufficialmente il *cyberspace* come nuovo dominio della conflittualità, integrandolo nelle strategie di difesa e nelle dottrine militari.

In particolare, a partire dall'episodio cardine di *Stuxnet* nel 2010, la riflessione accademica e politica ha dovuto confrontarsi con la consapevolezza che il dominio digitale non rappresenta più un ambito periferico, ma un fronte strategico in grado di incidere sugli equilibri internazionali.

Tuttavia, il concetto di guerra cibernetica non è affatto nuovo: se ne parla almeno dal 1993, quando John Arquilla e David Ronfeldt, in un articolo per la Rand Corporation intitolato "*Cyberwar is coming!*", affermarono che la guerra cibernetica era ormai imminente. Già negli anni Novanta, negli Stati Uniti vi era una crescente consapevolezza delle potenziali implicazioni per la sicurezza nazionale derivanti dalle minacce digitali. Da allora, il tema è stato ampiamente dibattuto e numerosi autori hanno espresso le loro opinioni. Nel 2012, Arquilla ha scritto su *Foreign Policy* che "la guerra cibernetica è già tra noi, sta accadendo oggi", sottolineando come eventi significativi – tra cui proprio la scoperta di *Stuxnet* nel 2010 – avessero rafforzato questa consapevolezza[12].

Oltre a quanto già citato, è importante ricordare gli attacchi subiti dall'Estonia nel 2007 e quello russo contro la Georgia nel 2008. Già in quegli anni, dunque, si era in un contesto caratterizzato da una rilevanza e un'attenzione – sia mediatica che internazionale – molto significative riguardo ai possibili effetti degli attacchi informatici.

Un autore particolarmente rilevante che si è schierato contro l'idea che la guerra cibernetica stesse effettivamente avvenendo è Thomas Rid. Nel 2013 Rid pubblicò il libro *Cyberwar will not take place*, nel quale sosteneva, già dal titolo, che la guerra cyber non sarebbe mai realmente avvenuta. Secondo Rid, la guerra nel cyberspazio non può mai possedere le caratteristiche clauswitziane fondamentali, quindi non si potrebbe parlare di *cyberwar*: per lui, infatti, la guerra nel dominio

[12] https://foreignpolicy.com/author/john-arquilla/, Cfr: J. Arquilla, *Bitskrieg*: *The New Challenge of Cyberwarfare*, *Polity Pr Editor,* 2021.

digitale non è né violenta, né strumentale, né politica – o, più precisamente, non può avere tutte e tre queste caratteristiche contemporaneamente.

Tuttavia, lo stesso Rid si è parzialmente ricreduto in seguito all'invasione russa dell'Ucraina, pubblicando poco dopo un articolo in cui riconosceva che, in realtà, la guerra cibernetica stava effettivamente avvenendo.

Vi sono poi altri autori che adottano un approccio più sfumato, concentrandosi sulla definizione stessa del concetto di guerra e su cosa contraddistingua la guerra nel cyberspazio. Tra questi, Colin S. Gray affermava che la guerra cyber si può definire solo come quella combattuta esclusivamente con mezzi cibernetici e tra i cosiddetti "*cyberwarriors*", ovvero una guerra puramente digitale.

Ancor più significativo è il contributo di Martin C. Libicki, il quale distingue tra "*Operational Cyberwar*" e "*Strategic Cyberwar*". Secondo Libicki, ciò che si è verificato finora può essere considerato solo *Operational Cyberwar*, cioè attacchi informatici condotti in tempo di guerra e rivolti a obiettivi militari. In altre parole, la *cyberwar* vera e propria, secondo lui, si manifesta soltanto all'interno di un conflitto bellico tradizionale, come ad esempio nell'invasione russa dell'Ucraina: in quel contesto, gli attacchi informatici sono parte integrante di un conflitto convenzionale.

Diversamente, la *Strategic Cyberwar* si riferisce a un tipo di conflitto che avviene senza una guerra tradizionale, cioè attacchi informatici contro uno Stato in assenza di un conflitto armato convenzionale. Libicki sostiene che questa forma di guerra cibernetica non si sia mai verificata[13][14].

Questa distinzione, seppur teorico-dottrinale, è utile per chiarire e restringere ciò che può essere considerato o meno "*cyberwar*". Infatti, nella prassi e nella comunicazione mediatica, ogni volta che si verifica una serie di attacchi informatici si parla spesso – e talvolta impropriamente – di *cyberwar*, senza un'adeguata riflessione sul contesto.

Questo discorso si lega anche a una questione giuridica importante: nel *cyberspace*, a differenza degli altri domini, è molto difficile distinguere tra pace e guerra, e di conseguenza risulta complesso capire quale diritto internazionale applicare. La maggior parte degli attacchi informatici si colloca nella cosiddetta "*grey zone*", una zona grigia al di sotto della soglia del conflitto armato, ma caratterizzata da azioni che potrebbero potenzialmente giustificare una risposta armata.

Un aspetto interessante è che spesso gli Stati preferiscono restare in questa zona grigia, o comunque operare entro questi confini senza superare mai una determinata soglia di escalation.

---

[13] Cfr: M. Libicki, *"What Is Information Warfare?"*, in *Center For Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defense University,* Washington DC, 1995, pp. 1-4.

[14] Cfr: M. Libicki, "*Cyberdeterrence and cyberwar",* in *RAND*, 2009, pp. 117-137 e 139-158

Da un punto di vista storiografico, alcuni esperti hanno proposto una periodizzazione dell'evoluzione della *cyberwarfare*. Tra questi, si segnala il manuale di Jason Healey, autore del concetto di "*spectrum of State responsibility*" e studioso della storia del conflitto nel cyberspazio. Healey individua tre fasi principali: *realization*, *takeoff* e *militarization*[15].

Secondo questa cronologia, l'origine della guerra cibernetica risale al 1986, anno in cui *hacker* tedeschi condussero una campagna di *cyber espionage* ai danni degli Stati Uniti, trafugando dati poi venduti al KGB, principale organo dell'*intelligence* sovietica.

La prima fase, che va da quell'episodio fino alla fine degli anni Novanta, viene definita *realization* perché è in questo periodo che gli Stati Uniti, e successivamente altri Paesi, prendono coscienza dell'importanza e della rilevanza della minaccia informatica per la sicurezza nazionale.

Questo periodo è segnato anche dal *Morris Worm*, il celebre virus informatico diffuso da uno studente della *Cornell University* che infettò numerosi computer, partendo dal laboratorio del MIT. Questo attacco ebbe una conseguenza significativa: in seguito al *Morris Worm*, gli Stati Uniti crearono il primo *CERT* (Computer Emergency Response Team), un team interno a organizzazioni pubbliche o private incaricato di gestire incidenti e crisi informatiche all'interno della struttura stessa.

Terminata questa fase, si definisce la seconda come quella di *takeoff*, che va dal 1998 al 2003. In questo periodo si svilupparono nuove strutture, organizzazioni e framework legislativi in ambito cybersecurity, e si intensificarono grandi campagne di *cyber espionage* su larga scala, condotte prevalentemente da attori statali, dato che in quegli anni l'utilizzo malevolo del cyberspazio da parte di attori non statali era ancora limitato.

Infine, Healey individua una terza fase, la cosiddetta *militarization*, che va dal 2003 al 2012, ma che si può probabilmente estendere fino ai giorni nostri (dato che il libro si ferma al 2012, coprendo solo quel periodo storico). La *militarization* consiste nella fase in cui gli Stati, consapevoli dell'importanza di possedere capacità offensive, iniziano a sviluppare e costruire strutture e strumenti militari cibernetici fondamentali per condurre operazioni sia offensive sia difensive nel cyberspazio. Questi anni sono segnati dalla scoperta di *Stuxnet*, dagli attacchi alla Georgia e all'Estonia, episodi che evidenziano come le dinamiche storiche e geopolitiche influenzino le strategie statali nel dominio digitale, sia in termini di azione sia di reazione.

Oltre all'aspetto cronologico e storico, nell'ambito della *cyberwarfare* emerge un tema centrale riguardante la natura stessa della conflittualità nel cyberspazio. Secondo i già citati Arquilla e Ronfeldt, autori che avevano previsto l'imminente guerra cibernetica, la guerra nel dominio digitale rivoluzionerebbe persino i concetti tradizionali di attacco, vittoria e sconfitta.

[15] Cfr: J. Healey, "*A Fierce Domain, Cyber Conflict 1986 to 2012"*, 2013, pp. 14-87

In primo luogo, gli attacchi nei domini convenzionali possono avere effetti devastanti e immediati, mentre gli attacchi informatici finora non hanno causato danni distruttivi paragonabili alle offensive militari più letali.

In secondo luogo, per quanto riguarda vittoria e sconfitta, nel cyberspazio tende a venir meno il senso classico di questi concetti che si ha nei domini tradizionali: in guerra convenzionale, vincere significa sconfiggere le forze nemiche, conquistare territori o raggiungere obiettivi strategici e diplomatici, con la conseguente sconfitta militare dell'avversario.

Nel cyberspazio, invece, gli attacchi difficilmente distruggono completamente le capacità militari dell'avversario. Di conseguenza, il concetto stesso di vittoria e sconfitta risulta in parte svuotato o almeno ridefinito.

La vittoria nel cyberspazio non si misura necessariamente con la sconfitta militare dell'avversario, perché quest'ultimo, finché disporrà di risorse organizzative, umane ed economiche, sarà sempre in grado di sviluppare armi cibernetiche. Questa distinzione è fondamentale e rappresenta, nel contesto delle relazioni internazionali, una novità importante, anche se di natura più teorica e dottrinale. Tuttavia, comprenderla è essenziale per avere una visione chiara del campo di gioco.

Un altro tema centrale per comprendere la *cyberwarfare* riguarda la deterrenza in ambito cibernetico. La deterrenza nasce come concetto teorico nel Secondo Dopoguerra ed è storicamente associata alla Guerra Fredda, periodo in cui si contrapponevano due blocchi. In effetti, la deterrenza ha funzionato in quel contesto — tanto che, in un certo senso, "siamo tutti ancora qui". Uno dei motivi principali del successo della deterrenza è stato il fatto che l'arma nucleare era considerata "l'ultima risorsa", ovvero uno strumento capace di causare una devastazione globale. Questo concetto, seppur in modo solo parziale, è ancora oggi alla base della deterrenza applicata al cyberspazio[16].

Nel tempo, la teorizzazione della deterrenza ha attraversato cinque ondate principali. Le prime tre si riferiscono alla Guerra Fredda, mentre la quarta è legata al crollo del Muro di Berlino e alla dissoluzione dell'Unione Sovietica.

In quel momento storico, non vi era più una netta contrapposizione tra blocchi, e l'attenzione iniziò a spostarsi verso nuove minacce, come quelle rappresentate dalle organizzazioni terroristiche. Queste, a partire dagli anni '90, divennero un problema crescente: dall'attentato del 1993 nel parcheggio del *World Trade Center* fino al tragico 11 settembre 2001, passando per numerosi altri attacchi tra la fine degli anni '90 e i primi anni 2000.

[16] Cfr: M. Clayton, "*The new cyber arms race*", in *The Christian Science Monitor*, 2011.

Durante questa quarta ondata, il focus rimaneva ancora sulle minacce "convenzionali", anche se in un contesto geopolitico mutato. Ci si interrogava su come potesse funzionare la deterrenza nei confronti di attori non statali, che agiscono secondo logiche differenti rispetto agli Stati.

La quinta ondata, tra il 2000 e il 2010, ha visto l'emergere delle minacce cibernetiche come questione di sicurezza internazionale. Fu soprattutto negli Stati Uniti che si cominciò a riflettere sull'efficacia della deterrenza applicata al cyberspazio, ponendo le basi per un dibattito sulle possibili modalità di implementazione.

In questo ambito, si distinguono tre tipi di attacchi rilevanti per la deterrenza cibernetica: attacchi cyber contro attacchi cinetici, attacchi cinetici contro attacchi *cyber*, e attacchi *cyber* contro altri attacchi *cyber*.

Le forme di deterrenza includono: (1) *Deterrence by punishment*: basata sulla minaccia di ritorsioni, molto efficace durante la Guerra Fredda; (2) *Deterrence by denial*: mira a negare il successo all'attaccante rafforzando le difese; (3) *Deterrence by entanglement*: fondata sull'interdipendenza dei sistemi globali, che rende rischioso l'attacco; (4) *Deterrence by normative taboos*: basata sulla creazione di norme e tabù condivisi[17].

Tuttavia, l'efficacia di questi approcci è limitata da alcune difficoltà, quali la complessità nell'attribuire con certezza la responsabilità degli attacchi, la possibilità di falsificare tracce digitali e la rapidità con cui gli eventi si susseguono.

L'esperienza storica mostra come una combinazione di strategie sia più efficace rispetto a un approccio unico: l'integrazione di capacità offensive limitate, il rafforzamento delle difese, l'imposizione di sanzioni economiche mirate e l'uso di strumenti reputazionali possono formare un pacchetto coerente, purché supportato da obiettivi chiari e prove credibili.

Nonostante i limiti, la deterrenza resta un elemento imprescindibile, non in grado di eliminare completamente il rischio, ma sicuramente utile a ridurne frequenza e gravità.

In questo senso, l'invasione russa dell'Ucraina nel 2022 ha rappresentato un banco di prova cruciale: sin dal 2014, l'Ucraina è stata oggetto di numerosi attacchi cibernetici, come quelli alle centrali elettriche che hanno provocato blackout su larga scala.

Nel 2022, tali azioni si sono intensificate e sono state integrate con l'offensiva militare convenzionale. Il sabotaggio della rete satellitare Viasat ha dimostrato la capacità degli attori russi di colpire infrastrutture critiche, ma ha anche evidenziato la resilienza ucraina, costruita grazie al sostegno occidentale e alla collaborazione con grandi aziende tecnologiche. La migrazione dei dati governativi sul cloud ha permesso di preservare informazioni vitali e garantire la continuità operativa,

[17] Cfr: M. Dunn Cavelty, "*The militarisation of cyberspace: Why less may be better*", in 4th *International Conference on Cyber Conflict* (*CYCON* 2012), 2012, pp. 1-13.

mentre la costituzione dell'*IT Army*, un esercito digitale di volontari volontari, ha mostrato l'importanza crescente degli attori non statali.

Gli Stati Uniti e l'Unione Europea hanno giocato un ruolo fondamentale nel rafforzamento delle difese ucraine: Washington ha dichiarato pubblicamente di condurre operazioni offensive di supporto, mentre Bruxelles ha attivato meccanismi di cooperazione, inviato team di risposta rapida e adottato sanzioni contro individui e organizzazioni responsabili di attacchi informatici.

L'esperienza ucraina conferma quindi che la *cyberwarfare* non è composta da episodi isolati, ma rappresenta un elemento strutturale dei conflitti moderni. Questo scenario ha anche sottolineato la centralità della cooperazione internazionale, poiché nessuno Stato può affrontare da solo le minacce digitali globali. Inoltre, ha messo in luce la sinergia tra dimensione statale e privata: società come *Microsoft*, *Amazon* e *Starlink* hanno avuto un ruolo determinante nel mantenimento delle comunicazioni e nella protezione dei dati[18][19].

Un altro caso rilevante è il conflitto tra Israele e Hamas, in cui le offensive informatiche si sono intrecciate con le operazioni militari tradizionali. Attacchi di *phishing*, *malware wiper* — una classe di malware progettata per cancellare i dati e i programmi dai dispositivi infettati — e campagne di disinformazione hanno accompagnato gli scontri sul terreno, con il coinvolgimento diretto e indiretto di attori statali come l'Iran. Israele, da parte sua, ha consolidato un sistema di difesa avanzato, il cosiddetto *Cyberdome*, progettato per proteggere le infrastrutture critiche, replicando in ambito digitale la logica difensiva del noto *Iron Dome* antimissilistico.

Il caso Stuxnet rimane emblematico del potenziale delle armi cibernetiche: pur avendo causato danni significativi, non ha impedito all'Iran di proseguire nel proprio programma nucleare, ma ha comunque aumentato la consapevolezza globale sull'importanza di difese robuste e strategie di resilienza.

Le *Advanced Persistent Threats* (*APT*) rappresentano un ulteriore esempio della natura duratura delle dinamiche cyber: si tratta di gruppi sponsorizzati da governi, in grado di infiltrarsi nei sistemi avversari e rimanere nascosti per anni, raccogliendo informazioni o preparando azioni distruttive. La loro esistenza sottolinea la persistenza della minaccia cibernetica e la difficoltà nel rilevarla e neutralizzarla.

Le *APT* evidenziano come il cyberspazio non sia un campo di battaglia occasionale, ma piuttosto un ambiente di conflitto permanente, dove la linea tra pace e guerra si fa sempre più sfumata.

---

[18] Cfr: J. Delcker, "*Ukraine's IT army: Who are the cyber guerrillas hacking Russia?",* in *Deutsche Welle*, 2022.

[19] U.S. Department of State, *"U.S. Support for Connectivity and Cybersecurity in Ukraine"*, 2022.

In questo contesto complesso, emerge la complessità della *cyber diplomacy*, che deve gestire questo continuum di ostilità: non solo prevenendo escalation verso conflitti convenzionali, ma anche costruendo regole condivise per il comportamento quotidiano nel cyberspazio. Le Nazioni Unite hanno avviato gruppi di esperti governativi e *open-ended working groups* con l'obiettivo di definire norme di condotta responsabile, ma i risultati restano limitati a raccomandazioni non vincolanti.

La competizione tra grandi potenze — in particolare Stati Uniti, Cina e Russia — ostacola l'adozione di strumenti giuridici vincolanti. L'Unione Europea si distingue invece per un approccio normativo e cooperativo, promuovendo l'adattabilità attraverso direttive, esercitazioni congiunte e meccanismi di solidarietà tra Stati membri[20].

Tuttavia, il problema dell'attribuzione resta centrale: stabilire chi sia responsabile di un attacco non è solo una questione tecnica, ma soprattutto politica, con tutte le conseguenze e i costi-benefici che ne derivano. Questo vale per tutte e tre le forme di attribuzione — pubblica, riservata e selettiva.

La mancanza di un quadro giuridico vincolante complica ulteriormente la situazione e rende indispensabile la diplomazia per evitare derive destabilizzanti. La dottrina militare degli Stati riflette la crescente importanza attribuita al dominio digitale: gli Stati Uniti hanno sviluppato la strategia di "*defend forward*", che consiste nell'individuare e neutralizzare le minacce direttamente nelle reti avversarie.

La Cina ha integrato le operazioni cibernetiche nella propria visione di "guerra informatica" e ha creato unità specializzate nell'Esercito Popolare di Liberazione. La Russia ha adottato una strategia offensiva del cyberspazio, combinando azioni di disinformazione con attacchi tecnici. Israele ha posto il cyberspazio al centro della propria dottrina di difesa, riflettendo la consapevolezza che la guerra cyber rappresenta una minaccia strutturale e permanente[21].

A complicare ulteriormente questo già complesso quadro vi è il ruolo degli attori non statali, molto numerosi e rilevanti, la cui proliferazione rende ancor più difficile ogni tentativo di regolamentazione. In questo contesto, le iniziative regionali e bilaterali assumono un'importanza crescente, così come il ruolo del settore privato, che detiene gran parte delle infrastrutture critiche e possiede capacità tecniche superiori a molti Stati. Su questi aspetti torneremo nel prossimo capitolo.

Tali approcci statali al cyberspazio e alla *cyberwarfare*, insieme all'importanza crescente e alla diversità degli attori non statali, mostrano come la *cyberwarfare* non sia più un tema marginale, ma una componente strutturale delle strategie nazionali di sicurezza. Nel complesso, il cyberspazio

[20] Cfr: D. Lo Prete, "*Cyberterrorismo: approcci della NATO e dell'UE a confronto*", *Geopolitica.info,* 2025.
[21] White House, *"National Cybersecurity Strategy"*, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023, 2023.

si configura come un'arena di conflitto permanente, in cui attori statali e non statali si confrontano attraverso *cyber espionage*, sabotaggi, disinformazione e tentativi di destabilizzazione.

La cyber *diplomacy* emerge come risposta necessaria per ridurre i rischi, costruire norme condivise e promuovere la cooperazione. Le sfide principali riguardano la gestione dell'attribuzione, la definizione di ciò che debba essere considerato un'infrastruttura critica (tema che affronteremo successivamente), la costruzione di meccanismi di deterrenza credibili e l'integrazione tra strumenti militari, tecnologici e diplomatici.

L'esperienza degli ultimi anni dimostra che, pur non potendo eliminare del tutto le minacce, è possibile rafforzare la resilienza e limitare i danni attraverso un approccio multilivello che coinvolge Stati, organizzazioni internazionali e attori privati. Tale approccio, per la sua complessità, può essere implementato attraverso molteplici soluzioni, discusse e proposte da esperti sia del settore pubblico sia privato, al fine di costruire una solida diplomazia *cyber*.

Sul piano operativo, è fondamentale costruire meccanismi efficaci di *incident response*: *CERT* nazionali e regionali, canali sicuri di scambio informativo, *playbook* condivisi ed esercitazioni periodiche sono prerequisiti essenziali per una reazione tempestiva. Dal punto di vista tecnico, pratiche come il patch management, la segmentazione delle reti, l'autenticazione forte e le architetture zero-trust riducono la probabilità di movimenti laterali e limitano la portata delle compromissioni.

La collaborazione pubblico-privato si è dimostrata cruciale e merita un'attenzione approfondita nei prossimi anni. Le grandi aziende tecnologiche hanno fornito supporto tecnico, intelligence sulle minacce *cyber* e infrastrutture fondamentali. È quindi indispensabile includere i *vendor* — ossia aziende specializzate in soluzioni di cybersicurezza che assistono altre organizzazioni nella protezione dagli attacchi — nei processi di *cyber diplomacy*. Tuttavia, questo ruolo solleva importanti questioni di accountability e governance, poiché la potenza operativa di soggetti privati può superare le capacità di controllo statale e influire sugli equilibri geopolitici[22].

L'esperienza ucraina ha evidenziato un ulteriore elemento: la mobilitazione di volontari digitali e hacktivisti può produrre effetti operativi significativi, ma introduce anche rischi legati al coordinamento e alla legittimità. Per questo, la regolamentazione delle attività non statali resta un tema sensibile e complesso.

Sul piano giuridico e normativo — che approfondiremo nel prossimo capitolo — si registra ancora un quadro in via di definizione: convenzioni sul cybercrime, iniziative ONU e quadri regionali cercano di colmare i vuoti, ma l'assenza di meccanismi vincolanti e di procedure condivise di

[22] Cfr: E. Schroeder, S. Dack, *"A parallel terrain: Public-private defense of the Ukrainian information environment",* in *Atlantic Council,* 2023.

enforcement limita l'efficacia. La definizione di infrastrutture critiche e la negoziazione di regole comuni sono passaggi necessari per costruire una governance internazionale credibile.

Infine, a livello pratico-operativo, è ampiamente riconosciuto che occorre investire in formazione specialistica e capitale umano, promuovere pratiche di *secure by design* e responsabilità nella *supply chain*, introdurre requisiti di trasparenza nella disclosure delle vulnerabilità e incentivare l'adozione di *standard* di sicurezza per i fornitori. Politiche di procurement pubblico orientate alla sicurezza, obblighi normativi per operatori critici e strumenti di cooperazione giudiziaria possono rendere più difficili le azioni degli attori criminali e aumentare il costo degli attacchi.

La gestione della comunicazione durante incidenti informatici, la preservazione delle evidenze forensi e la cooperazione transfrontaliera nelle indagini sono tutti elementi operativi essenziali per supportare attribuzioni e misure repressive.

La sfida principale è dunque trasformare questa realtà del cyberspazio — caratterizzata da anonimato, asimmetrie e interconnessioni — in un contesto governato da regole condivise e responsabilità chiare. Costruire una *cyber diplomacy* efficace non è solo auspicabile, ma necessario per garantire la stabilità delle relazioni internazionali nel XXI secolo.

CAPITOLO II

Il quadro giuridico internazionale

2.1 Diritto internazionale e cyberspazio: un rapporto complesso

Come già evidenziato nel capitolo precedente, tale affermazione non rispecchia pienamente la realtà, poiché permangono significative problematiche relative all'applicabilità del diritto internazionale al *cyberspace*. Tra queste, la questione dell'attribuzione e della responsabilità si configurano come le principali difficoltà, accanto all'assenza di una visione condivisa che risulta centrale nella dinamica complessiva del rapporto tra il mondo *cyber* e il diritto internazionale.

Per questo motivo, assume particolare rilevanza il lavoro di *cyber diplomacy*, volto a raggiungere una visione comune a livello internazionale tra gli Stati, favorendo una convergenza di interessi e di percezioni benché nell'ambito del *soft law*.

Altra questione spinosa che si segnala è che alcuni Stati interpretano la normativa internazionale nel *cyberspace* come una possibile limitazione della propria sovranità. In alcuni casi, tali iniziative sono state percepite come un eccessivo restringimento della sovranità statale, fino a configurarsi come una restrizione di diritti fondamentali dei cittadini, quali la tutela della *privacy* o l'accesso libero alle informazioni. Come si vedrà anche in seguito, tale mancanza di convergenza a livello globale è accentuata dalla natura stessa di alcuni regimi politici: ad esempio, governi non democratici tendono a rivendicare una sovranità quasi illimitata nel *cyberspace*, limitando l'accesso libero a Internet attraverso pratiche di censura e altre attività analoghe.

Analizzando il contesto storico in cui si inserisce il diritto internazionale nel *cyberspace*, si può osservare come, dopo una prima iniziativa russa nel 1998 finalizzata all'introduzione di controlli in ambito informatico, negli anni 2010 emergono i primi sforzi concreti a livello internazionale, con l'obiettivo di formulare proposte normative: queste ultime, sebbene parzialmente ispirate alla precedente iniziativa russa, provengono principalmente dagli Stati Uniti.

Nel 2013 tali norme trovano un primo riconoscimento formale con l'approvazione da parte del *Group of Governmental Experts* (UNGGE) presso le Nazioni Unite[23], mentre il *corpus* più rilevante di norme è stato adottato nel 2015, anch'esso su impulso dagli Stati Uniti[24].

[23] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General; https://digitallibrary.un.org/record/799853?v=pdf; https://www.ispionline.it/it/pubblicazione/dallonu-al-g7-i-primi-passi-della-comunita-internazionale-17212

[24] National position of the United States of America (2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021).

Nel dettaglio, gli Stati Uniti sostengono che il diritto internazionale esistente si applica pienamente anche al cyberspazio, promuovendo così maggiore prevedibilità e riducendo il rischio di conflitti involontari. In particolare, si riferiscono sia al *jus ad bellum*, che regola l'uso della forza e il diritto di autodifesa, sia al *jus in bello*, che disciplina la condotta durante i conflitti armati.

Le attività cibernetiche possono costituire un uso della forza se provocano danni significativi comparabili a un attacco convenzionale, e in tal caso possono legittimare l'autodifesa statale, che deve però essere sempre necessaria e proporzionata. Gli Stati devono rispettare i principi del diritto internazionale umanitario, evitando di colpire obiettivi civili e proteggendo personale e strutture mediche.

La sovranità statale si estende anche alle attività informatiche nel proprio territorio, sebbene con limiti dettati dal diritto internazionale e dai diritti umani, come la libertà di espressione[25].

Gli Stati possono violare la sovranità o il divieto di intervento coercitivo con azioni che interferiscano significativamente con le scelte interne di un altro Stato, come manipolare elezioni o danneggiare la salute pubblica. Tuttavia, lo spionaggio cibernetico in tempo di pace non è di per sé vietato, salvo effetti rilevanti.

Riguardo alla responsabilità, uno Stato è responsabile per atti illeciti attribuibili a sé o a suoi *proxy*, e l'attribuzione, sebbene complessa, richiede una valutazione ragionevole piuttosto che certezza assoluta. In risposta a tali atti, è legittimo adottare contromisure non violente, proporzionate e volte a far cessare la violazione, mentre le ritorsioni, come sanzioni o espulsione di diplomatici, sono sempre consentite nel rispetto del diritto internazionale[26].

Parallelamente, a livello europeo si compiono rilevanti sforzi nel campo della *cyber diplomacy*. Infine, nel 2021, viene pubblicato un nuovo rapporto statunitense che sostanzialmente richiama i principi formulati nel 2015.

Entrando nel merito, è fondamentale partire da un presupposto base del diritto internazionale: esso disciplina esclusivamente gli Stati e le relazioni tra Stati, nonché non si applica direttamente ai cittadini privati o alle aziende. Questa caratteristica costituisce una prima criticità nel contesto del *cyberspace*, poiché è ormai noto il ruolo rilevante svolto dagli attori privati.

Le società private, infatti, offrono molteplici servizi, inclusi quelli relativi allo spionaggio informatico a favore di Stati o altri soggetti, configurandosi come fornitori di servizi che possono essere acquistati sia da privati sia da enti statali.

---

[25] Cfr: H. Hongju Koh, "*International Law in Cyberspace",* in Harvard International Law Journal, 2012.

[26] Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021; UNODA, Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security https://digitallibrary.un.org/record/3934214?v=pdf

Un caso emblematico che ha attirato grande attenzione mediatica è quello del software *Pegasus*, impiegato – secondo alcune inchieste – anche dalle autorità italiane per attività di *cybersurveillance* ai danni di giornalisti. La vicenda è ancora oggetto di dibattito, e in certi casi sembra siano state violate norme sia del diritto nazionale sia del diritto internazionale, in particolare quelle legate alla tutela della *privacy*. Questo episodio evidenzia una delle questioni più complesse in materia di *cybersecurity*: la necessità di conciliare sicurezza e diritti fondamentali. Poiché gran parte delle infrastrutture digitali è in mano a soggetti privati, non è lo Stato a implementare direttamente le misure di protezione, ma piuttosto a imporre obblighi attraverso il diritto interno.

Di conseguenza, il ruolo degli attori non statali è centrale: essi sono spesso i primi a rilevare attività malevole, disponendo delle capacità tecniche per farlo, come nel caso della *cyber threat intelligence*. Oggi, per esempio, un'organizzazione che desideri valutare le proprie vulnerabilità si rivolge a società private specializzate in sicurezza informatica.

Il conflitto russo-ucraino ha ulteriormente dimostrato la rilevanza strategica degli attori privati nel cyberspazio: basti pensare al ruolo di SpaceX, che ha garantito la connettività in aree di conflitto tramite il servizio *Starlink*, o alla migrazione al *cloud* dei dati governativi ucraini tramite Amazon Web Services (AWS). In questo contesto, le *norms* – intese come aspettative collettive su comportamenti appropriati – assumono un ruolo chiave nel regolare la condotta nel cyberspazio.

Tali norme non nascono nel vuoto, ma si sviluppano a partire da prassi condivise tra Stati, che vengono successivamente formalizzate, ad esempio in documenti elaborati in sede ONU. Per essere efficaci, devono godere di un ampio consenso internazionale, poiché la loro legittimità dipende dalla condivisione da parte di un numero significativo di Stati.

Come spesso accade nel diritto internazionale, sono gli stessi Stati a conferire forza e rilevanza a queste norme attraverso la loro adesione – che, ovviamente, può anche non essere rispettata. L'adesione, inoltre, è spesso guidata da valutazioni strategiche o reputazionali: uno Stato ha interesse a essere percepito come promotore o rispettoso di un determinato insieme di norme, anche in ambito digitale.

Nonostante la loro natura non vincolante, queste norme devono comunque comportare obblighi specifici, agendo come raccomandazioni forti piuttosto che come mere dichiarazioni di principio[27]. Devono inoltre essere dinamiche, adattandosi a un panorama tecnologico in costante trasformazione, come dimostrato dalla recente evoluzione dell'intelligenza artificiale. In questo ambito, l'Unione Europea si è distinta con l'*AI Act*, prima iniziativa normativa di ampio respiro nel settore, adottata proprio per rispondere alle sfide poste da tecnologie emergenti. Lo stesso principio

[27] Cfr: B. Buchanan, *"The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, Oxford University Press*", 2016.

vale per il diritto applicato al cyberspazio, dove già dagli anni 2000 si è riconosciuta la crescente rilevanza delle minacce cibernetiche per la sicurezza internazionale.

In Italia, le prime normative e le prime strategie di *cybersecurity* arrivano negli anni 2013-2015. Quindi, a distanza di 10-15 anni, il diritto prende chiaramente in considerazione l'evoluzione tecnologica, ma in maniera non predittiva, bensì reattiva.

Non è stato dall'oggi al domani che Internet ha avuto l'impatto osservato negli anni successivi: sono stati necessari 30-40 anni affinché venisse prima creato il *World Wide Web* e poi si sviluppassero e diffondessero massivamente gli *smartphone* e i *social media*. È per questo che, negli anni 2000-2010, si è assistito a un progressivo incremento della digitalizzazione della società, un'evoluzione le cui tempistiche sono state successivamente seguite anche dalla normativa.

Ovviamente, è possibile essere critici riguardo alle tempistiche o alla gestione normativa, spesso reattiva rispetto ai cambiamenti tecnologici. Alcuni Stati agiscono con maggiore rapidità, mentre altri preferiscono lasciare maggiore libertà, normando di meno: tutto dipende dall'approccio che ciascuno Stato ha nei confronti delle norme. È chiaro che un elemento essenziale della norma è la sua possibile violazione: ci saranno Stati che le infrangono, ma ciò non implica che la norma cessi di esistere. Significa, piuttosto, che può evolversi o eventualmente essere abrogata, qualora una pluralità di Stati – gli stessi che l'hanno istituita – decida in tal senso[28].

Un aspetto fondamentale riguarda le fonti del diritto, in particolare lo Statuto della Corte Internazionale di Giustizia, che stabilisce come le fonti del diritto internazionale si basino su due elementi: la prassi degli Stati e l'*opinio iuris*. Le fonti del diritto internazionale – che si riscontrano anche nel contesto *cyber* – includono convenzioni internazionali, consuetudine internazionale, principi generali del diritto, giurisprudenza e, in alcuni casi, anche la dottrina degli autori più esperti.

Da qui emergono alcune problematiche legate all'applicazione del diritto internazionale nel cyberspazio, prima fra tutte la presenza di attori non statali.

Questo vale in due direzioni: da un lato, vi sono organizzazioni private che devono garantire la *cybersecurity* e che, di conseguenza, rivestono un ruolo chiave. Tuttavia, non operano direttamente nel diritto internazionale, né partecipano ai tavoli multilaterali tra Stati. Esistono comunque *partnership* pubblico-private, attività di *advocacy* o di *lobbying* fondamentali per la tutela di diritti e interessi specifici.

Dall'altro lato, esistono anche attori di minaccia non statali. Gli Stati, quindi, devono attrezzarsi per contrastare attacchi informatici condotti da questi soggetti. In quest'ottica sono nate, ad esempio, convenzioni come la *Budapest Convention* sul *cybercrime* del 2001 e l'ultima

[28] D. Van Puyvelde, A.F. Brantly, "*Cybersecurity: politics, governance and conflict in cyberspace", Polity Press,* 2019

Convenzione ONU del 2025 sul *cybercrime*, che sarà firmata a ottobre. Questo costituisce un primo elemento che ha imposto una riflessione sull'impostazione stessa del diritto internazionale, nel momento in cui si cerca di applicarlo alle condotte e alle relazioni tra Stati in ambito *cyber*.

Un ulteriore elemento problematico è rappresentato dalla costante evoluzione dello scenario delle minacce, che spinge il diritto a evolversi rapidamente. Si pensi, ad esempio, agli attacchi *ransomware*: nell'ultimo anno – e in particolare negli ultimi mesi – diversi Paesi, tra cui l'Italia, hanno avanzato proposte normative per contrastare questo tipo di minaccia. Gli attacchi *ransomware* mirano a criptare e rendere inaccessibili i dati dell'organizzazione colpita, per poi sottrarli e chiedere un riscatto (*ransom*), minacciando la pubblicazione dei dati in caso di mancato pagamento.

Per contrastare il fenomeno, molto diffuso e remunerativo, alcune normative – come quelle proposte nel Regno Unito e in Italia – prevedono l'obbligo per tutte le organizzazioni colpite di notificare l'attacco alle autorità competenti. Questo permette a enti come lo *CSIRT Italia* (*Computer Security Incident Response Team*), incaricato della gestione degli incidenti, o alla Polizia Postale, di supportare le organizzazioni sia nella risposta all'incidente, sia nella gestione del ricatto. Alcune proposte prevedono anche il divieto di pagamento del riscatto. In altri casi, invece, le forze dell'ordine hanno consigliato di pagarlo, al solo scopo di tracciarne il percorso. Anche se il pagamento avviene in criptovalute – rendendo più difficile il tracciamento – con strumenti adeguati si è riusciti più volte a risalire alle organizzazioni criminali responsabili.

Questi esempi mostrano come si muovono le autorità nazionali e dimostrano che anche il diritto internazionale deve adeguarsi dinamicamente allo scenario delle minacce, che – come già detto – è in continua evoluzione. Ancora una volta, non si può prescindere da una riflessione sulla rapidissima evoluzione tecnologica, in particolare nel campo dell'intelligenza artificiale.

Già oggi l'*intelligenza artificiale* viene utilizzata per condurre attacchi più sofisticati; quindi, è un elemento che il diritto internazionale deve prendere in considerazione.

Questo diventa molto più complesso quando non si tratta di legiferare a livello di parlamento nazionale, ma quando si cerca di trovare una condivisione su delle norme a livello internazionale, quindi tra Stati: un processo molto più lento, perché coinvolge Stati diversi che devono trovare un accordo tra visioni differenti.

C'è poi il problema legato alla soglia di conflitto armato: lo vedremo più avanti, quando parleremo di diritto umanitario internazionale applicato al cyberspazio. Come detto poc'anzi, in realtà la maggior parte degli attacchi avviene in quella che è definita come zona grigia, quella *grey zone* che si colloca al di sotto della soglia di conflitto armato. Ma tale zona risulta già difficile da definire di per sé, perché gli Stati non vogliono che un attacco informatico causi delle ripercussioni nel mondo

cinetico. Tuttavia, ciò implica una difficoltà nello stabilire quando applicare il diritto umanitario internazionale[29].

Anche se si parla continuamente di *cyberwar* e di guerra *cyber*, la terminologia in tal senso diventa fondamentale nel momento in cui si debba prevedere l'applicazione del diritto. Come conseguenza dell'applicazione del diritto umanitario internazionale, si riscontra poi il vasto tema delle sanzioni: quando uno Stato è sanzionabile per una condotta nel cyberspazio, se non ci sono norme vincolanti in tale ambito? Questo, al di là, chiaramente, dell'estrema ipotesi della morte di persone o di danni diretti a persone, eventualità che ad oggi non sono verificabili.

Va poi affrontato il tema dell'anonimato e dell'attribuzione, che vedremo meglio più avanti, e che però si ricollega al problema di non sapere chi ha condotto l'attacco, chi ne è responsabile; e anche, qualora si identifichi il computer da cui è partito l'attacco, resta da stabilire chi è il responsabile effettivo, chi ha dato l'ordine di attaccare e se si tratti di uno Stato oppure no. Ma gli Stati spesso si nascondono dietro attori *proxy*, quindi dietro gruppi di *cybercrime* o altri attori, talvolta anche gruppi di *hacktivisti*: questo complica ulteriormente l'*attribution*.

D'altra parte, l'anonimato non può essere garantito con assoluta certezza, ma può essere favorito dall'utilizzo di strumenti o tecniche, come analizzato precedentemente, mediante operazioni *false flag*, l'utilizzo di *VPN* o di *botnet*: tutti strumenti che favoriscono l'anonimato nel cyberspazio, e che costituiscono un elemento di vantaggio per gli Stati. Gli Stati, infatti, hanno un interesse operativo nel cyberspazio, proprio perché è più difficile dimostrare che abbiano avuto una condotta non coerente con il diritto internazionale[30].

Infine, un'ultima problematica da rilevare: non può esistere un regime di controllo degli armamenti nel cyberspazio. In primo luogo, perché è difficile dimostrare le capacità degli Stati, ovvero identificare e dichiarare le armi *cyber* di uno Stato è pressoché impossibile, poiché non sono visibili. Sia le capacità in termini di *cyberweapon* (quindi vulnerabilità, capacità di *cyber espionage* e simili) sia quelle in termini organizzativi: ad esempio, le strutture militari non sono pubbliche o, anche quando lo sono, non si conosce il personale addestrato al loro interno, né le capacità effettive, né i finanziamenti destinati ad operazioni offensive o difensive[31].

---

[29] L. Martino, *"La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica", Centro di Studi Strategici Internazionali e Imprenditoriali (CSSII),* 2014.

[30] F. J. Egloff, *"Contested public attributions of cyber incidents and the role of academia", Contemporary Security Policy 1 (2020),* pp. 55–81.

[31] A. Lupovici, *"The "Attribution Problem" and the Social Construction of "Violence", International Studies Perspectives,* 2016, Vol. 17, No. 3 (2016), pp. 322-342.

Soprattutto – ed è un altro elemento centrale del cyberspazio – le tecnologie sono *dual use*: ovvero, un *software* può, mediante la semplice modifica di alcune linee di codice, trasformarsi in un *malware*. Quindi, come si può vietarne lo sviluppo? Perché dovrebbe essere vietato anche lo sviluppo di un *software* che non nasce con uno scopo malevolo, ma che viene strumentalizzato e trasformato in un'arma?

Un'ultima grande problematica è poi il tema della sovranità, già precedentemente introdotto. Si tratta di un nodo centrale nel dibattito sull'applicabilità del diritto internazionale al cyberspazio, che continua a generare forti disaccordi tra gli Stati.

Ad esempio, la Cina ribadisce la centralità del principio di sovranità nel cyberspazio, preferendo un controllo stretto e diretto sulle infrastrutture digitali e sulle attività in Internet, anche a costo di ricorrere alla censura e di sacrificare diritti individuali. L'Unione Europea, invece, si muove fortemente sul piano dell'*advocacy*, promuovendo il diritto a un Internet accessibile, aperto, con informazioni disponibili per tutti, e dando priorità alle libertà individuali, come quella di espressione.

Dall'altra parte, la Russia propone la creazione di un nuovo strumento giuridico. Mentre Stati come gli Stati Uniti e l'Unione Europea prediligono l'applicazione al cyberspazio del diritto internazionale esistente, la Russia ha sempre sostenuto la necessità di nuove norme specificamente pensate per il cyberspazio[32].

Dopo aver analizzato queste problematiche, è necessario considerare anche altre sfide del diritto internazionale nel contesto *cyber*. Innanzitutto, il silenzio degli Stati: per molti anni, gli Stati non si sono espressi sull'applicazione del diritto internazionale al cyberspazio. Come già trattato, ciò è iniziato ad avvenire concretamente solo a partire dagli anni '10. È del 2013, infatti, l'adozione del primo *report* del *UNGGE*. Questo ritardo ha inevitabilmente rallentato anche l'applicazione e la condivisione delle norme a livello internazionale.

Le motivazioni del silenzio possono essere varie: da una parte, la volontà di evitare di esporsi a controversie internazionali; dall'altra, la mancanza di competenze tecniche e giuridiche adeguate per comprendere e affrontare le sfide del diritto internazionale in ambito *cyber*.

Come già detto, esistono anche divergenze di natura esistenziale: alcuni Stati contestano l'applicabilità del diritto internazionale al cyberspazio, compreso il diritto internazionale umanitario e il diritto all'autodifesa. In questi casi, viene privilegiata la sovranità nazionale rispetto ai diritti individuali o rispetto a ciò che potrebbe essere percepito come un'ingerenza del diritto internazionale negli affari interni.

---

[32] C. Gray, *"Making strategic sense of cyber power. Why the sky is not falling", Strategic Studies Institute, US Army War College*, 2013.

Vi sono poi sfide interpretative. Esiste molta ambiguità nell'applicazione del diritto internazionale al cyberspazio, ad esempio riguardo al principio del non intervento: non esiste consenso su cosa debba essere considerato "affare interno" di uno Stato e quindi protetto da tale principio.

Un altro tema interpretativo cruciale è quello delle infrastrutture critiche. Sebbene vi sia un accordo, sancito ad esempio dalle norme del 2015, sul fatto che non debbano essere condotti attacchi contro infrastrutture critiche, non esiste un consenso internazionale su cosa esse siano. Come si può, dunque, applicare una norma se non c'è chiarezza sull'oggetto della sua applicazione?

Per spiegare in modo semplice questa problematica: la Cina potrebbe colpire una struttura che gli Stati Uniti considerano infrastruttura critica, ma che la Cina non riconosce come tale – e viceversa – con tutte le conseguenze che ciò comporta.

2.2 Criticità sottese e riflessioni sul ruolo del diritto internazionale

Le principali norme di diritto internazionale in sede ONU vengono stabilite nel 2015, ribadite nel 2021 e adottate dall'Assemblea Generale con la risoluzione ONU 70/237. Risulta necessario e interessante analizzare nel dettaglio questi principi, poiché costituiscono il principale set di norme a livello internazionale applicabili al cyberspazio.

Partendo dal rapporto dell'ONU del 2015, esso si basava originariamente su due aspetti proposti dagli Stati Uniti, per poi essere ampliato fino a comprendere undici principi. I principali ambiti su cui il documento si concentra sono numerosi: in primo luogo, il focus è posto sulle minacce esistenti ed emergenti; seguono le norme e le regole per il comportamento responsabile degli Stati; le misure di *confidence building*, ovvero non solo l'adesione a norme di diritto internazionale, ma la creazione di meccanismi che rafforzino la fiducia reciproca tra Stati. Questo perché, attraverso la trasparenza, si crea affidabilità e si sviluppano rapporti basati su rispetto e credibilità reciproci. Altri ambiti trattati includono la cooperazione internazionale e il *capacity building*, l'applicabilità del diritto internazionale (fortemente sostenuta dagli Stati Uniti) e infine le raccomandazioni per i lavori futuri.

Le scelte delle tematiche poste al centro del documento sono state il frutto di anni di lavoro complesso, orientato alla ricerca di un accordo tra le grandi potenze, un lavoro che continua ancora oggi, tra difficoltà e momenti più produttivi nello sviluppo delle normative. Negli anni successivi al 2015, infatti, si è assistito a una fase di stallo nei lavori in sede ONU, ripresi nel 2019, ma nuovamente interrotti nel 2020 a causa della pandemia da Covid-19. Infine, nel 2021, si è giunti a ribadire le misure approvate nel 2015 attraverso un nuovo documento.

Nel rapporto del 2015, tali misure pongono particolare enfasi sui pericoli derivanti da attacchi contro sistemi e infrastrutture critiche. La visione degli Stati Uniti contrasta con quella della Russia: mentre la posizione statunitense mira a stabilire misure volontarie, la Russia propende per l'introduzione di obblighi morali che rappresentino un primo passo verso l'adozione di nuove norme giuridicamente vincolanti[33].

Il documento del 2015 è stato il risultato di un lungo processo avviato a partire dal rapporto del 2013, il primo ad essere approvato dal gruppo di lavoro dell'ONU. Tuttavia, rispetto a quest'ultimo, il documento successivo introduce alcune aggiunte sostanziali: vengono inclusi il principio di sovranità statale, l'uguaglianza sovrana, la risoluzione pacifica delle controversie, l'astensione dalla minaccia o dall'uso della forza nelle relazioni internazionali, il principio di non intervento negli affari interni di altri Stati e il rispetto dei diritti umani e delle libertà fondamentali.
Gli undici principi individuati sono i seguenti: la cooperazione tra Stati; il dovere di tenere in considerazione tutte le informazioni rilevanti; la prevenzione dell'uso malevolo dei sistemi ICT all'interno del proprio territorio; la cooperazione per porre fine al crimine e al terrorismo; il rispetto dei diritti umani e della privacy; il divieto di danneggiare le infrastrutture critiche; la protezione delle proprie infrastrutture critiche; l'obbligo di rispondere a richieste di assistenza, ad esempio in caso di incidenti che coinvolgano altri Stati; la garanzia della sicurezza della *supply chain*; la segnalazione delle vulnerabilità ICT; infine, il divieto di arrecare danno ai *CERT* o *CSIRT*, ovvero i team che si occupano della risposta alle emergenze o agli incidenti informatici[34].

Entrare nel dettaglio di ciascun principio consente di ottenere una visione più chiara e completa delle norme di diritto internazionale applicate al cyberspazio.
Innanzitutto, la cooperazione tra Stati rappresenta un fondamento del diritto internazionale, anche nel contesto digitale. Gli Stati devono cooperare per due ragioni principali: da un lato, per sviluppare e applicare misure atte a incrementare la stabilità e la sicurezza dei sistemi ICT; dall'altro, per prevenire pratiche dannose legate all'uso delle tecnologie ICT, come attacchi informatici, attività di *cyber espionage* e simili. Il mantenimento della pace e della sicurezza internazionale, pilastri del diritto internazionale, rappresenta quindi anche uno degli obiettivi centrali nel cyberspazio.

Per promuovere una cooperazione efficace nel cyberspazio, è fondamentale che gli Stati si dotino innanzitutto di una legislazione nazionale solida, accompagnata da normative e politiche mirate che incentivino la collaborazione internazionale in ambito cyber. A ciò deve affiancarsi la creazione di meccanismi per la gestione delle crisi e degli incidenti informatici, nonché la stipula di

[33] https://digitallibrary.un.org/record/799853?v=pdf
[34] U.N. GGE, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security",* 2015.

accordi di cooperazione, sia bilaterali che multilaterali, non solo con altri Stati, ma anche con il settore privato. In questo senso, assumono un ruolo centrale le partnership pubblico-private, che dovrebbero includere anche il mondo accademico e la società civile, al fine di creare un ecosistema resiliente e condiviso. Come per ogni principio fondamentale, anche rispetto alla cooperazione lo Stato deve interrogarsi sulla propria effettiva aderenza: ad esempio, se partecipa attivamente e con continuità ai principali forum multilaterali e regionali (come NATO, OSCE, ONU), dove si affrontano anche tematiche legate alla *cybersecurity* e alla *cyber diplomacy*. Tuttavia, la sola partecipazione formale non è sufficiente: lo Stato deve disporre di risorse e competenze adeguate, in particolare di personale qualificato con conoscenze sia tecniche che diplomatiche, in grado di contribuire attivamente allo sviluppo delle norme internazionali nel dominio cyber. Un altro elemento chiave è rappresentato dalla definizione di una strategia nazionale di cybersecurity, che preveda obiettivi specifici anche in termini di cooperazione internazionale. L'Italia, ad esempio, ha già adottato una strategia in tal senso, e prevede di pubblicarne una nuova dopo il 2026. La cooperazione è particolarmente cruciale poiché gli attacchi informatici, a differenza di quelli tradizionali (cinetici), hanno spesso una natura transfrontaliera. Questo accade perché il cyberspazio non conosce confini fisici, e la natura stessa delle infrastrutture digitali – fondate sul cloud e su reti globali – rende possibile colpire bersagli ovunque nel mondo, senza dover attraversare territori statali. Inoltre, in una società sempre più digitalizzata e interconnessa, in cui sistemi civili e militari sono profondamente intrecciati, un singolo attacco può avere ripercussioni su scala globale. Ne è un esempio il caso Microsoft Exchange, in cui una vulnerabilità non rilevata è stata sfruttata per operazioni di cyber spionaggio che hanno coinvolto non solo gli Stati Uniti, ma anche altri Paesi e organizzazioni internazionali. Tutto ciò dimostra quanto sia essenziale la cooperazione internazionale e, in particolare, la condivisione tempestiva delle informazioni. In caso di incidenti *cyber*, è inoltre indispensabile che lo Stato consideri tutte le informazioni rilevanti, analizzando il contesto più ampio in cui si inserisce l'evento e valutando le sue implicazioni sistemiche e potenzialmente globali.

2.3 Cyberspazio e diritto internazionale: un dibattito che sta ridefinendo le regole globali?

Il dibattito su come si applichi il diritto internazionale al cyberspazio sta avendo un impatto profondo e potenzialmente trasformativo su molte delle regole fondamentali del diritto internazionale. Questa discussione è ancora in corso e coinvolge numerosi contesti: dai negoziati intergovernativi come quelli del gruppo di lavoro ONU (*Open-Ended Working Group*)[35] sulla sicurezza informatica, alle iniziative della Croce Rossa Internazionale sull'applicazione del diritto umanitario nei conflitti armati nel cyberspazio. Anche esperti e studiosi contribuiscono attivamente, attraverso documenti come i *Tallinn Manuals* o l'*Oxford Process*.

A oggi, circa 40 Stati e due organizzazioni regionali (l'Unione Africana e l'Unione Europea) hanno pubblicato documenti ufficiali che esprimono la loro posizione sull'applicazione del diritto internazionale nel cyberspazio. Questo è un fenomeno raro: raramente gli Stati si sono espressi pubblicamente – e in modo così approfondito – sul contenuto di norme giuridiche così fondamentali[36]. Le posizioni affrontano temi centrali come il divieto dell'uso della forza, la non ingerenza, i diritti umani (privacy, libertà di espressione), la *due diligence*, la legalità del *cyber espionage*, e principi di diritto umanitario come la definizione di "obiettivo civile", la proporzionalità e i limiti alle *information operations* o alla *psychological warfare*. Sono discussi anche concetti di diritto secondario, come l'*attribution*, la *necessity* e le *countermeasures*.

Quello che rende questo dibattito così rilevante è che non si tratta di una discussione puramente tecnica: gli Stati non si limitano a spiegare come le norme si applichino nello spazio cibernetico, ma offrono vere e proprie interpretazioni di diritto internazionale generale, mostrando esempi concreti di condotte che potrebbero violare queste norme nel contesto digitale.

Per questo motivo, anche i giuristi internazionali che non si occupano direttamente di tecnologia dovrebbero prestare attenzione. Non è un tema di nicchia, ma un confronto che può ridefinire le basi stesse del diritto internazionale. Un utile strumento per approfondire questo dibattito è il recente *Handbook on Developing a National Position on International Law and Cyber Activities*, pensato proprio per aiutare i governi a sviluppare una posizione chiara e accessibile su questi temi.

Il manuale mostra che, pur con alcune differenze, gli Stati concordano su un punto fondamentale: il diritto internazionale si applica anche nel cyberspazio. Questo principio, spesso dato

[35] https://www.ohchr.org/en/hr-bodies/hrc/open-ended-intergovernmental-working-groups
[36] H. Moynihan, (2020). "*The vital role of international law in the framework for responsible state behaviour in cyberspac*e", in *Journal of Cyber Policy*, 2020, pp. 394–410.

per scontato, è in realtà di grande importanza perché implica che non è necessario riscrivere tutte le norme ogni volta che emergono nuove tecnologie[37].

Tuttavia, gli Stati differiscono sull'interpretazione di molte di queste norme, come dimostrano le varie posizioni sul divieto dell'uso della forza: alcuni ritengono che solo gli effetti "fisici" equiparabili a un attacco *kinetic* rientrino nel divieto, mentre altri includono anche i danni funzionali o economici. Ecco perché il silenzio di uno Stato in questo dibattito potrebbe essere interpretato come una forma di consenso implicito alle opinioni più diffuse, soprattutto se queste iniziano a consolidarsi. Inoltre, fino a poco tempo fa, questo dibattito era dominato da attori occidentali; la recente adozione di una posizione comune da parte dell'Unione Africana ha segnato un importante passo avanti per includere prospettive diverse. Coinvolgere più Stati, con tradizioni giuridiche e interessi politici differenti, è essenziale per rafforzare la legittimità e l'equilibrio del diritto internazionale che si va delineando nel cyberspazio[38].

Di fatto, attualmente bisogna considerare il fatto che la situazione inerente la gestione effettiva del cyberspazio risulta comunque in mano alle decisioni dei più grandi *player* tecnologici e geopolitici, quindi chiaramente gli Stati Uniti, la Russia, la Cina e l'Unione Europea.

Oltre ai documenti redatti in ambito ONU, vale la pena ribadire l'importanza della Budapest Convention del 2001: anche per il semplice fatto che si sia trattato del primo strumento giuridico globale dedicato specificamente ai reati commessi tramite computer e reti, e all'uso della tecnologia per commettere crimini tradizionali. Infatti, sebbene non riguardi direttamente i conflitti armati, essa stabilisce dei principi fondamentali per la cooperazione internazionale, nella prevenzione e repressione dei crimini informatici.

La Convenzione promuove la condivisione di informazioni, l'armonizzazione delle legislazioni nazionali e l'adozione di strumenti investigativi comuni. Tuttavia, la sua efficacia è limitata dall'assenza di alcune potenze tra i firmatari, come Russia e Cina, che contestano l'approccio occidentale ritenendolo sbilanciato: le tensioni geopolitiche emergono anche in questo contesto, rendendo difficile costruire un quadro normativo universale.

Va infine ricordato come l'Unione Europea abbia sviluppato un proprio approccio attraverso lo *European Cyber Diplomacy Toolbox*: un insieme di strumenti politici e giuridici per rispondere a cyberattacchi gravi, con misure diplomatiche, sanzioni e azioni coordinate.

L'obiettivo è rafforzare la resilienza degli Stati membri, promuovere la cooperazione e inviare un segnale dissuasivo agli attori malevoli. La logica del *Toolbox* riflette l'idea che la cybersicurezza

[37] Cfr: M. Helal, *"The Application of International Law in Cyberspace – A Debate that is Recoding International Law", Blog of the European Journal of International Law, 2025.*
[38] Cfr: D. Hollis "*A Brief Primer on International Law and Cyberspace*" in *Carneige Endowment for International* Peace, 2021.

non possa essere garantita solo con misure tecniche, ma richieda un approccio integrato che includa diplomazia, diritto e cooperazione multilaterale[39].

L'UE si distingue così per un modello basato sulla regolamentazione, sulla promozione di norme condivise e sulla difesa dei valori democratici, in contrapposizione a modelli più assertivi come quello statunitense o più restrittivi come quello cinese. Gli Stati Uniti adottano una strategia che combina difesa e deterrenza, riservandosi la possibilità di rispondere a cyberattacchi anche con mezzi cinetici. La logica americana privilegia la flessibilità e l'uso della potenza come strumento dissuasivo, enfatizzando il diritto alla legittima difesa e la centralità della superiorità tecnologica.

La NATO, dal canto suo, ha riconosciuto il cyberspace come dominio operativo al pari di terra, mare, aria e spazio, sottolineando la necessità di integrare le capacità cyber nella pianificazione militare. La logica dell'Alleanza è quella della difesa collettiva, per cui un attacco informatico grave potrebbe violare l'articolo 5 del Trattato di Washington. Questa posizione rafforza l'importanza del *cyberspace* nelle strategie di sicurezza collettiva, ma solleva interrogativi sull'attribuzione degli attacchi e sulla proporzionalità delle risposte.

[39] Cfr: D. Lo Prete, "*Cyberterrorismo: approcci della NATO e dell'UE a confronto*", *Geopolitica.info,* 2025

CAPITOLO III

Cyber Diplomacy e Politica Estera

3.1 Cyber diplomacy, sicurezza nazionale e relazioni internazionali: alcuni casi studio

Uno Stato non può considerare un attacco informatico preso singolarmente: deve andare a identificare chi è l'attore, in quale contesto potenzialmente geopolitico si inserisce. Oggi risulta particolarmente evidente, alla luce sia della conflittualità in Medio Oriente, sia della conflittualità tra Russia e Ucraina. Questo ha riguardato anche il cyberspazio: quindi lo Stato deve prendere in considerazione anche quegli elementi per capire la natura dell'attacco e potenzialmente anche dell'incidente, di conseguenza valutando anche quali misure mettere in piedi per mitigare l'impatto di attacchi futuri.

Non solo: il secondo principio considera informazioni rilevanti le discusse sfide dell'attribuzione nell'ambiente ICT, ovvero nel cyberspazio; esse sono numerose: l'anonimato è una delle principali, quindi l'*attribution* diventa molto complessa, sia da un punto di vista tecnico, che da un punto di vista politico. Identificare non solo il responsabile operativo, ovvero il PC da cui è partito l'attacco, ma anche potenzialmente il mandante dell'attacco (il quale possibilmente potrebbe anche essere uno Stato), quindi il responsabile ultimo[40].

Infine, il secondo principio tiene in considerazione la natura e l'estensione delle conseguenze: un attacco cyber con un impatto su un'infrastruttura critica di un determinato Stato, potrebbe avere un impatto ancora più elevato sull'infrastruttura critica di un altro Stato. Questo risulta utile e interessante poiché potrebbe portare uno Stato, da un lato, a essere obbligato a condividere informazioni con altri Stati, dall'altro anche a cooperare; questo perché magari si è subito lo stesso incidente o attacco, quindi si potrebbe cooperare per capire come gestire l'incidente e come mitigare l'impatto, o come ripristinare i sistemi colpiti.

Di conseguenza, per rispettare questa norma, gli Stati dovrebbero sviluppare delle strutture a livello nazionale, ad esempio degli CSIRT, o delle autorità cyber, e dovrebbero sviluppare delle politiche e delle procedure cyber per gestire incidenti, condividere informazione e sviluppare anche dei meccanismi di coordinamento con gli altri Stati.

[40] Cfr: F.J. Egloff e M. Smeets, *"Publicly attributing cyber attacks: a framework", Journal of Strategic Studies,* 2021.

Ad esempio, nel caso italiano risulta fondamentale la cooperazione a livello di Unione Europea: l'ENISA, ovvero l'Agenzia Europea per la Cybersicurezza, offre degli strumenti fondamentali anche di condivisione delle informazioni e anche delle opportunità di confronto tra i vari Stati membri[41].

Ma quali domande dovrebbe porsi uno Stato, per capire se realmente stia implementando questa norma? Innanzitutto, per appunto, se dispone di questi processi e di questi framework, per la valutazione dell'impatto.

A seguire, valutare se e quali agenzie governative siano coinvolte nel processo di valutazione e di gestione dell'incidente *cyber*, se in primo luogo abbia sviluppato o meno queste capacità; quindi anche se tale Stato abbia, per l'appunto, messo a disposizione o abbia previsto uno CSIRT nazionale, se abbia un CERT nazionale (in Italia c'è lo CSIRT Italia, che opera all'interno dell'Agenzia per la Cybersicurezza Nazionale).

A livello europeo, per rendere un esempio ancora più concreto, la direttiva NIS2 prevede un obbligo specifico per i soggetti che ricadono nella direttiva, e che quindi devono sottostare alla direttiva stessa, di notificare l'incidente entro 24 ore: questo in modo tale che lo CSIRT possa anche fornire un proprio feedback, un proprio supporto a queste organizzazioni; ma anche perché, spesso, le organizzazioni non hanno nemmeno le capacità necessarie, poiché non in tutte le organizzazioni c'è un team cyber in grado di gestire un incidente, soprattutto in quelle più piccole e con una maturità cyber inferiore. Quindi è di fondamentale importanza anche il supporto che può dare lo Stato[42]. Il terzo principio prevede che gli Stati non dovrebbero permettere consapevolmente che il proprio territorio sia utilizzato per atti illeciti tramite il cyberspazio.

In questo caso, si utilizza come criterio il c.d. "*spectrum state responsibility*", il quale, semplicisticamente parlando, con una valutazione da un livello 1 a un livello 10, consiste in una modalità per identificare la responsabilità degli Stati.

Ovvero, se uno Stato viene a conoscenza, anche in buona fede, che un atto illecito venga svolto dal proprio territorio, ad esempio un attacco informatico condotto dal proprio territorio (ai danni di un altro Stato), tale Stato dovrebbe prendere tutte le misure necessarie per contrastare gli attaccanti: quindi, sia per aiutare l'altro Stato, sia per contrastare l'attaccante, di conseguenza con misure di polizia e altre tipologie di misure.

Vi sono stati infatti dei casi reali in cui le gang di cybercrime sono state arrestate. Chiaramente deve essere anche compreso cosa si intende con atto internazionalmente illecito: questo è definito

41 https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape
42 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

come un atto che costituisce una violazione di un obbligo internazionale di uno Stato, attribuibile a un particolare Stato o a Stati, secondo il diritto internazionale. Quindi chi è il responsabile?

Non, nel caso in cui sia coinvolto un gruppo di *cybercrime*, il gruppo di *cybercrime*, ma l'atto internazionalmente illecito è compiuto dallo Stato che permette quell'attività, se chiaramente se ne riesce a venire a conoscenza, altrimenti risulta difficile e quasi impossibile poter fare qualcosa in merito.

Quindi quello che può fare uno Stato, per assicurare gli altri Stati riguardo la sua volontà di impedire che vengano commessi atti di questo tipo sul proprio territorio, è intraprendere attività investigative. Innanzitutto, sviluppando capacità investigative e repressive, per poi intraprendere attività di diverso tipo: attività anticrimine in primis, però allo stesso tempo, aderire alle convenzioni sul *cybercrime*, adottando di conseguenza quei principi che sono stabiliti, ad esempio, nella c.d. convenzione di Budapest, ovvero la Budapest Convention on *cybercrime*.

Anche qui, sul *cybercrime* non c'è un consenso su cosa sia definito come un atto che viene commesso tramite tecnologie di *information technology* o di Internet, in cui il computer o la rete sono il target dell'attacco: quindi un atto criminale, compiuto tramite l'utilizzo di tecnologie ICT o Internet, che ha per obiettivo un computer o una rete.

Ad esempio, la diffusione di un malware risulta essere un'attività di *cybercrime*: in questo caso, cosa si dovrebbe chiedere lo Stato per capire se stia veramente implementando questa norma? In primo luogo, dovrebbe chiedersi se ha previsto o meno delle norme che prevedano il *cybercrime* stesso, che quindi condannino il commettere attacchi informatici. A seguire, si dovrebbe valutare se lo Stato abbia sviluppato o meno quelle capacità di contrastare queste azioni criminali: ad esempio, essendo in grado di disattivare i siti che vengono utilizzati da questi cybercriminali, oppure se ha sviluppato delle capacità di contrastare o disattivare le infrastrutture che vengono utilizzate (PC, reti e via discorrendo) per commettere attacchi informatici; infine se lo Stato ha per l'appunto aderito o meno a convenzioni internazionali sul cybercrime.

Tra queste, si segnala la citata Convenzione di Budapest, ovvero la Convenzione ONU sul *cybercrime*, attualmente nella fase finale di sviluppo, che verrà firmata ad Ottobre 2025. Interessante osservare, nel contesto italiano, come il DPCM del 30 aprile 2025 preveda degli specifici elementi di cybersicurezza da applicare quando le organizzazioni pubbliche, e anche alcune organizzazioni private, si riforniscono: ovvero, il DPCM prevede che degli specifici *software* o *hardware*, con un'elencazione dettagliata di quali categorie di software e hardware, debbano contenere tutta una serie di elementi di cybersicurezza.

Questo perché uno dei problemi più grandi in ambito *cybersecurity*, non solo nel contesto italiano, è legato alla catena di fornitura, anche in ottica di security by design: ovvero, implementare la *cybersecurity* nella fase di progettazione[43].

Su questo c'è anche la normativa a livello europeo: il *Cyber Resilience Act* prevede tutta una serie di requisiti di *cybersecurity* per tutti coloro i quali producono, importano o distribuiscono prodotti digitali; ma essendo tali prodotti digitali molto variegati e numerosissimi, ci si è accorti dell'esigenza di attenzionare il problema legato alla catena di fornitura e alla *security by design*[44]. Questo poiché garantire la sicurezza già in fase di progettazione risulta fondamentale, perché chiaramente in un sistema che è "dentro un ecosistema" caratterizzato da PC vulnerabili, questo fattore aumenta l'esposizione verso l'esterno. Infatti, il grande problema legato alla *supply chain* è dovuto al fatto che, in molti casi, si riscontra l'uso di sistemi anche molto obsoleti, magari progettati dieci anni fa, dove la cybersecurity non era così attenzionata.

Il magistrato Nicola Gratteri, nel suo testo "Il grifone", evidenziava come le pubbliche amministrazioni (soprattutto in riferimento ai tribunali e ai ministeri, i quali trattano informazioni altamente critiche) abbiano delle vulnerabilità importanti a livello di cybersicurezza: come espresso nel capitolo precedente, nel contesto *cyber* (come in tutti i contesti in realtà) non si può ridurre mai la vulnerabilità a zero, però chiaramente si può lavorare con l'obiettivo di avere una minore esposizione alle vulnerabilità.

Se si utilizzano sistemi obsoleti, per esempio dei computer su cui è installato *Windows 98* (e non è un modo di dire, perché ancora oggi, in alcuni casi, delle organizzazioni pubbliche e private utilizzano sistemi così obsoleti), il punto non è che quel sistema risulti meno sicuro, poiché è stato progettato in modo meno sicuro quando la *cybersecurity* esisteva, ma non era concepita come è concepita oggi: il problema più grande è che non esistono più, dopo un certo numero di anni e dopo un certo numero di versioni rilasciate, gli aggiornamenti di sicurezza.

Un noto e interessante, quanto semplice, parallelismo in tal senso, piuttosto comune nel gergo del mondo *cyber*, è quello della sicurezza di una casa privata: se in una casa si rompe una finestra, e la casa è molto vecchia, al punto che non vendono più le finestre per quella stessa casa, la casa rimane senza finestra; questa è la rappresentazione di sistema di *cybersecurity* datato.

Diversamente, in una casa nuova, si può comunque rompere la finestra, ma la si può aggiustare, risolvendo quella vulnerabilità; stessa cosa per i software più recenti e con gli aggiornamenti di sicurezza. Altro tema legato a questo, è il tema delle vulnerabilità *zero-day*: le

[43] https://www.gazzettaufficiale.it/eli/id/2025/05/05/25A02717/sg
[44] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

vulnerabilità *zero-day* sono quelle vulnerabilità che vengono scoperte quando ancora non esiste l'aggiornamento di sicurezza.

Quindi se un attaccante, un attore di minaccia, scopre una vulnerabilità zero-day, per cui ancora non c'è una *patch*, un aggiornamento di sicurezza, egli può sfruttare quella vulnerabilità, proprio perché i sistemi hanno delle vulnerabilità. Questo è il motivo per il quale negli ultimi anni è cresciuta moltissimo l'attenzione verso la *security by design*: il tentativo è di garantire il più possibile, già in fase di progettazione, che i sistemi non abbiano vulnerabilità.

Il quarto principio del documento ONU del 2015, dal canto suo, prevede sempre una cooperazione tra Stati, con l'obiettivo di fermare il *cybercrime* e le attività terroristiche nel cyberspazio: quindi scambiare informazioni, cooperare, scambiare anche le c.d. "buone pratiche" sul contrasto al terrorismo e al crimine informatico[45].

Questo soprattutto perché le organizzazioni criminali tradizionali sempre più utilizzano le tecnologie per coprire le proprie operazioni, oppure proprio per compiere attività criminali.

Nel libro di Gratteri, ad esempio, si mette in evidenza come le mafie abbiano avuto maggiori incentivi nell'utilizzo del cyberspazio, proprio perché alcune attività criminali, per esempio la vendita di sostanze stupefacenti, o anche la vendita di armi, risultano facilitate tramite l'utilizzo del *dark Web*, mediante l'uso pagamenti in criptovalute, il che garantisce un maggiore anonimato. Questo è un altro aspetto di fondamentale importanza, più specifico sul *cybercrime* e sul terrorismo.

Ciò però ha comportato anche il fatto che gli Stati abbiano adottato dei meccanismi, come anche delle politiche, per il contrasto a livello nazionale del crimine e del terrorismo; e che quindi collaborino e cooperino con altri Stati, anche tramite strumenti a livello internazionale o regionale. Basti pensare ad esempio all'Europol, il quale prevede una sezione dedicata al *cybercrime* e che si occupa di tutte le attività di polizia necessarie per il contrasto al *cybercrime*.

Gli Stati devono poi avere dei meccanismi di condivisione delle informazioni, in modo tale da avvertire anche altri Stati su eventuali attività criminali commesse sul proprio territorio, e via dicendo. Quindi, come può lo Stato valutare il proprio impegno in questo ambito, chiedendosi se ha messo in essere queste politiche?

In primis, se ha delle capacità, anche in termini organizzativi, di strutture per il contrasto al *cybercrime* e al *cyberterrorism*, e se è parte di queste strutture (quindi Interpol, o Europol, le quali si occupano anche di contrasto alla criminalità, anche quella informatica)[46].

[45] https://digitallibrary.un.org/record/799853?v=pdf

[46] Cfr: D. Lo Prete, "*Cyberterrorismo: approcci della NATO e dell'UE a confronto*", *Geopolitica.info,* 2025

Il quinto principio è il rispetto dei diritti umani e della *privacy*: questo è uno dei temi chiave, che spesso si è scontrato con il concetto di sovranità degli Stati. Ovvero, gli Stati, per il concetto di sovranità, una volta potevano, a tratti possono, fare quello che vogliono nel cyberspazio, anche limitare i diritti: la sovranità degli Stati viene prima dei diritti individuali dei cittadini, dei diritti umani, dei diritti alla *privacy*.

Gli Stati dovrebbero rispettare alcune risoluzioni del Consiglio dei Diritti Umani dell'ONU, le quali sono proprio volte alla promozione, alla protezione, al godimento dei diritti umani su Internet. Quindi vi sono in questo caso delle risoluzioni specifiche per quanto riguarda i diritti umani all'interno del cyberspazio.

Inoltre, gli Stati dovrebbero partecipare anche ai forum che promuovono la creazione di norme, come anche prevedere l'applicazione di norme per la protezione dei diritti umani.

Ad esempio, la Convenzione ONU sul *Cybercrime* di recente approvazione, è stata molto criticata da diverse organizzazioni non governative, in quanto è stato osservato come alcuni articoli nello specifico potessero essere usati come un potenziale strumento normativo, nelle mani di governi autoritari, per reprimere la libertà di stampa, quindi applicando la censura, e anche come potessero portare a legittimare delle violazioni significative dei diritti alla *privacy*, mediante sorveglianza e attività analoghe.

Per verificare se lo Stato stia rispettando questa norma, si dovrebbe chiedere se lo Stato stesso consenta la libertà di espressione e i diritti alla *privacy* online: in tal senso, esiste un interessante indice della libertà online, redatto annualmente da *Freedom House*, ovvero il *Freedom on the net*. Sulla base di questo documento, risulta a tratti persino sorprendente la posizione di alcuni Stati democratici (come gli Stati Uniti, oppure la stessa Italia), perché in realtà, persino in molti Stati democratici, la libertà online non ha un grado che si ritiene adeguato a quello che invece dovrebbe essere il contesto di democrazia[47].

Altro criterio per verificare l'adeguamento o meno di uno Stato al quinto principio, è verificare se lo Stato abbia o meno le capacità e i mezzi per far rispettare i diritti umani online e la *privacy*: il che risulta un punto oggettivamente complicato da attuare, in quanto la rete è un ambito sul quale si ha un controllo limitato; Internet non è nelle mani degli Stati, almeno nella maggior parte dei democratici, e non essendo nelle mani degli Stati, gli attori predominanti sono quindi i soggetti privati, basti pensare ai social media.

[47] Cfr: A. Funk, K. Vesteinsson, G. Baker, *"Freedom On the Net: the Struggle for Trust Online 2024", Freedom House,* 2025.

Diventa in tal senso anche difficile intervenire, per riuscire a garantire e verificare anche delle violazioni dei diritti umani all'interno di social media e su Internet in generale.

Arrivando al sesto principio, questo afferma l'esistenza di un divieto specifico per gli Stati, ovvero: gli Stati non dovrebbero arrecare danno a infrastrutture critiche degli altri Stati.

Questo significa astenersi da tutta una serie di attacchi, ma anche attività di cyber espionage, che possono arrecare danno alle infrastrutture critiche. Il grande problema è che non esiste una visione condivisa di quelle che siano le infrastrutture critiche a livello internazionale: quindi, anche qui, si crea il problema dell'interpretazione della normativa.

Ciò comporta che gli Stati devono essere in grado di identificare quelle che sono le infrastrutture critiche dell'altro Stato, il che comporta anche il dover verificare se il proprio Stato abbia delle capacità offensive che possano nuocere agli altri Stati, oppure che possano arrecare danno alle infrastrutture critiche di altri Stati.

Infine è prevista anche in questo caso la necessità di collaborare, anche a livello internazionale, bilaterale e multilaterale, per rafforzare la resilienza e la sicurezza delle infrastrutture critiche.

Il settimo principio risulta essere l'altra faccia della medaglia rispetto al punto precedente, ovvero una misura attiva: l'obbligo di proteggere le infrastrutture critiche. Quindi gli Stati devono adottare delle misure che siano adeguate in modo da proteggere le proprie infrastrutture critiche da minacce cyber. Ma anche in questo caso, risulta un problema di interpretazione normativa, stavolta per quanto riguarda il concetto stesso di protezione: questo poiché ognuno ha dei concetti diversi di infrastrutture critiche. Non solo: anche in questo caso, la maggior parte delle infrastrutture digitali critiche sono nelle mani di privati.

Questo è il grande tema: gli Stati non possono agire in modo diretto per garantire la *cybersecurity* di tutte le infrastrutture critiche. Persino nel caso delle infrastrutture critiche legate alla pubblica amministrazione, in realtà, il governo in quel caso si limita a legiferare, può imporre degli obblighi, come fatto di recente per le pubbliche amministrazioni e anche per le aziende private.

Quindi proteggere le infrastrutture critiche rappresenta un grande problema per gli Stati, almeno per quegli Stati che hanno la maggior parte delle infrastrutture in mano a privati, proprio perché agiscono indirettamente. Questa è una prima grande sfida; poi, chiaramente gli Stati devono avere le capacità per proteggere le proprie infrastrutture critiche.

Ad esempio, per quanto riguarda quelle in mano alle amministrazioni pubbliche, vi devono essere risorse adeguate, sia in termini economici, quindi di investimenti, sia in termini di persone. Ovvero, non basta dire che bisogna implementare misure di sicurezza, o che bisogna implementare

firewall, o fare dei corsi di formazione: bensì, ci devono essere persone formate, in grado di entrare nel merito di queste misure, che siano tecniche e che fanno formazione e *awareness*.

Quindi, tanti aspetti della *cybersecurity* ruotano intorno alle capacità delle persone, ovvero dei team: però, chiaramente, dipendono anche dalle effettive capacità e dalle conoscenze delle persone. Il che risulta essere un punto abbastanza manchevole, in quanto si riscontra attualmente una carenza, a livello globale, di milioni di posizioni non coperte, sia in ambito tecnico che non tecnico, nel contesto *cyber*.

In conclusione, lo Stato deve essere adeguatamente consapevole anche di quelle che sono le infrastrutture critiche del proprio paese: in Italia ad esempio, la normativa europea, ovvero la direttiva NIS2, definisce quelle che sono le infrastrutture critiche, e la legge 133 del 2019 ha definito altri settori più specifici, che riguardano e allargano il perimetro delle infrastrutture critiche.

Sulla base di tale perimetro, si interviene per assicurare un maggiore livello di *cybersecurity*: quindi lo Stato deve prima identificare le infrastrutture critiche, i settori considerati, ma anche le organizzazioni che fanno parte di quelle stesse infrastrutture critiche[48].

Infine, vi devono essere dei meccanismi di coordinamento tra governo e queste infrastrutture critiche: questi con lo scopo di fornire gli aggiornamenti riguardo le misure di sicurezza implementate, come per la semplice notifica degli incidenti, la segnalazione della vulnerabilità e via dicendo; quindi meccanismi di coordinamento, ma anche di information sharing.

L'ottava misura prevede poi che gli Stati rispondano alle richieste per assistenza: quindi, nel caso in cui uno Stato sia vittima di attività criminali o di attacco informatico di una propria infrastruttura critica, e chieda aiuto a un altro Stato, questi è tenuto a rispondere alla richiesta di aiuto. Emblematico in tal senso è stato il caso dell'Ucraina, alla quale molti Stati, già in precedenza rispetto all'invasione russa del 2022, hanno fornito aiuto.

Gli Stati Uniti, oltre che gli Stati membri dell'UE, hanno fornito aiuto all'Ucraina per rafforzarne le difese *cyber* e poi per mitigare gli impatti degli attacchi informatici[49][50].

Per verificare la conformità su questo punto, uno Stato si deve chiedere se ha le capacità di rispondere a una richiesta di aiuto, se quindi possiede un team dedicato per la pronta risposta. L'Unione Europea, pur non essendo chiaramente uno Stato, ha attivato un team specifico per supportare l'Ucraina nella risposta agli incidenti *cyber*: quindi il principio non riguarda solo gli Stati, ma anche le organizzazioni a carattere regionale.

---

[48] https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg

[49] Cfr: T. Grossman, M. Kaminska, J. Shires, M. Smeets, *"The Cyber Dimensions of the Russia-Ukraine War",* in *ECCRI*, 2023.

[50] Cfr: B. Smith, "*Defending Ukraine: early lessons from the cyber war*", in *Microsoft on the issues,* 2022.

Il che chiaramente comporta avere anche visibilità riguardo quel che avviene negli altri Stati: significa creare delle partnership tra agenzie *cyber* nazionali (o comunque, governo nazionale) e altri governi o agenzie cyber, su tematiche di *cybersecurity*, quindi per esempio, agire mediante la condivisione di informazioni su incidenti, minacce o richieste di aiuto.

Sostanzialmente, vi devono essere dei canali che avvengono o in modo bilaterale o tramite l'Unione Europea, tramite l'ONU, e così via. Vi è poi il tema della *supply chain*: secondo il nono principio, gli Stati dovrebbero innanzitutto adottare misure per garantire l'integrità della *supply chain* e dovrebbero cercare di prevenire la proliferazione di strumenti e tecniche ICT dannose, o l'uso di funzioni nascoste dannose.

Di conseguenza, tutte le tematiche relative, ad esempio, a software malevoli la cui diffusione dovrebbe essere prevenuta. Questo comporta l'implementazione di diverse politiche e capacità per garantire la sicurezza della catena di approvvigionamento.

Nell'Unione Europea è stato definito, oltre al *Cyber Resilience Act,* anche uno schema di certificazione *cyber*, laddove dei prodotti digitali possono essere certificati tramite specifiche valutazioni, viene data una certificazione di *cybersecurity*: quindi quei prodotti, uno specifico software ad esempio, è definito ed elencato nello schema di certificazione, quindi ha ricevuto il bollino dall'Unione Europea, che risulta sicuro dal punto di vista *cyber*.

Questo poi deve essere recepito nei singoli Stati: l'Italia, dal canto suo, ha recepito questo schema a livello nazionale. Inoltre, è stato poi previsto il recepimento anche della direttiva NIS2, la quale introduce anche l'obbligo, per le organizzazioni, di prevedere specifici requisiti di *cybersecurity* per i fornitori. Quindi la gestione da un lato dei fornitori, dall'altro dei prodotti. Il *Cyber Resilience Act* quindi mira a mitigare l'impatto di vulnerabilità a livello in fase di produzione.

Il decimo principio prevede l'elemento legato alle vulnerabilità: devono essere previsti dei sistemi per la comunicazione e la condivisione di informazioni relative a vulnerabilità; questo proprio perché, come discusso prima, una vulnerabilità potrebbe riguardare un sistema che è utilizzato in tanti altri Stati, quindi condividere prontamente quell'informazione di una vulnerabilità sfruttata, significa potenzialmente prevenire un incidente su una scala più ampia.

Questo richiede sia procedure di condivisione di informazioni, come anche capacità di identificare le vulnerabilità: quindi avere delle capacità statali (o meglio, delle persone all'interno degli apparati statali) che siano in grado di identificare le vulnerabilità, tramite attività di *vulnerability assessment* e *penetration test*, le quali sono volte proprio a identificare delle vulnerabilità nei sistemi valutati.

Infine, l'undicesimo e ultimo principio consiste in un divieto, ovvero non arrecare danno ai team di risposta agli incidenti: questo perché gli Stati non dovrebbero condurre o supportare attività che danneggiano i sistemi dei team di risposta alle emergenze; questo perché sarebbe in parte, facendo un parallelismo con tutte le distinzioni del caso, come attaccare un ospedale, perché consisterebbe in un attacco rivolto a una struttura che è prevista per gestire un'emergenza nel cyberspazio, potenzialmente come l'ospedale nel mondo fisico. Quindi i team, i *computer emergency response teams* (i CERT e anche i CSIRT nazionali) non dovrebbero essere target di attacchi informatici. Allo stesso tempo, i CERT nazionali non dovrebbero essere utilizzati dagli Stati per condurre attacchi informatici: quindi dovrebbero essere utilizzati solo in ottica difensiva e non anche offensiva. Questo perché chi sviluppa capacità e opera all'interno di un CERT, potenzialmente, potrebbe anche avere delle conoscenze tecniche tali da condurre potenzialmente attacchi *cyber*[51].

[51] https://digitallibrary.un.org/record/799853?v=pdf

CONCLUSIONI

Il cyberspazio risulta allo stesso tempo, nel contesto contemporaneo, una roboante quanto (paradossalmente) silenziosa rivoluzione, da moltissimi punti di vista e in diversi settori, anche apparentemente lontani tra loro: un'analisi complessiva, come quella tentata a grandi linee in questo elaborato, non può fare a meno di analizzare diversi campi e saperi, che vanno dallo sviluppo e dall'evoluzione tecnologica, alla politica estera e alla geopolitica, passando per il diritto internazionale quanto nazionale, come anche per l'economia e la difesa dei soggetti tanto pubblici quanto privati.

Se le soluzioni e le risposte risultano complesse e allo stesso tempo complicate da trovare e ancor più da attuare, le domande in questo senso sono molte e continuano ad aumentare, tanto nella quantità quanto nell'impatto che comportano nella vita di tutti i giorni, dalla semplice quotidianità alle grandi questioni internazionali e globali: risulta sempre più centrale tentare di trovare delle soluzioni che siano coerenti, soprattutto dal punto di vista di quella parte del mondo che si ispira e si basa su valori e concetti democratici, ma allo stesso tempo concrete ed efficaci.

La cyber diplomacy potrebbe risultare al centro della risoluzione di molte delle problematiche legate al contesto cyber: le soluzioni non possono risultare solo legate all'aspetto tecnologico o a quello legislativo, in primo luogo risulta e risulterà probabilmente sempre di più necessario trovare dei compromessi, degli accordi e delle soluzioni condivise, se non a livello di unanimità, perlomeno con un ampio consenso internazionale. In tal senso, come espresso nei tre capitoli di questo testo, sono stati effettuati molti passi avanti, per quanto lenti e mai realmente vincolanti.

In primis, dal punto di vista delle Nazioni Unite, con i vari report dell'UNGGE a partire dal 2013, ancora prima con un altro importante punto di riferimento del settore, rappresentato dalla *Budapest Convention*, il primo trattato internazionale volto a contrastare il *cybercrime*.

In particolare, per quanto sia molto discusso e dibattuto da molti, l'approccio europeo risulta essere il più proattivo (secondo alcuni, a diverse sfumature di criticità, il più invasivo) tra i grandi attori internazionali, nel cercare soluzioni quanto a normare e regolamentare il settore cyber: il che non stupisce eccessivamente, considerato come approccio si sia riscontrato anche in quasi tutte le altre questioni più importanti degli ultimi decenni, anche molto diverse, da quella ambientale a quella recentissima dell'Intelligenza Artificiale.

Tale aspetto viene spesso criticato da diversi esperti interni quanto esterni all'Unione, valutando il tutto come caratterizzato da un'eccessiva burocratizzazione, lentezza e limitazione per l'innovazione e lo sviluppo dei vari settori, con delle conseguenze inintenzionali complessivamente peggiori nei risultati rispetto alle aspettative dei vari interventi: il dibattito in tal senso è sempre aperto, anche nel contesto cibernetico.

Di fatto, il confronto tra i diversi approcci mostra come il cyberspazio sia divenuto un terreno di competizione normativa e strategica: l'UE tende a privilegiare la costruzione di norme condivise e la cooperazione multilaterale, gli Stati Uniti puntano su deterrenza e flessibilità, la NATO sulla difesa collettiva, mentre Russia e Cina promuovono modelli alternativi fondati sul controllo statale delle reti e sulla sovranità digitale.

Sarà il tempo a valutare se, ed eventualmente quanto, la cyber diplomacy riuscirà a divenire sempre più uno strumento centrale, oltre che un approccio centrale, all'interno delle dinamiche globali, non solo legate al *cyberspace*; e sarà il tempo a mostrare verso quale direzione (o magari, direzioni diverse) questo influenzerà e impatterà il contesto internazionale, tanto normativo quanto tecnologico, ma anche politico e culturale.

BIBLIOGRAFIA

DOTTRINA

1) Buchanan B., *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, Oxford University Press,* 2016.
2) Clayton M., "*The new cyber arms race*", in *The Christian Science Monitor,* 2011.
3) Delcker J., "*Ukraine's IT army: Who are the cyber guerrillas hacking Russia?",* in *Deutsche Welle,* 2022.
4) Dunn Cavelty M., "*The militarisation of cyberspace: Why less may be better*", in *4th International Conference on Cyber Conflict* (*CYCON* 2012), 2012.
5) Egloff F.J., *"Contested public attributions of cyber incidents and the role of academia",* in *Contemporary Security Policy 1,* 2020.
6) Egloff F.J., Smeets M., *"Publicly attributing cyber attacks: a framework",* in *Journal of Strategic Studies,* 2021.
7) Funk A., Vesteinsson K., Baker G., *"Freedom on the Net: Struggle for Trust Online 2024",* in *Freedom House,* 2025.
8) Grossman T., Kaminska M., Shires J., Smeets M., *"The Cyber Dimensions of the Russia-Ukraine War",* in *ECCRI*, 2023.
9) Gray C., *"Making strategic sense of cyber power. Why the sky is not falling",* in *Strategic Studies Institute, US Army War College*, 2013.
10) Hadnagy C., "*Social Engineering: The Science of Human Hacking, chapter 3, Wiley Editor"*, 2018.
11) Healey J., "*A Fierce Domain, Cyber Conflict 1986 to 2012"*, 2013.
12) Helal M., *"The Application of International Law in Cyberspace – A Debate that is Recoding International Law", Blog of the European Journal of International Law,* 2025.
13) Hollis D., "*A Brief Primer on International Law and Cyberspace*" in *Carneige Endowment for International* Peace, 2021.
14) Hongju Koh H., "*International Law in Cyberspace",* in *Harvard International Law Journal*, 2012.
15) Libicki M., *"What Is Information Warfare?"*, in *Center For Advanced Command Concept and Technology, Institute for National Strategic Studies, National Defense University,* Washington DC, 1995.

16) Libicki M., "*Cyberdeterrence and cyberwar",* in *RAND*, 2009.
17) Lo Prete D., "*Cyberterrorismo: approcci della NATO e dell'UE a confronto*", in *Geopolitica.info*, 2025.
18) Lupovici A., *"The "Attribution Problem" and the Social Construction of "Violence",* in *International Studies Perspectives,* Vol. 17, No. 3, 2016.
19) Martino L., *"La quinta dimensione della conflittualità. La rilevanza strategica del cyberspace e i rischi di guerra cibernetica",* in *Centro di Studi Strategici Internazionali e Imprenditoriali (CSSII),* 2014.
20) Moynihan H., "*The vital role of international law in the framework for responsible state behaviour in cyberspac*e", in *Journal of Cyber Policy*, 2020.
21) Rid T.,*"Cyber War Will Not Take Place*", in *Journal of Strategic Studies,* 2012.
22) Schmitt M., "*Grey Zones in the International Law of Cyberspace*", in *Yale Journal of International Law,* 2017.
23) Smith B., "*Defending Ukraine: early lessons from the cyber war*", in *Microsoft on the issues,* 2022.
24) Schroeder E., Dack S., *"A parallel terrain: Public-private defense of the Ukrainian information environment",* in *Atlantic Council,* 2023.
25) U.N. GGE, *"Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security",* 2015.
26) U.S. Department of State, *"U.S. Support for Connectivity and Cybersecurity in Ukraine",* 2022.
27) Van Puyvelde D., Brantly A.F., *Cybersecurity: politics, governance and conflict in cyberspace",* in *Polity Press,* 2019.

SITOGRAFIA

1) https://www.darpa.mil; sulle prospettive future dell'Agenzia cfr: D. Theresa, *"Liberty Lifter: How Cold War tech inspired DARPA's next-gen transport"* in https://interestingengineering.com/military/liberty-lifter-darpa-transport
2) *"The birth of the Web*", in *Cern Resources*, https://home.cern/science/computing/birth-wehttps://submarine-cable-map-2024.telegeography.com/
3) https://datareportal.com/reports/digital-2024-deep-dive-the-state-of-internet-adoption
4) https://www.varutra.com/the-hidden-internet-exploring-the-secrets-of-the-dark-web/
5) https://submarine-cable-map-2024.telegeography.com/
6) Dati del 2023, disponibili su: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023
7) https://foreignpolicy.com/author/john-arquilla/, Cfr: J. Arquilla, *Bitskrieg*: *The New Challenge of Cyberwarfare, Polity Pr Editor,* 2021.
8) White House, *"National Cybersecurity Strategy"*, https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023, 2023.
9) Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note / by the Secretary-General, https://digitallibrary.un.org/record/799853?v=pdf ; https://www.ispionline.it/it/pubblicazione/dallonu-al-g7-i-primi-passi-della-comunita-internazionale-17212
10) National position of the United States of America (2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021).
11) Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021; UNODA, Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security;
12) https://digitallibrary.un.org/record/3934214?v=pdf
13) https://www.ohchr.org/en/hr-bodies/hrc/open-ended-intergovernmental-working-groups
14) https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape
15) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
16) https://www.gazzettaufficiale.it/eli/id/2025/05/05/25A02717/sg
17) https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

18) https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg
19) https://digitallibrary.un.org/record/799853?v=pdf