ALESSANDRO
PISCHEDDA

TTS
CENTRO STUDI SVILUPPO
RELAZIONI PER LA SICUREZZA

LA LEGITTIMA DIFESA NELLA CYBER WARFARE: PROFILI GIURIDICI INTERNAZIONALISTICI

Alessandro Pischedda autore

La legittima difesa nella cyber warfare:
profili giuridici internazionalistici

ISBN: **9791281687004**

Realizzato e pubblicato in collaborazione con l'autore da

Centro Studi Sviluppo Relazioni per la Sicurezza – TTS

Università degli studi di Roma UnitelmaSapienza

www.ttsecurity.it

centrostuditts@gmail.com

Instagram: Tts Centrostuditts
Facebook: TTS Centro Studi Sviluppo Relazioni per la Sicurezza
Linkedin: TTS thinktanksecurity
YouTube: Centrostudi TTS

Alessandro Pischedda

La legittima difesa nella cyber warfare:
profili giuridici internazionalistici

Indice

Introduzione

Il XXI secolo viene sociologicamente identificato come l'età della "information society" [1], una società post industriale frutto di grandi trasformazioni paradigmatiche. Tre grandi periodi, negli ultimi 250 anni, hanno modificato radicalmente le nostre abitudini: Il periodo tra il 1760 e il 1830, che ha visto lo sviluppo del trasporto a vapore e della ferrovia, il periodo tra il 1875 e il 1930 caratterizzato dall'elettricità, dal telefono e dallo sviluppo dei motori a combustione ed il periodo coincidente con l'invenzione, nel 1958, del circuito integrato a cura dell'ingegnere americano e premio nobel Jack Kilby, componente che segnò la nascita della cosiddetta microelettronica caratterizzata da una significativa riduzione del costo al dettaglio dei calcolatori elettronici ed una distribuzione massiva degli stessi.

Quello che ne scaturì fu però lo studio di un sistema di comunicazione rivoluzionario che consentisse un'interconnessione diffusa[2], progetto successivamente sviluppato a livello militare dall' Information Processing Techniques Office (IPTO) all'interno dell'Advanced Research and Development Agency (ARPA) americano.

L'inedita possibilità di scambio informativo a livello globale ed in tempo reale evidenziò, in contropartita, la necessità di regolamentare i rapporti tra gli attori coinvolti, in particolar modo a livello internazionale.

---

[1] SMITH B., The Third Industrial Revolution: Policymaking for the Internet, in *Science and Technology Law Review*, vol. *3,* 2019, disponibile su https://doi.org/10.7916/stlr.v3i0.3621

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

In principio infatti, non essendoci ancora riferimenti giuridici definiti in materia, vigeva una forma di coordinamento basato su prassi tecniche attivate di volta in volta in virtù delle esigenze comunicative del caso, consuetudini che, a seguito dell'improvvisa espansione della rete, entrarono inevitabilmente in crisi[3].

Il risultato fu che la fantascienza immaginata alla fine del secolo precedente divenne in poco tempo realtà.

Oggi, nei teatri internazionali di crisi, operazioni offensive vengono quotidianamente perpetrate su palcoscenici asimmetrici dove risulta ormai difficile individuare le tradizionali distinzioni tra mondo militare e civile, tra state e non-state actors.

Un'evoluzione così rapida non ha consentito e non consente in buona sostanza la puntuale applicazione del diritto internazionale esistente soprattutto in un'era nella quale il comportamento di attaccanti e attaccati si è discostato da quanto tradizionalmente previsto da trattati e dottrina.

Ecco, dunque, che la Comunità internazionale si trova sempre più spesso a valutare se siano ancora attuali ed adattabili le storiche previsioni dei trattati internazionali e cosa sia da considerare legittimo parlando di difesa e spazio cibernetico.

Karl Von Clausewitz, generale prussiano, scriveva che "*la difesa non esiste che contro l'attacco e ciò presupponendolo necessariamente"*[4]*.* Ecco, allora, che un'analisi sulla difesa nel cyber spazio impone il comprendere tre aspetti fondamentali: Cosa sia effettivamente il dominio cibernetico, quale sia l' attacco virtuale da prendere in considerazione per attivare una legittima

[3] SARTOR G., La rivoluzione informatica e la globalizzazione, in Diritto, politica e realtà sociale nell'epoca della globalizzazione – Atti del XXII Congresso della Società Italiana di filosofia giuridica e politica, Macerata, 2002, p. 161, disponibile su https://eum.unimc.it/it/index.php?controller=attachment&id_attachment=789

[4] CLAUSEWITZ K. von, Della guerra (Vom Kriege prima ed. 1832), trad. it, Milano, 1995, Libro sesto, § VII, p. 473.

difesa e, in caso, quali siano gli strumenti internazionalistici a disposizione per rispondere alla minaccia. Da questi quesiti discendono questioni non meno rilevanti e spesso ancora oggi irrisolte quali l'equiparazione di tali attacchi agli attacchi cinetici, la responsabilità internazionale, la proporzionalità nella legittima difesa e la possibilità di risposta cinetica a minacce che per loro natura non lo sono.

Trovare una strada giuridica condivisa è oltremodo complesso. Non possiamo infatti non considerare che il diritto in ambito bellico vive sulla tradizionale dicotomia tra ius ad bellum e ius in bello e in questa rigidità terminologica la Comunità internazionale, in uno scenario mutevole quanto inedito, fatica ad applicare se non addirittura a tentare di implementare la "via del diritto".

Per comprendere se sia possibile una convivenza tra convenzionale e non convenzionale è opportuno in primis conoscere i fondamenti del diritto internazionale in materia e a tal proposito l'intento del primo capitolo sarà fissare innanzitutto i due concetti chiave che rappresentano il corpus imprescindibile in materia: quello di "uso della forza" e quello di "legittima difesa" procedendo anche attraverso un excursus storico con particolare attenzione alla legittima difesa collettiva.

Con il secondo capitolo verrà introdotto il concetto di cyberspazio con l'intenzione di descriverne le peculiarità in modo da poter, con il terzo capitolo, far incontrare le due macro aree e analizzare le criticità occorrenti nel momento in cui riferimenti classici vengono inseriti in contesti inediti.

Capitolo 1 - Uso della forza e legittima difesa

1. L'uso della forza prima del 1945

Fino a quasi tutto il 1800 l'unico mezzo di risoluzione delle controversie tra Stati era il ricorso autogestito alla forza armata. Al fine di limitare la discrezionalità nell'uso della forza le Convenzioni dell'Aja del 1889[5] e del 1907[6] ebbero come intento quello di far porre in essere gli sforzi necessari alla risoluzione pacifica delle controversie[7].

Nel 1920 l'entrata in vigore del Patto della Società delle Nazioni[8], sancì addirittura espressamente il dovere di ricorrere ad un regolamento arbitrale presso la Corte permanente di giustizia internazionale o presso il Consiglio della società delle nazioni[9].

Che fossimo però ancora ai primordi di una ricerca di regolamentazione lo dimostra il fatto che tale patto non esprimesse un ripudio assoluto della guerra facendo comunque sorgere il divieto di ricorso alla stessa solo in caso di accettazione delle pronunce di tali organismi[10].

La previsione sanzionatoria specificatamente riguardante la guerra lasciava però libero spazio ad altre forme di uso della forza armata come la rappresaglia[11], non intesa come azione di autotutela ma ancora come azione punitiva.

---

[5] II Convenzione internazionale dell'Aja concernente le leggi e gli usi della guerra terrestre, l'Aja, 1899 disponibile su https://www.studiperlapace.it/view_news_html?news_id=20041031201007

[6] Convenzione concernente le leggi e gli usi della guerra per terra, l' Aja, 1907, disponibile su https://www.studiperlapace.it/view_news_html?news_id=20041031202458

[7] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, pp. 23-24.

[8] Patto della Società delle nazioni, Parigi, 1919 disponibile su https://www.studiperlapace.it/documentazione/socnazioni.html

[9] *Ibidem*, p. 436.

[10] *Ibidem*

[11] *Ibidem*, p. 24.

Il Patto Kellogg-Briand[12], dai nomi del Ministro degli Esteri francese Briand e del Segretario di Stato americano Kellog, anche conosciuto come Patto di Parigi, volle rafforzare il principio di non utilizzo dello scenario bellico proponendosi l'obiettivo di eliminare del tutto la guerra come strumento di politica internazionale e invocando ulteriormente il dovere di ricorrere a mezzi pacifici di risoluzione delle controversie.

In tale occasione desiderio francese fu quello della stipulazione di un trattato bilaterale mentre, al contrario, la visione della controparte americana, approfittando dell'occasione, si esplicitò nel tentare di coinvolgere anche Germania, Italia, Giappone e Gran Bretagna ad un tavolo di trattative.

Se da parte francese venne presentata una proposta di testo molto articolata, da parte americana la previsione fu molto più snella e divenne, con qualche modifica, il testo finale del successivo trattato.

Sicuramente il patto ratificato rappresentò un cambio storico di atteggiamento nei rapporti internazionali. Per la prima volta, infatti, gli Stati, almeno nelle intenzioni, rinunciavano a quella totale autodeterminazione per diritto naturale a cui erano stati storicamente abituati. Il testo finale, come detto, sposò la linea sintetica americana arrivando a prevedere unicamente due articoli principali più il terzo di impegno alla ratifica[13]:

---

[12] Patto di Parigi di rinuncia alla Guerra, Parigi, 1928, firmato nella sede del Ministero degli Esteri francesi il 27 agosto 1928 ed entrato in vigore il 24 luglio 1929, disponibile su https://www.studiperlapace.it/view_news_html?news_id=briandkellog

[13] *Ibidem,* art. 1: "Le alte parti contraenti dichiarano solennemente in nome dei loro popoli rispettivi di condannare il ricorso alla guerra per la risoluzione delle divergenze internazionali e di rinunziare a usarne come strumento di politica nazionale nelle loro relazioni reciproche", art. 2: "Le alte parti contraenti riconoscono che il regolamento o la risoluzione di tutte le divergenze o conflitti di qualunque natura o di qualunque origine possano essere, che avessero a nascere tra di loro, non dovrà mai essere cercato se non con mezzi pacifici", art. 3: "Il presente trattato sarà ratificato dalle alte parti contraenti designate

Da una analisi del testo appare chiara ancora una volta la carenza assoluta di componenti sanzionatorie in caso di violazione degli accordi. L'unico punto in tal senso fu la parte in cui venne affermato che: "*tutti i Paesi firmatari che cercheranno di sviluppare gli interessi nazionali, facendo ricorso alla guerra, saranno privati dei benefici del presente trattato*" [14].

Pur rappresentando una evoluzione del Covenant della Società delle Nazioni e ricevendo grande adesione[15], il Patto di Parigi non ebbe mai effettiva applicazione in considerazione dei vuoti ancora presenti su alcuni punti chiave e del timore suscitato circa la possibile perdita di immunità e protezione in caso di attacco.

Si poneva inoltre il problema della portata del trattato, essendo, come da art. 2 dello stesso, un accordo valevole unicamente tra i firmatari. In aggiunta a questo non si faceva ancora cenno esplicito alla legittima difesa, concetto che, come da parole dello stesso Segretario Kellog durante un intervento all'American Society of International Law del 1928, non era necessario esplicitare essendo a suo avviso da considerare implicito in ogni trattato. Egli dichiarò infatti, che: "*there is nothing in the American draft of an anti-war treaty which restricts or impairs in any way the right of self-defence. That right is inherent in every sovereign state and it is implicit in every treaty. Every nation is free at all times and regardless of treaty provisions to defend its territory from attack or invasion and it alone is*

---

nel preambolo, conformemente alle esigenze delle loro costituzioni rispettive, e comincerà ad avere effetto non appena tutti gli strumentini ratificazione saranno stati depositati a Washington"

[14] DINSTEIN Y., War, Aggression and self defense, Cambridge, 1994, pagg. 81-82

[15] Il patto di Parigi nel 1939 venne ratificato dal 63 stati tra cui oltre Stati Uniti e Francia, Australia, Canada India, Italia, Unione del Sudafrica, Giappone.

competent to decide whether circumstances require recourse to war in self-defence"[16].

Infine, come nel caso del patto della Società delle Nazioni, l'accordo era ancora troppo specificatamente riferito alla guerra lasciando un pericoloso spazio interpretativo al concetto di uso della forza armata.

I principi del Kellogg-Briand furono ripresi anche nel secondo dopoguerra in occasione del patto di Londra del 1945[17], istituente il Tribunale di Norimberga, in cui venne tra l'altro considerata la c.d. guerra di aggressione come crimine contro la pace[18] passibile di responsabilità penale per chi l'avesse decisa e attuata.

Saranno le Nazioni Unite, con la Carta del 24 ottobre 1945[19] a colmare le pericolose lacune dei precedenti patti e andando ad allargare le maglie interpretative del concetto di uso della forza armata. Nello specifico il paragrafo 4 dell'articolo 2 della Carta sancirà, in maniera volutamente generica[20], l'obbligo di astenersi dalla minaccia o dall'uso della forza per colpire l'indipendenza politica o l'integrità territoriale di un qualsiasi altro Stato[21].

---

[16] LAMBERTI ZANARDI P., La legittima difesa nel diritto internazionale, Milano, 1972, pagg. 83-84

[17] Patto di Londra e statuto del Tribunale internazionale militare di Norimberga, Londra, 1945 disponibile su https://unipd-centrodirittiumani.it/it/strumenti_internazionali/Patto-di-Londra-e-Statuto-del-Tribunale-internazionale-militare-di-Norimberga-1945/170

[18] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, pp. 24-25.

[19] ONU, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, 1945 disponibile su https://unric.org/it/lo-statuto-delle-nazioni-unite/.

[20] a tal proposito v. VIGLIONE S., La nozione di minaccia e il riferimento ai rapporti tra Stati ex art. 2 , § 4 della Carta ONU, in ius in itinere, 2018, disponibile su https://www.iusinitinere.it/la-nozione-minaccia-riferimento-ai-rapporti-stati-ex-art-2-par-4-della-carta-onu-7758

[21] art. 2 , § 4 Carta della Nazioni Unite: "I Membri devono astenersi nelle loro relazioni internazionali dalla minaccia o dall'uso della forza, sia contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato, sia in qualunque altra maniera incompatibile con i fini delle Nazioni Unite."

2. La carta ONU ed il divieto dell'uso della forza

L'entrata in vigore della Carta, o Statuto, delle Nazioni Unite il 24 ottobre 1945, rappresentò la svolta definitiva verso il divieto di ricorso alla guerra quale strumento di risoluzione dei conflitti.

La Carta, definita a San Francisco al termine della Conferenza delle Nazioni Unite sull'Organizzazione Internazionale, fu il prodotto dell'evoluzione giuridica e politica dei precedenti patti e volle definitivamente, almeno nelle intenzioni, andare a colmare quei punti lasciati, spesso consapevolmente, aperti.

Il fine della Carta venne dichiarato nell'art. 1 e identificato nella ricerca del mantenimento della pace e della sicurezza internazionale in particolar modo attraverso la restrizione del diritto all'uso della forza, concetto formalmente specificato al noto paragrafo 4 del secondo articolo[22].

È significativo evidenziare come il concetto di divieto di uso della forza non risieda unicamente nel citato paragrafo ma sia andato nel tempo oltre il diritto pattizio addivenendo norma consuetudinaria universalmente considerata come ius cogens, dunque assolutamente inderogabile, come sancito dalla pronuncia della Corte Internazionale di Giustizia nel caso Nicaragua c. Stati Uniti del 1986[23].

La consuetudine, probabilmente più che l'accordo, ha visto però delle deroghe spesso di dubbia legittimità al divieto di uso della forza, come il caso dell'intervento umanitario o la c.d. responsabilità di proteggere, teorie meglio analizzate nei paragrafi

[22] v. COT J. P. - PELLET A., La Charte des Nationes Unites, Parigi-Bruxelles, 1995.

[23] Corte internazionale di giustizia, case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), sentenza del 27 giugno 1986, ICJ Reports, 1986, P.100

successivi[24], finalizzate spesso ad una legittimazione, a tratti forzata, di specifici interventi.

Dubbi sorsero inoltre circa la possibilità di estendere il concetto di uso della forza alla coercizione economica come richiesto dal Brasile durante la fase dei lavoratori preparatori della conferenza di San Francisco, proposta comunque rigettata e, in tal senso, chiarita dalla posizione dell'Assemblea Generale ONU nella dichiarazione sulle relazioni amichevoli del 1970 nonché nella risoluzione sulla definizione di aggressione nelle quali la coercizione economica non venne ricondotta ad aggressione[25].

Ulteriore punto non definitivamente chiarito fu quello del concetto di minaccia ex. art. 2 della Carta ONU. La Corte internazionale di giustizia (CIG), a tal proposito, si è vista chiamare in causa e, nel parere del 1996 riguardante la legittimità dell'uso e della minaccia di uso di armi nucleari[26], ha affermato che alla minaccia va collegato comunque l'effettivo uso della forza[27] e che nel caso sia considerato lecito, lecita sarà anche la minaccia andando ad impattare su istituti quali, ad esempio, la legittima difesa stessa[28].

Altro caso collegato all'uso della forza fu quello albanese in merito alla presunta violazione della sovranità nazionale causata dal passaggio di navi militari britanniche nelle proprie acque territoriali. Nel caso di specie la CIG escluse ci fossero state violazioni del diritto internazionale considerando la navigazione in

---

[24] *Infra,* parr. 4.2 e 4.3

[25] Assemblea Generale delle Nazioni Unite, ris. 3314-XXIX quando il concetto di aggressione nel 1974 venne definito come "the most serious and dangerous form of the illegal use of force".

[26] Corte internazionale di giustizia, Legality of the Threat or Use of Nuclear Weapons, parere consultivo del 8 luglio 1996, I.J.C. Reports 1996

[27] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, p. 30

[28] Corte internazionale di giustizia, Legality of the Threat or Use of Nuclear Weapons, parere consultivo del 8 luglio 1996, I.J.C. Reports 1996, p. 226

esame quale legittimo esercizio di passaggio inoffensivo in uno stretto internazionale e dunque non una minaccia all'uso della forza[29].

Va inoltre aggiunto che il divieto di minaccia o di uso della forza era riferito ai rapporti tra gli Stati membri e questo comportò non pochi dubbi circa l'applicabilità dello stesso in eventi alternativi quali, ad esempio, guerre civili o crisi interne.

Ad esempio l'interpretazione letterale del trattato sembrerebbe non far rientrare un'insurrezione nel divieto. Nel caso in cui però tale evento sia, nonostante tutto, reputato pericoloso per il mantenimento della pace a livello internazionale viene comunque prevista la possibilità da parte del Consiglio di Sicurezza di intervenire, salvo veti dei membri permanenti, ai sensi del Capitolo VII della Carta[30]. È certo una valutazione, quella del livello di interesse internazionale, fortemente dipendente dalle valutazioni caso per caso del Consiglio di sicurezza.

Casi emblematici in tal senso furono da una parte gli scontri tra la minoranza Rohinjya in Myanmar e l'esercito nazionale fatti rientrare in mero affare interno a seguito di veto da parte di Russia e Cina[31] e dall'altra, di esito opposto, il caso del muro costruito in territorio palestinese giudicato dalla Corte di Giustizia internazionale rientrante nell'interesse internazionale e dunque in quanto previsto dalla Carta[32].

---

[29] Corte internazionale di giustizia, The Corfù channel case, sentenza del 9 aprile 1949, I.C.J. Reports, 1949, p. 30.
[30] Capitolo VII Carta ONU: "Azione rispetto alle minacce alla pace, alle violazioni alla pace ed agli atti di aggressione".
[31] China and Russia veto US/UK-backed Security Council draft resolution on Myanmar, in UN News, 2007 disponibile su https://news.un.org/en/story/2007/01/205732.
[32] Corte internazionale di giustizia, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, parere consultivo del 9 luglio 2004, I.C.J. Reports 2004, § 246

Come già detto, nel divieto all'uso della forza convivono un'anima pattizia ed una consuetudinaria. Ad ogni modo esistono eccezioni a tale previsione, alcune universalmente condivise come per l'autorizzazione da parte del Consiglio di sicurezza, altre di dubbia ammissibilità, una su tutte il c.d. caso di intervento umanitario meglio analizzato successivamente[33].

3. Ius ad bellum e Ius in bello

Parlare dell'art. 2 della Carta ONU implica citare una fondamentale distinzione, quella tra ius ad bellum e ius in bello. Per *ius ad bellum* ci si riferisce ai presupposti giuridici legittimanti il diritto degli Stati di ricorrere alla guerra in tempo di pace. Per i*us in bello* ci si riferisce invece al diritto dei conflitti armati, dunque a conflitto iniziato, in uno scenario di avvenuta violazione della pace. Trattasi di un bivio non derogabile, *tertium non datur.*

Va ricordato, come già scritto, che prima della stipulazione dei trattati riguardanti la rinuncia alla guerra, gli Stati erano liberi di gestire le proprie controversie anche con l'uso della forza armata senza che nessun organo internazionale potesse intervenire. La forza armata era fondamentalmente la più importante forma di manifestazione della propria sovranità[34].

La guerra, dunque, pur trattandosi di una extrema ratio, non solo non era ripudiata ma veniva supportata giuridicamente, in caso d'uso, da un diritto naturale, vero e proprio retaggio culturale dei popoli.

È con l'inizio del XX secolo però, con la stipulazione delle prime convenzioni limitanti la soggettività, che si ebbe un effettivo cambio nella percezione del ricorso alla forza. Nel primo dopo guerra, la Conferenza di pace di Parigi ed il Trattato di Versailles

[33] v. *infra*, cap. 1, § 4.2
[34] RONZITTI N., *Diritto Internazionale*, VI[a] ed., Torino, 2019, pag.22.

del 1919[35] vollero una volta per tutte individuare punti e istituzioni interessate in tema di sicurezza internazionale.

Precedentemente, nell'autunno del 1914, Thomas Woodrow Wilson, Presidente degli Stati Uniti da un biennio, propose un patto fra tutti gli Stati del continente americano. I principi di tale patto vennero meglio esplicati prima in un discorso al Senato nel 1917 e poi in 14 punti scritti nel 1918.

L'idea del Presidente era quella di formare un'associazione generale di nazioni al fine di avere garanzie reciproche in tema di indipendenza politica e territoriale. Tale idea diede origine al *Covenant* o statuto della Società delle Nazioni adottato durante la Conferenza di Parigi ed integrato nel Trattato di Versailles. Fu la prima vera organizzazione internazionale a carattere politico, utile a quel graduale incremento di consenso sul divieto di ricorso alla guerra come risoluzione delle controversie internazionali.

Sarà però con la già citata Carta delle Nazioni Unite che tale divieto assurgerà ad un nuovo livello.

Va anche considerato che a seguito del divieto di cui all'art. 2, § 4, lo ius ad bellum è risultato invocabile unicamente in risposta ad un attacco, attuato in violazione della previsione della Carta e già sferrato da altri[36]. Si potrebbe in altri termini affermare che lo stesso ius ad bellum si sia, in quel momento, trasformato nel diritto alla legittima difesa individuale, diritto movibile unicamente in risposta ad un attacco armato come disciplinato in particolar modo nell'art. 51.

---

[35] Trattato di pace di Versailles tra le potenze alleate e associate, Società delle Nazioni, Versailles, 1919 adottato il 28 giugno 1919

[36] MCCOUBREY H. – WHITE N.D., International law and armed conflict, Dartmouth, 1992, pagg. 8-10

4. Le eccezioni al divieto di uso della forza

Il granitico divieto ex. art. 2, § 4, in realtà tale non sarebbe, essendo previste alcune deroghe allo stesso. Eccezioni condivise nei casi di autorizzazione del Consiglio di sicurezza e della legittima difesa, altre frutto di controverse interpretazioni quali l'uso della forza giustificata dall'intervento umanitario o la c.d. dottrina del "responsibility to protect".

4.1 L'autorizzazione del Consiglio di sicurezza

Ai sensi dell'articolo 24 della Carta delle Nazioni Unite il Consiglio di Sicurezza ha il compito di mantenere la pace e la sicurezza internazionale attraverso le azioni indicate nel capitolo VI, per soluzione delle controversie non implicanti l'uso della forza, e nel capitolo VII relativamente ad eventuali azioni attuabili in caso di violazione della pace o minaccia di essa[37].

Tali misure possono essere inoltre provvisorie come nel caso delle mere raccomandazioni non vincolanti finalizzate al contenimento delle criticità riguardanti ad esempio il ritiro delle truppe, il cessate il fuoco, o in generale tregue e armistizi[38], forme tuttavia non elencate in previsioni scritte ma discendenti da interpretazioni della prassi.

Diverso invece il caso dell'art. 41, in cui vengono espressamente elencate le misure non implicanti l'uso della forza adottabili a supporto delle decisioni già prese[39].

---

[37] CONFORTI B. – FOCARELLI C., *Le Nazioni Unite,* 12. ed., Milano, 2020*,* pp. 214 e ss.

[38] CONFORTI B. – FOCARELLI C., *Le Nazioni Unite,* 12. ed., Milano, 2020, p. 273.

[39] art. 41 Carta della Nazioni Unite: "Il Consiglio di Sicurezza può decidere quali misure, non implicanti l'impiego della forza armata, debbano essere adottate per dare effetto alle sue decisioni, e può invitare i Membri delle Nazioni Unite ad applicare tali misure. Queste possono comprendere un'interruzione totale o parziale delle relazioni economiche e delle comunicazioni ferroviarie, marittime,

La carta prosegue con l'articolo 42, circa le misure implicanti l'uso della forza, e l'art 43 concernente il "sistema di sicurezza ONU" ovvero l'utilizzo di contingenti militari messi a disposizione dai paesi a seguito di specifici accordi e sottoposti ad un comando internazionale a cura del Consiglio[40].

Va detto che il Sistema di sicurezza ONU non ha mai, di fatto, visto la luce se non attraverso localizzate operazioni di "peace keeping" o "peace enforcement", terminologie utili a sancire il non uso della forza che non sia per legittima difesa.

Vennero invece occasionalmente autorizzati gli Stati membri ad operare in proprio con le rispettive Forze armate o nel contesto di organizzazioni regionali. Tali autorizzazioni vennero erogate sulla base di un potere almeno apparentemente non mutuato da alcun articolo specifico se non indirettamente dall'articolo 53, co. 1, contenente la possibilità di autorizzare l'uso della forza appunto attraverso organizzazioni regionali[41].

È questo un passaggio controverso che sembrerebbe lasciare spazio a deroghe circa l' uso della forza da parte di singoli Stati, cosa assolutamente non voluta dalla conferenza di San Francisco che anzi mirò a "spersonalizzare" questo tipo di interventi

---

aeree, postali, telegrafiche, radio ed altre, e la rottura delle relazioni diplomatiche."

[40] CONFORTI B. – FOCARELLI C., *Le Nazioni Unite,* 12. ed., Milano, 2020, p. 322.

[41] art. 53, co. 1 della Carta della Nazioni Unite: "Il Consiglio di Sicurezza utilizza, se del caso, gli accordi o le organizzazioni regionali per azioni coercitive sotto la sua direzione. Tuttavia, nessuna azione coercitiva potrà venire intrapresa in base ad accordi regionali o da parte di organizzazioni regionali senza l'autorizzazione del Consiglio di Sicurezza, eccezion fatta per le misure contro uno Stato nemico, ai sensi della definizione data dal paragrafo 2 di questo articolo, quali sono previste dall'articolo 107 o da accordi regionali diretti contro un rinnovarsi del la politica aggressiva da parte di un tale Stato, fino al momento in cui l'organizzazione potrà, su richiesta del Governo interessato, essere investita del compito di prevenire ulteriori aggressioni da parte del detto Stato".

prevedendo la possibilità di utilizzo delle Forze armate unicamente sotto la direzione ONU e non dei singoli governi[42].

4.2 L'uso della forza per intervento umanitario

In caso di insuccesso delle misure preventive ex. art. 41, l'utilizzo della forza sembrerebbe poter essere legittimato da un intervento di natura umanitaria a seguito di grave violazione dei diritti umani da parte di uno Stato nei confronti dei suoi cittadini[43]. Questa possibilità, che non vede specifica previsione né all'interno della Carta del 1945 né nella consuetudine, andrebbe attuata, secondo alcuni Paesi, come extrema ratio in caso di palesi e perpetrate gross violations su larga scala. Paradossalmente non essendoci, come detto, previsione né pattizia né consuetudinaria, ad oggi un uso della forza armata a difesa di una popolazione è a tutti gli effetti un illecito internazionale al quale lo Stato incriminato, potrebbe lecitamente eccepire la non osservanza del principio di non ingerenza.

In conclusione, la tesi dell'intervento umanitario non può ad oggi essere considerata eccezione al divieto ex. art. 2, § 4.

4.3 La "responsibility to protect"

La dottrina della Responsibility to protect o responsabilità di proteggere (R2P), richiama, almeno apparentemente, quella dell'intervento umanitario pur prevedendo un iter più strutturato. Tale teoria ha come base tre principi: la responsabilità di uno Stato, l'obbligo di aiuto da parte della Comunità internazionale e la responsabilità della stessa qualora lo Stato fallisca.

---

[42] CONFORTI B. – FOCARELLI C., *Le Nazioni Unite,* 12. ed., Milano, 2020, p. 351.
[43] PUSTORINO P., Lezioni di tutela internazionale dei diritti umani, 2. ed., Bari, 2020, p. 257 e seg.

Durante il World summit ONU del 2005 venne valutata la possibilità di poter intervenire in difesa delle popolazioni in caso di gross violations. Il concetto di R2P altro non fu che l'evoluzione di quel filone cominciato già nel 1948 e 1949 con le convenzioni per la prevenzione e repressione del delitto di genocidio[44] e con le successive convenzioni di Ginevra e relativi protocolli aggiuntivi[45].

Con il sopraggiungere nel tempo di numerosi conflitti interni, in particolar modo con le questioni del genocidio ruandese e dei Balcani negli anni 90, la responsabilità di proteggere vide una ufficializzazione nel 2001 all'interno del secondo capitolo del report della Commissione internazionale sull'intervento e la sovranità dello stato. Tale capitolo, intitolato "Un nuovo approccio: la responsabilità di proteggere", sottolineava che l'interesse generale non doveva essere proteggere le grandi potenze ma la gente comune dall'incapacità, o la non volontà, di un qualsiasi Stato di voler proteggere la propria popolazione. Vennero in tale occasione citate le tragedie della Somalia, del

[44] Assemblea generale, Convention on the Prevention and Punishment of the Crime of Genocide, adottata il 9 dicembre 1948 con risoluzione 260 (III), entrata in vigore il 12 gennaio 1951 disponibile su https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-prevention-and-punishment-crime-genocide

[45] Con il termine convenzioni di Ginevra si intende un insieme normativo specifico del diritto umanitario approntato dall'ONU a Ginevra, composto da quattro convenzioni e tre protocolli aggiuntivi. Le convenzioni sono state adottate a Ginevra il 12 agosto 1949 e sono la I Convenzione per il miglioramento delle condizioni dei feriti e dei malati delle Forze armate in campagna, la II Convenzione per il miglioramento delle condizioni dei feriti, dei malati e dei naufraghi delle Forze armate sul mare, la III Convenzione sul trattamento dei prigionieri di guerra e la IV Convenzione sulla protezione delle persone civili in tempo di guerra. Nel 1977 vennero integrate con due protocolli aggiuntivi, il I protocollo aggiuntivo relativo alla protezione delle vittime dei conflitti armati internazionali ed il II protocollo aggiuntivo relativo alla protezione delle vittime dei conflitti armati non internazionali entrambi adottati l' 8 giugno 1977. Infine l'8 dicembre 2005, al fine di dotare le organizzazioni internazionali umanitarie di un simbolo non collegato ad alcuna confessione religiosa, è stato adottato il III protocollo aggiuntivo relativo all'adozione di un emblema distintivo aggiuntivo. Disponibili su https://www.eda.admin.ch/eda/it/dfae/politica-estera/diritto-internazionale-pubblico/diritto-internazionale-umanitario/convenzioni-ginevra.html

Ruanda, di Srebrenica e del Kosovo al fine di stimolare una discussione su quello che sarebbe stato il palcoscenico mondiale del ventunesimo secolo.

Nello stesso periodo, precisamente nel 2001[46], l'Unione Africana, nel suo atto costitutivo, sanciva il diritto di intervento degli Stati membri, su decisione dell'Assemblea, in caso di crimini di guerra o violazione dei diritti umani.

È il primo esempio di formalizzazione del R2P anche se sarà durante il successivo World Summit del 2005 che, a conclusione dei lavori dell'Assemblea Generale delle Nazioni Unite, verrà adottata una risoluzione contenente un paragrafo rubricato "*Responsibility to protect populations from genocide, war crimes, ethnic cleaning and crimes against humanity*"[47].

Gli articoli 138 e 139 della risoluzione decretarono tre principi chiave: 1) lo Stato ha la responsabilità di proteggere la propria popolazione da qualsiasi violazione di diritti umani considerati parte dello ius cogens, come genocidio, crimini di guerra e crimini contro l'umanità. 2) lo Stato che voglia applicare tale protezione deve essere supportato dalla comunità internazionale che ha a sua volta la responsabilità di assisterlo. 3) Ex art. 139, la comunità internazionale stessa ha la responsabilità di usare ogni mezzo diplomatico, umanitario e pacifico per proteggere le popolazioni in caso di fallimento dello Stato nel suo primo obbligo.

La risoluzione non fu esente da critiche, alcune correnti di pensiero infatti la interpretarono come una legittimazione all'ingerenza negli affari interni degli altri Stati.

---

[46] L'11 luglio 2000 in Togo viene firmato l'atto costitutivo dell'Unione africana che sostituì la precedente Organizzazione dell'unità africana. Disponibile su https://au.int/sites/default/files/pages/34873-file-constitutiveact_en.pdf

[47] Assemblea generale, risoluzione concernente il 2005 world summit outcome, UN Doc. A/RES/60/251 del 15 marzo 2006, disponibile su https://www.globalr2p.org/resources/2005-world-summit-outcome-a-60-l-1/

L'evoluzione cronologica ha visto nel 2006 una conferma dei principi indicati nel 2001[48] nonché l'autorizzazione al dispiegamento di truppe ONU per un'operazione di peacekeeping in Darfur[49].

Successivamente, nel 2009, il segretario generale ONU Ban Ki-moon, pubblicò il report "*implementing the responsibility to protect*" con il quale definì le linee guida da seguire ed i paesi interessati sulla base dei tre principi. Il report ebbe come risultato la produzione della prima risoluzione ufficiale in materia e la conseguente sottoscrizione in data 7 ottobre 2009[50].

Partendo dal già citato caso del Darfur, successive applicazioni del principio si sono avute nel 2011 in Libia e Costa d'Avorio con azioni militari che portarono alla destituzione dell'allora Presidente. Seguì il Sudan del Sud e lo Yemen.

Caso interessante fu quello siriano del 2012. Il Consiglio infatti votò per un appoggio al piano della Lega Araba per la risoluzione della crisi ma si scontrò con il veto di due membri permanenti, Cina e Russia[51]. Dopo un ulteriore veto russo-cinese alla risoluzione del 4 febbraio 2012[52], il 26 marzo 2012 il governo siriano accettò una proposta in sei punti avanzata dall'allora

---

[48] Consiglio di sicurezza, risoluzione n. 1647 (2006), adottata il 28 aprile 2006, relativa alle vittime civili nei conflitti armati.

[49] Consiglio di sicurezza, risoluzione n. 1706 (2006), adottata il 31 agosto 2006, relativa ad una missione ONU in Sudan (UNIMIS) per supportare l'implementazione dell'accordo di pace in Darfur. Disponibile su https://digitallibrary.un.org/record/582107

[50] Assemblea generale, UN Doc. A/RES/63/308 del 7 ottobre 2009.

[51] La Federazione Russa ha posto il veto sulla questione siriana 13 volte dal 2011 al 2018, 8 delle quali singolarmente e 5 assieme alla Cina, altro membro permanente del Consiglio di sicurezza ONU. La stessa federazione avvisò inoltre gli altri membri del Consiglio che l'interferenza di Stati terzi nella situazione siriana avrebbe potuto mettere a rischio la sicurezza regionale durante il meeting n. 6520 del 21 aprile 2011disponibile su *https://daccess-ods.un.org/tmp/5891825.55675507.html* e durante il meeting n. 6524 del 26 aprile 2011, disponibile su https://www.securitycouncilreport.org/un-documents/document/syria-s-pv-6524.php.

[52] Consiglio di sicurezza, risoluzione n.77 (2012), adottata del 4 febbraio 2012.

inviato speciale per la Siria Kofi Annan[53] ma il tutto non risultò efficace in quanto il governo siriano non mantenne le promesse iniziali decretando quello che a detta dell'assemblea ONU stessa fu il fallimento del Consiglio di sicurezza[54].

Al contrario il 2013 venne definito, anche in considerazione della questione kenyota, l'anno di completa applicazione di tale principio.

Allo stato attuale le aree di crisi osservate dagli analisti internazionali sono quelle del Sahel centrale, del Congo, del Mozambico, della Nigeria ed altre particolarmente seguite quali il Venezuela ed il conflitto Russo-Ucraino.[55]

5. La legittima difesa

Dalla valutazione sull'uso della forza, discende il secondo e principale argomento del presente lavoro, quello della legittima difesa, istituto centrale da introdurre al fine di meglio comprendere gli elementi di atrito tra il diritto internazionale, tradizionalmente inteso e la cyber warfare.

A supporto ed integrazione di quanto sancito dall'articolo 2 della Carta ONU è necessario ora introdurre una ulteriore possibile eccezione al divieto all'uso della forza, l'articolo 51 concernente la legittima difesa declinata in forma individuale o collettiva.

L'articolo 51 riporta che: "*Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o*

---

[53] Segretario generale, Syrian Government Accepts UN-Arab League Envoy's Six-Point Plan to End Crisis, del 27 marzo 2012, v. https://edition.cnn.com/2012/03/27/world/meast/syria-annan-plan/index.html

[54] Assemblea generale, UN Doc A/RES/66/253 B del 3 agosto 2012 sulla situazione nella Repubblica araba siriana, disponibile su https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_res_66_253_b.pdf.

[55] Global Centre for the responsibility to protect, R2P Monitor, 2023, disponibile su https://www.globalr2p.org/publications/r2p-monitor-issue-65-1-june-2023/,

collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale. Le misure prese da Membri nell'esercizio di questo diritto di autotutela sono immediatamente portate a conoscenza del Consiglio di Sicurezza e non pregiudicano in alcun modo il potere e il compito spettanti, secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quell'azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale".[56]

E' importante comprendere la straordinaria importanza imputata al diritto all'autodifesa, un diritto definito come "naturale", talmente forte da poter derogare, anche se provvisoriamente, uno jus cogens quale quello dell' art. 2, § 4.

Altro punto chiave è il fatto che l'articolo 51 in realtà non voglia rimanere generico ma ben specifichi quale sia il genere di attacco legittimante la deroga ovvero il c.d. attacco "*armato".*

È chiaro che la possibilità di poter non osservare un punto della Carta implichi una attenta valutazione che porti ad escludere offese di livello inferiore ad una determinata soglia.

Esempio calzante può essere un incidente di lieve portata, al confine tra due paesi, che, per quanto degno di attenzione, non arriva ad attivare l'iter legittimante la risposta armata[57].

È infatti necessario essere in presenza di un uso illegale della forza ed anche di particolare gravità, tale da non poter attendere convocazioni e deliberazioni del Consiglio di Sicurezza[58].

---

[56] ONU, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, 1945, art. 51.
[57] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, p. 37.
[58] La giurisprudenza internazionale si è espressa in tal senso in occasione del caso Nicaragua-Stati Uniti e Iran-Stati Uniti andando a tratteggiare una

Oltremodo importante è definire il concetto di "*aggressione".*

A tal proposito l'articolo 39 della Carta ONU[59] ne da una prima definizione: "*Il Consiglio di Sicurezza accerta l'esistenza di una minaccia alla pace, di una violazione della pace, o di un atto di aggressione, e fa raccomandazione o decide quali misure debbano essere prese in conformità agli articoli 41 e 42 per mantenere o ristabilire la pace e la sicurezza internazionale*."

Ad integrazione di ciò, l'articolo 1 della risoluzione 3314 dell'Assemblea Generale delle Nazioni Unite del 1974 in tema di aggressione (*Definition of Aggression*)[60] riporta: "*L'aggressione è l'uso della forza armata da parte di uno Stato contro la sovranità, l'integrità territoriale o l'indipendenza politica di un altro Stato, o in qualsiasi altro modo incompatibile con Carta delle Nazioni Unite, come stabilito in questa definizione*".

La Corte Internazionale di Giustizia ha inoltre fatto riferimento, nei noti casi Nicaragua c. Stati Uniti e Iran c. Stati Uniti, alla gravità definendo l'attacco armato come la più grave forma di uso della forza[61], consentendoci di collegarci a quanto già espresso dall'Assemblea generale, in apertura della citata risoluzione 3314, circa la qualificazione dell'aggressione.

6. L'articolo 51 della Carta ONU ed il diritto naturale di autotutela.

La Carta ONU, se da un lato ha comportato un' evoluzione, almeno sperata, nei rapporti tra gli Stati, ha dall'altro dato un

---

distinzione tra forme più o meno gravi di uso della forza specificando quali possano essere considerate come legittimanti.

[59] ONU, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, 1945, art. 39

[60] Assemblea generale, risoluzione 3314 (XXIX) del 14 dicembre 1974 sulla definizione di aggressione, disponibile su https://daccess-ods.un.org/tmp/1415046.45347595.html.

[61] ICJ, Reports, 1986, p. 101, § 191.

duro colpo all'autonomia decisionale degli stessi. Anche per questo durante gli incontri prodromici alla stesura della Carta, come nel caso dei negoziati di Dumbarton Oaks[62], si è pensato di conservare la possibilità di agire in casi estremi a protezione delle singole integrità.

Non a caso venne detto che la legittima difesa fosse in realtà un cavillo politico per lasciare aperta la possibilità di agire in autonomia e fu argomento per certi versi scomodo e controverso per chi ancora conservava aspirazioni nazionalistiche.

Va aggiunto che per taluni paesi fu invece un problema tutto sommato poco sentito. A tal proposito non deve stupire il fatto che nelle proposte inoltrate alla Conferenza di San Francisco del 1945, il tema della legittima difesa risultasse assolutamente marginale se non addirittura assente.

In ogni caso, al di là della presenza o meno dell'argomento negli ordini del giorno, gli Stati risultarono tutelati grazie al riconoscimento implicito del diritto all'autotutela in caso di aggressione[63], il c.d. "inherent right" alla difesa della propria integrità territoriale o politica.

Questo però a molti paesi non bastò e venne per questo chiesto l'inserimento espresso di tale disposizione nel testo della Carta[64].

7. La clausola sulla legittima difesa.

La necessità di una clausola scritta nasceva da un evento ben preciso: la conferenza di Yalta ed il potere di veto delle cinque

[62] Dal nome della villa in cui si svolse la Conferenza del 1944 presenziata da Stati Uniti, Gran Bretagna e Unione Sovietica in merito alla proposta per la creazione di un'organizzazione internazionale generale, evento che costituì l'impianto per la Carta ONU.
[63] LAMBERTI ZANARDI P., La legittima difesa nel diritto internazionale, Milano, 1972, pag.193
[64] *Ibidem*, pag.194:

potenze vincitrici del secondo conflitto mondiale, i futuri membri permanenti. Questo potere di veto da parte di Stati Uniti, Russia, Cina, Francia ed Inghilterra impensieriva gli altri paesi che temevano l'impossibilità di una tutela in caso di aggressione.

Un'ulteriore questione, non interna alle Nazioni Unite, riguardava i c.d. accordi regionali a carattere difensivo. Tali accordi rappresentavano un comodo sostituto della Carta ONU, prevedendo già una forma di difesa collettiva tra Stati firmatari.

Emblematico fu l'Atto di Chapultepec del 1945 stipulato in America Latina proprio al fine di prevedere l'intervento di Stati terzi, quindi non interessati direttamente, ma chiamati in causa dall'offeso. Si arrivò anche a valutare la possibilità, per le organizzazioni regionali, di eludere l'autorizzazione del Consiglio di sicurezza in caso di ingente pericolo[65].

Indubbiamente tutto ciò rappresentava una potenziale crepa nell'univocità delle Nazioni Unite e a tal proposito i membri permanenti decisero, preservando comunque questi accordi, di conservare l'inderogabilità dell'autorizzazione preventiva del Consiglio di sicurezza consentendo di mantenere la posizione di supremazia dello stesso.

8. Necessità e proporzionalità della legittima difesa.

Come già emerso dai precedenti paragrafi il ricorso alla legittima difesa, sia in forma autonoma che collettiva, è un potente strumento che per poter ricevere la legittimazione internazionale impone il rispetto di specifici requisiti quali necessità, proporzionalità e immediatezza. Tali criteri non

[65] *Ibidem*, pag.198

provengono da una previsione scritta della Carta bensì dalla consuetudine giuridica internazionale[66].

Necessità e proporzionalità furono in passato considerati come intercambiabili tra loro anche se la CIG, nel caso Nicaragua c. Stati Uniti, ritenne che andassero invece considerati separatamente[67].

In aggiunta, nel caso delle Oil Platform, venne sancito dalla Corte che necessità e proporzionalità, in riferimento alla distruzione da parte USA di piattaforme petrolifere[68], potessero essere posti anche quali limiti all'esercizio dell'uso della forza nella legittima difesa.

Nel caso di specie si ritenne il requisito della necessità non sussistente in quanto le piattaforme mancavano di rilevanza militare e che, nella risposta americana, non sussistesse neanche quello della proporzionalità avendo gli Stati Uniti causato oltre la distruzione delle piattaforme, anche la distruzione di navi da guerra iraniane in contropartita all'attacco subito da una loro imbarcazione.

In dottrina, circa necessità e proporzionalità, si sono storicamente succedute visioni alternative.

Venturini sostenne che "*lo Stato che intenda affermare il carattere difensivo della sua azione militare deve condurla sempre e costantemente entro i limiti della necessità e della proporzionalità rispetto all'aggressione subita, indipendentemente*

[66] Viene considerata come una prima citazione di necessità e proporzionalità il caso del 1837 Stati Uniti – Regno Unito, "Caroline"
[67] GREENWOOD C., Self-Defence, in Max Planck Encyclopedia of Public International Law, Oxford Unversity Press, 2011, § 25-26.
[68] *Ibidem*

dalla maggiore o minore entità che entrambe possano assumere"[69] auspicando il non superamento di determinate soglie.

Visione alternativa quella di Grigory Tunkin, giurista russo del 900, il quale asserì che "*as regards the proportionate reaction to a violation of international law, this principle could have been considered operative only with respect to compensation of damage and to reprisals; it did not, however, extend to war*"[70], intendendo che la proporzionalità andasse considerata unicamente nell'ambito del risarcimento del danno subito e delle ritorsioni, non estendendo il concetto alle azioni di guerra.

Nel panorama nazionale, il Quadri affermò che "*se la legittima difesa assume i caratteri della guerra, in tal caso appare impossibile assegnarle un limite del genere indicato*"[71], ad indicare che limitare le capacità di risposta di uno Stato offeso avrebbe significato ridurre l'efficacia della risposta e dunque, secondo questa visione, riconoscendo il diritto dello Stato attaccato ad utilizzare ogni mezzo.

La tendenza in linea generale rimane ad ogni modo quella di preservare la parità delle parti[72] in ossequio delle previsioni internazionali. Una conferma in tal senso risiede nel parere della CIG in tema di liceità sull'adozione delle armi nucleari[73], parere che mai mise in discussione lo ius in bello e il diritto umanitario.

La Corte, infatti, specificò che in caso di legittima difesa, come in generale in caso di conflitto, la protezione di civili e l'evitare

---

[69] VENTURINI G., Necessità e proporzionalità nell'uso della forza militare in diritto internazionale, Milano, 1988, pag. 55
[70] TUNKIN G. I., Theory of International Law, Cambridge, 1974, pag.391
[71] QUADRI R., Diritto Internazionale Pubblico, Napoli, 1968, pag.274
[72] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, pag. 138.
[73] Corte internazionale di giustizia, Legality of the Threat or Use of Nuclear Weapons, parere consultivo del 8 luglio 1996, I.J.C. Reports 1996

dolore inutile agli stessi militari[74], fosse l' interesse prioritario da non dimenticare.

Interessante riportare che a seguito della pronuncia del 1996 emersero nel tempo controverse interpretazioni in merito all'uso delle armi nucleari. Nel caso di specie, infatti, le conclusioni della Corte non furono assolutamente dirimenti. In taluni passaggi sembrava lasciarsi intendere che, in controtendenza a quanto già affermato, la Corte ritenesse che in caso di "*situazioni estreme di legittima difesa*" si potesse derogare al diritto umanitario e dunque consentire l'uso dell'arma atomica, cosa ritenuta un inquietante supporto giurisprudenziale per chi avesse deciso di procedere per la strada nucleare[75].

9. Il parametro temporale ed il concetto di immediatezza.

Il tema dell'immediatezza venne riportato da Roberto Ago, giurista e giudice della Corte Internazionale di Giustizia, durante l'attività giuridica di codificazione in tema di responsabilità internazionale[76]. Agire con immediatezza consiste nel quantificare il tempo a disposizione per rispondere ad un'offesa ai sensi dell'art. 51 della Carta. L'articolo, comunicandoci che il limite massimo entro il quale il diritto possa essere esercitato corrisponde alle deliberazioni del Consiglio di Sicurezza, conferma due punti importanti: la supremazia del Consiglio nella risoluzione

[74] *Ibidem*, § 78: "le droit humanitaire a très tôt banni certaines armes, soit parce qu'elles frappaient de façon indiscriminée les combattants et les populations civiles, soit parce qu'elles causaient aux combattants des souffrances inutiles, c'est-à-dire des souffrances supérieures aux maux inévitable que suppose la réalisation d'objectifs militaires légitimes".

[75] RONZITTI N., La Corte Internazionale di Giustizia e la questione della liceità della minaccia o dell'uso delle armi nucleari, in Rivista di diritto internazionale, 4/1996, p. 880, disponibile su https://www.unife.it/giurisprudenza/giurisprudenza-magistrale-rovigo/studiare/diritto-internazionale/materiale-didattico/RONZITTI_RDI_1996_861-liceita.pdf/at_download/file

[76] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, p. 95

delle controversie internazionali e l'eccezionalità della legittima difesa.

Se da una parte l'articolo 51, come detto, pone il limite massimo dall'altra specifica che la legittima difesa può essere esercitata quando un attacco armato "abbia luogo" andando dunque a definire anche il limite minimo. Ad una interpretazione letterale si potrebbe pensare di escludere la possibilità di reagire ad attacco non concluso.

Questa, ad ogni modo, non sarebbe una conclusione equa in quanto uno Stato notevolmente capace militarmente potrebbe perpetrare costantemente attacchi fino a neutralizzare le possibilità di controffensiva della vittima.

Come ben possiamo imparare dall'articolo 32 della Convenzione di Vienna sul diritto dei trattati del 1969,[77] l'interpretazione letterale di una norma non può condurre a un risultato che è "*manifestamente assurdo o irragionevole*". È dunque pacifico, sia ai sensi del diritto consuetudinario che di quello pattizio, che il diritto alla legittima difesa possa esercitarsi contro un attacco armato imminente in quanto l'eventuale attesa comporterebbe l'incapacità di respingere.[78]

Ecco dunque presentarsi un ulteriore parametro, quello della necessità dell'imminenza. A tal proposito è opportuno citare, a beneficio di una corretta ricostruzione storica, la corrispondenza epistolare tra Stati Uniti e Gran Bretagna in occasione del caso Caroline del 1837 nella quale venne ribadito che la necessità di

[77] Convenzione di Vienna sul diritto dei trattati, Vienna, 1969, articolo 32, lett. b)

[78] v. WILMSHURST E., The Chatham House Principles of International Law on the Use of Force in Self-Defence, in International & Comparative law quarterly, vol. 55, n. 4. Cambridge, 2006, p. 968

legittima difesa dovesse essere "*instant, overwhelming, and leaving no choice of means, and no moment for deliberation"*[79].

Circa i limiti temporali, come spesso accade in campo internazionale, l'interpretazione non risulta univoca lasciando spazio ad una varietà di pareri. Considerato il fattore dell'imminenza dell'attacco, ci si chiede, ad esempio, se superato un determinato tempo la risposta possa essere comunque qualificata come legittima difesa o vada considerata in altra maniera, ad esempio come una rappresaglia.

A tal proposito il Ronzitti ritiene che: "*È ovvio che se uno Stato, dopo aver compiuto un attacco armato, si ritira e rientra nei propri confini, una successiva e tardiva reazione da parte dello Stato leso si configura più come un'azione di rappresaglia, che come esercizio di legittima difesa*"[80].

La rappresaglia[81] andrebbe dunque intesa come l'invito al rispetto di obblighi internazionali violati. Una parte della dottrina ritiene che sia comunque opportuno corretto entrare nel merito del singolo caso valutando di volta in volta. Va da sé infatti che, in astratto, una impreparazione o una diversa capacità bellica possa comportare esiti diversi da Stato a Stato[82] non garantendo dunque la formazione di una consuetudine.

Un caso di studio assolutamente peculiare è quello dell'occupazione. Nello specifico si discute se tale fattispecie sia equiparabile all'aggressione e quale arco temporale vada preso in considerazione per poter esercitare la legittima difesa,

---

[79] Lettera di Daniel Webster a Henry S. Fox - 24 aprile 1841, British and Foreign State Papers, vol. 29, 1137 s.
[80] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, p. 42
[81] GILL T.D., "Chapter 5. The Temporal Dimension of Self-Defense: Anticipation, Pre-emption, Prevention and Immediacy", in International Law and Armed Conflict: Exploring the Faultiness, Leiden, 2007, pp. 113-155
[82] *Ibidem*, pp. 113-155.

considerando che un'occupazione può essere diffusa nel tempo senza che vi sia reazione immediata da parte dello Stato vittima.

Circa la definizione di aggressione nel 1974, l'Assemblea generale delle Nazioni Unite[83], nel primo articolo della risoluzione 3314, utilizzò la formula "*Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another. State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition*"[84].

Stilò inoltre una lista di atti configurabili come aggressione. La lettera (a) dell'art. 3 della risoluzione 3314 sulla definizione di aggressione, infatti, riporta che: "th*e invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof*"[85], andando a inserire l'occupazione tra le azioni costituenti a tutti gli effetti aggressione come da definizione del già citato art. 1.

Tale visione sembrerebbe dunque consentire la legittima difesa pur restando da definire se vada effettuata all'interno di uno specifico arco temporale. Parte della dottrina[86] ritiene che una volta esperite senza successo tutte le azioni volte ad una pacifica risoluzione della controversia un Paese possa, per recuperare il territorio perso, passare legittimamente all' applicazione dell'articolo 51 della Carta ONU.

---

[83] Assemblea generale, risoluzione 3314 (XXIX) del 14 dicembre 1974 sulla definizione di aggressione, disponibile su https://daccess-ods.un.org/tmp/1415046.45347595.html
[84] *Ibidem*, art. 1.
[85] *Ibidem*, art. 3 (a)
[86] RONZITTI N., Diritto internazionale dei conflitti armati, 6. ed., Torino, 2017, p. 42.

La stessa dottrina però fissa l'impossibilità di invocare la legittima difesa in caso di occupazione consolidata nel tempo.

A tal proposito si sostiene che "*il diritto internazionale tutela il possesso, purché qualificato dall'effettività e dall'acquiescenza o dall'assenza di proteste, sarebbe difficilmente giustificabile il ricorso alla legittima difesa per riappropriarsi di un territorio su cui lo Stato interveniente vanti un titolo giuridico*"[87].

A sostegno di questo va considerato che l'occupazione prolungata nel tempo non può essere configurata come attacco armato continuato, previsto dall'articolo 51 come tipologia legittimante l'istituto in esame.

Inoltre, da una attenta analisi dello stesso articolo si vede come venga utilizzata la formula "*if an armed attack occurs*"[88] dove il termine "occurs" va a definire la specifica collocazione nel tempo, un avvenimento non temporalmente diffuso ma puntiforme e che, dunque, non consente di poter dilatare il concetto di immediatezza.

L'"occurs" della Carta, in conclusione, ci aiuta ad individuare il preciso istante dal quale è possibile invocare il diritto alla legittima difesa.

Ad ogni modo non sembrerebbero ravvisarsi casistiche giustificanti un ricorso alla legittima difesa tardivo anche in caso di prolungata violazione del diritto internazionale seppur l'articolo 14, § 2, del draft articles on responsibility of states for internationally wrongful acts[89], affermi che "*The breach of an international obligation by an act of a State having a continuing*

---

[87] Ibidem.
[88] ONU, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, 1945, art. 51.
[89] Commissione di diritto internazionale, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, art. 14 , § 2, disponibile su https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

character extends over the entire period during which the act continues and remains not in conformity with the international obligation". A mente di quanto riportato la violazione internazionale non decade con il passare del tempo o per tacita accettazione e questo in teoria potrebbe supportare la tesi che vede la possibilità di usare la forza armata in risposta.

Sia i favorevoli che i contrari a tale visione concordano però che vada distinto una particolare fattispecie: il caso dell'occupazione avvenuta a seguito di un conflitto armato.

Secondo parte della dottrina, infatti, il solo fatto che l'occupazione sia derivata da un attacco armato configura il "continuo attacco armato" legittimante la legittima difesa anche dopo molto tempo[90].

Il trovarsi invece in presenza di una occupazione non derivante da attacco armato configurerebbe al contrario la necessità di risolvere pacificamente il contendere trovandosi, all'atto pratico, in una cosiddetta disputa territoriale.

Ad ogni modo risulta difficile considerare disputa territoriale un'occupazione stando a quanto definito dal già citato articolo 3, lett. (a) della ris. 3314 dell'Assemblea Generale delle Nazioni Unite[91] in cui, si ribadisce, l'occupazione è un atto costituente aggressione, e dunque, un attacco armato.

Sull'argomento rimane in ogni caso una mancanza di definizione, cosa che inevitabilmente lascia spazio a teorie e valutazioni discrezionali.

---

[90] AKANDE D. – TZANAKOPOULOS A., Use of Force in Self-Defence to Recover Occupied Territory: When Is It Permissible? in EJIL:Talk!, Blog of the European Journal of International Law, 2020, disponibile su https://www.ejiltalk.org/use-of-force-in-self-defence-torecover-occupied-territory-when-is-it-permissible/.

[91] Assemblea generale, risoluzione 3314 (XXIX) del 14 dicembre 1974 sulla definizione di aggressione, art. 3 (a)

10. La legittima difesa collettiva

L'articolo 51 della Carta ONU prevede due tipi di legittima difesa: individuale, a cura dello Stato che subisce, e collettiva a cura di terzi non coinvolti direttamente.

Il concetto di legittima difesa collettiva venne inserito nell'art. 51 su richiesta degli stati latinoamericani volendo trovare un supporto giuridico ai c.d. patti di difesa regionali, in particolare l'Atto di Chapultepec del 3 marzo 1945[92].

Ad integrazione di quanto già previsto per l'individuale, al fine di consentire l'intervento plurilaterale, lo Stato deve in primis dichiarare di essere vittima di un attacco armato esterno e successivamente richiedere l'assistenza di altri Stati[93].

La CGI ha evidenziato l'importanza che tale possibilità rientri nella consuetudine in modo da poter essere attivata anche in mancanza di ratifica o modifica della stessa Carta ONU.[94]

Va infatti ricordato che l'articolo 51 prevede che lo Stato oggetto di attacco sia a tutti gli effetti membro delle Nazioni Unite. Questo sembrerebbe escludere la possibilità di una difesa collettiva per non membri ma a tal proposito risulta interessante quanto avvenuto durante la guerra in Vietnam, quando gli Stati Uniti intervennero nonostante il Vietnam, al tempo, non fosse membro ONU.

Tale atto infatti sembrò di per sé un'integrazione fattuale dell'articolo 51 e, definitivo in materia, fu il già citato caso Nicaragua c. Stati Uniti con il quale la CIG, come già detto, sancì il

---

[92] Il 3 marzo del 1945 a margine della conferenza interamericana di Città del Messico, la quasi totalità dei ministri degli Esteri delle repubbliche americane, ad eccezione di Argentina e Salvador, siglarono una dichiarazione di "assistenza reciproca e solidarietà".
[93] Corte internazionale di giustizia, case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), sentenza del 27 giugno 1986, ICJ Reports, 1986.
[94] *Ibidem*, § 176.

carattere consuetudinario alla legittima difesa collettiva allargando di fatto lo stesso all'intera Comunità internazionale.

Ultimo aspetto interessante dell'istituto in esame è quello che, in un certo senso, rappresenta una limitazione per lo Stato terzo chiamato in causa.

L'imminenza dell'attacco deve essere di tale portata da far risultare l'opera di soccorso richiesta non meno che necessaria in considerazione dell'impossibilità della vittima di resistere con i propri mezzi[95] ed è per questo motivo che non si può prescindere da una richiesta di aiuto.

Lo stato richiedente dovrà dunque valutare la propria capacità interna di resistere all'offesa ma contemporaneamente lo Stato che intenda intervenire in assistenza dovrà valutare la sostenibilità dell'intervento a livello operativo e giuridico in quanto, mancando i presupposti di cui all'articolo 51, ben si potrebbe configurare l'illecito internazionale per ingerenza negli affari interni altrui.

[95] Ronzitti N., *Introduzione al diritto internazionale*, IV ed., Torino, 2013, p. 425.

Capitolo 2 – Il cyberspazio

1. Definizione di cyberspazio ed excursus storico

Definire in maniera univoca il cyberspazio è, forse oggi più che mai, estremamente complesso essendo allo stesso tempo contesto fisico e virtuale.

Se è vero che la prima cosa a cui pensiamo quando immaginiamo il mondo cyber è un terminale connesso alla rete, bisogna innanzitutto fare i conti con il fatto che gli attacchi cibernetici possono avvenire attraverso qualsiasi canale comunicativo possibile, dalle reti intranet aziendali ai dispositivi casalinghi dell' "*internet of things*". Lo spazio cibernetico non va dunque identificato esclusivamente come qualcosa di esterno alle nostre abitudini lavorative o private.

Essendo difficile immaginare un luogo o un oggetto specifico, prenderemo in prestito la definizione utilizzata nel 2010 dall'esercito americano in un documento dedicato allo stato di previsione delle capacità in ambito cibernetico di forza armata nel periodo dal 2016 al 2028[96] in cui viene riportata la dicitura: "*A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*".

Da questa definizione comprendiamo come il cyberspace non sia caratterizzato unicamente da internet ma piuttosto lo includa. L'International Telecommunication Union (ITU), agenzia ONU

[96] The United States Army's Cyberspace Operations Concept Capability Plan, TRADOC Pamphlet 525-7-8, 22 febbraio 2010, p. 6, disponibile su http://fas.org/irp/doddir/army/pam525-7-8.pdf.

specializzata in tecnologie dell'informazione, descrive il cyberspace come un "*campo fisico e non fisico creato da e/o composto da alcuni o tutti i seguenti elementi: computer, sistemi di computer, network e programmi informatici, i dati, i contenuti di questi di dati, il traffico di dati e gli utenti*" [97].

In maniera forse ancora più analitica Derek Reveron, professore presso lo US Naval war college, in una nota pubblicazione del settore[98] divide il cyber spazio in livelli, uno fisico, uno di dati o "*infocom*" ed uno corrispondente alle interazioni virtuali tra persone.

Sulla falsariga di Reveron, un'altra nota divisione su livelli è quella ipotizzata nell'ultima definizione che si ritiene di dover prendere in considerazione, quella di due esponenti di alto profilo in materia ovvero Shmuel Even e David Siman-Tov, ricercatori presso l'istituto per gli studi per la sicurezza nazionale israeliana e membri della Israeli Intelligence Community. In una pubblicazione specialistica dividono infatti il cyberspace in tre livelli interdipendenti: Il primo "umano", composto dagli utenti, il secondo "logico", quindi software e dati, il terzo "fisico", con terminali e apparati di rete quali, ad esempio, i sistemi di "*Supervisory Control And Data Acquisition*" (Scada), per il controllo dei processi industriali[99].

Lette queste definizioni si comprende quanto parlare di contesto cibernetico in maniera univoca abbia poco senso. Un attacco può infatti avvenire attraverso un passaggio di dati come anche attraverso la compromissione fisica di un server o ancora si

---

[97] www.itu.int/cybersecurity

[98] REVERON D. S., An introduction to National Security and Cyberspace, in Cyberspace and National Security, Washington (DC), 2012, p. 5

[99] EVEN S., SIMAN-TOV D., Cyber Warfare: *Concepts and Strategic Trends*, INSS - Memorandum 117, Tel Aviv, 2012, p. 10

può decidere di attaccare gli utenti stessi attraverso raffinate e prolungate tecniche di social engineering.

Indipendentemente dal tipo di accesso a risultare indebolito sarà il sistema nel suo complesso.

2. Il conflitto nel dominio cibernetico

Al giorno d'oggi, in particolar modo nel mondo militare, più che di spazio si usa parlare di dominio[100] e questo perché il c.d. dominio cibernetico è stato equiparato agli altri storicamente classificati risultando però ricco di peculiarità anche rispetto agli ambiti più giovani e tecnologici come quello aereo e quello spaziale. Si tenterà, a tal proposito, di indicare alcune differenze esplicative:

1. Armamenti con costi di produzione e tempi estremamente ridotti rispetto ai cinetici;
2. Attacchi che non risentono di spazio e tempo: una penetrazione in un sistema informatico può avvenire ed essere ripetuta in tempo reale con valutazione del danno fondamentalmente istantanea;
3. Concreta possibilità, da parte dell'attaccante, di rimanere occulto potendosi celare dietro attacchi differiti nel tempo e agenti inconsapevoli;
4. Difficoltà da parte dell'offeso di reagire in tempo reale;
5. Basso rischio di danni collaterali: si confronti il sorvolo su una batteria contraerea e le conseguenti perdite umane.

[100] NATO, Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, 9 July 2016, § 70: «[…] we reaffirm Nato's defensive mandate and recognise cyberspace as a domain of operations in which Nato must defend itself as effectively as it does in the air, on land, and at sea».

Se da una parte l'attacco cibernetico non comporta, in linea di massima, rischi per chi lo compie, di contro i danni arrecati godono di un'alta percentuale di resilienza e reversibilità[101].

Se ad esempio viene compromesso un software governativo, salvo attacchi profondi, verrà ripristinata la versione precedente all'attacco nonché, lesson learned, eliminata la vulnerabilità[102].

In tal senso Edward Luttwak diceva che un attacco cibernetico, se funziona, funziona una volta sola e se perpetrato sarà inevitabilmente destinato al fallimento[103].

Aspetto peculiare inoltre è la difficoltà nel trovare una netta linea di demarcazione tra mondo militare e civile. A tal proposito si pensi ad hacker reclutati da difese militari governative o all'utilizzo di infrastrutture civili, come reti dati o di interesse strategico nazionale, da parte di personale militare.

3. Principali tipologie di attività malevoli cibernetiche

Le azioni malevoli poste in essere in ambito cibernetico sono per alcuni versi simili a quelle che possono trovarsi all'interno di un comune opuscolo finalizzato alla sensibilizzazione in materia. Possiamo brevemente elencarne qualcuna:

- Spamming: azione verso la quale siamo tutti potenzialmente esposti. Si manifesta nell'invio di comunicazioni a mezzo e-mail di tipo generalmente commerciale. Obiettivo non è il danno diretto ma il poter inoculare malware o applicativi occulti anche ad attivazione differita nel tempo (c.d. software dormienti).

[101] CLARKE, KNAKE, Cyber War; BRENNER J, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, New York, 2011

[102] GIACOMELLO G - BADIALETTI G, Manuale di Studi Strategici. Da Sun Tzu alle nuove guerre, Milano, 2016, pp. 1 e succ.

[103] LUTTWAK E, Strategy: The Logic of War and Peace, Cambridge (MA), 2001

- Phishing o spear phishing: espediente mirato alla raccolta informativa umana a mezzo inganno. Si esegue attraverso identità fasulle ma verosimili allo scopo di indurre il bersaglio alla condivisione di informazioni sensibili, come una password.
- Cross-site scripting: viene eseguito uno script attraverso un sito terzo. Si attiva nel momento in cui la vittima visita un sito appositamente manipolato. Consente l'accesso, anche in remoto, del terminale targhettizzato;
- Defacciamento: Viene modificato un sito web senza averne autorizzazione. Spesso sostenuto da motivazioni ideologiche;
- Spoofing: Simile al phishing, consiste nella falsificazione di identità o di pagine web al fine di una interazione di fiducia con il target;
- Botnet: compromissione di una rete di macchine che prendono la denominazione di "zombie". Una volta infettate rispondono ai comandi dell'attaccante all'insaputa del reale proprietario;
- Denial of Service e Distribuited Denial of Service (DOS o DDOS): attacco massivo ad un server al fine di esaurirne le capacità di elaborazione. Si manifesta in un bombardamento di richieste superiore alla quantità gestibile dall'elaboratore. Viene effettuato anche ai danni di bande dati per esaurirne la portata o non consentire ulteriori connessioni. È "distribuited" quando le fonti di attacco sono multiple, come nel caso di botnet. Questo ultimo tipo garantisce l'anonimato o almeno ritarda le attività di identificazione non essendo il mittente facilmente rintracciabile figurando, come attaccanti, i server zombie[104];

[104] Nel 2007, l'Estonia è stata colpita massicciamente da un attacco DDOS che ha bloccato servizi, telecomunicazioni e banche. L'attacco, reputato proveniente da hacker patriottici russi, è stato scatenato dalla rimozione di un monumento di guerra sovietico dal centro di Tallinn. Si è trattato di un massiccio attacco Ddos. La tipologia di attacco ha comportato l'impossibilità di una precisa attribuzione e dunque di una sanzione nei confronti della Russia.

- Malware, virus, worm: codici di programmazione maligni inseriti in elaboratori. Lo scopo è la compromissione dei dati attraverso cancellazioni, esportazioni o inibizioni o generare il malfunzionamento di software, hardware o reti in generale[105]. I malware rappresentano, informaticamente parlando, la più grave forma di offesa nelle relazioni tra Paesi. Di seguito alcuni esempi:
- Logic bomb: codice inserito in un software che si innesca a seguito di determinate condizioni come una specifica azione, una data ecc. Può arrivare all'inibizione completa del calcolatore compromesso;
- Trojan: vanno fisicamente installati sul pc di volta in volta al fine di applicare istruzioni maligne finalizzate, solitamente, all'apertura di "back door";
- Backdoor: consente il superamento dei sistemi di sicurezza installati;
- Rootkit: malware capace di aggirare la necessità di autorizzazione da parte dell'amministratore di sistema in modo da poter operare all'interno dello stesso;
- Virus: codice in grado di autoriprodursi al fine di colpire sempre più efficacemente i terminali infettati;
- Worm: simile ai virus ma senza necessità di altri file presenti per la diffusione.

Quanto sopra sinteticamente elencato vuole mostrare, a fronte della volontà di attacco, quante modalità di attivazione esistano. Possiamo infatti dire che per analizzare un attacco subito, al di là del danno, vanno considerati molti altri elementi, tra cui la natura dell'aggressore, l'obiettivo, le modalità di esecuzione e l'entità del danno.

[105] v. Il caso di Stuxnet, *infra*.

Ben si comprende quanto anche un semplice attacco dimostrativo, come un defacciamento, sia molto complicato da classificare o, meglio ancora, quanto sia complicato trovare definizioni univoche e categorie durevoli nel tempo, anche per il continuo aggiornamento dello stato dell'arte e questo perché, come già detto precedentemente, difficilmente un attacco ripetuto nelle medesime modalità sarà efficace alla stessa maniera.

Non deve stupire quindi il fatto che organizzazioni governative a livello planetario, come anche diverse comunità epistemologiche, abbiano tentato di definire, accademicamente, cosa sia un attacco cibernetico.

L'attacco cibernetico, inteso in chiave operativa bellica e dunque nell'ambito della cyber warfare, ha subito una straordinaria evoluzione storica al punto che già nel 1995 Martin Libicki, celeberrimo professore americano autore di un altrettanto famoso saggio[106], ritenesse impossibile definire cosa effettivamente fosse una guerra cibernetica.

Quando nel 1998 Libicki si unì al collettivo Research and Development (RAND)[107], facendo tesoro dell'esperienza in ambito Difesa, racchiuse la cyberwarfare sotto quelle forme di offesa definite "semantiche". Un sistema sotto "attacco semantico" infatti, pur restando efficiente, genera risposte non coerenti con la realtà[108]. In altre parole, l'attacco di tipo semantico riesce a danneggiare infrastrutture fisiche o logiche senza far rilevare alcun tipo di problema ma dando output diversi dal previsto.

---

[106] LIBICKI M. C., Information Technology Standards: Quest for the Common Byte, Berkeley, 1995.
[107] RAND, da Research and Development, è un collettivo o "think tank" non-profit costituito nel 1948 finanziato, oltre che dal mondo accademico e da diverse organizzazioni, in gran parte dal governo americano e il cui scopo è fare ricerca in molteplici campi.
[108] LIBICKI M. C., what is Information Warfare? Washington, 2005

Pur precisa ed attuale, la definizione di Libicki non basta a coprire l'eterogeneità dell'universo cibernetico di offesa.

Uno dei massimi riferimenti americani in tema di sicurezza telematica, Richard Clarke[109], ha associato le cyberwars a quelle azioni portate avanti per penetrare terminali o reti di un'altra nazione, avendo come fine ultimo il danneggiamento sotto forma di interdizione[110].

Grazie a Clarke si passa dagli attacchi semantici di Libicki ai cosiddetti attacchi "sintattici", capaci di provocare danni ai sistemi operativi, perdite di dati e danneggiamenti fisici dell'apparato[111].

Si ritiene comunque che anche la definizione di Clarke sia poco adatta alla realtà contemporanea nel momento in cui identifica l'attacco come un'azione statuale, escludendo altri tipi di attaccanti come "non-state actors", gruppi autonomi, hacker, attivisti, terroristi ecc., tutte formazioni che verranno meglio descritte in un apposito paragrafo[112].

Va considerato che negli scritti di Clarke, come anche in quelli di Libicki, il focus si pone sulla natura tecnica dell'apparato colpito nonché sul fatto che l'attacco parta e arrivi in luoghi ben definiti lasciando poco spazio alle motivazioni ed alla natura del mandante.

Ciò che può realmente comportare una diversificata applicazione del diritto caso per caso può infatti risiedere in molteplici elementi quali ad esempio le motivazioni ispiratrici o

---

[109] Richard Clarke, esperto di sicurezza nazionale americano, riferimento mondiale in tema di cybersecurity nonché ex membro dello staff per gli affari militari del governo americano. www.richardaclarke.net.
[110] CLARKE R., KNAKE R., *Cyber War*, 2012, p. 6
[111] Il caso Stuxnet, supposto attacco del 2009 perpetrato dagli Stati Uniti e da Israele ai danni di un impianto di arricchimento dell'Uranio iraniano, meglio descritto successivamente in un apposito paragrafo, può essere considerato un ibrido di entrambe le tipologie, semantico in quanto forniva ordini non previsti senza allarme, sintattico per il tipo di danno fisico arrecato.
[112] v. *Infra*, § 2.4.

anche il danno atteso. Si pensi ad una semplice visione di dati su un computer, al prelevamento degli stessi, all'inibizione di un server a scopo di riscatto, all'inibizione da parte governativa di un impianto di arricchimento atomico di un altro paese. Si tratta evidentemente in ogni caso di azioni classificabili come cyber attacco ma di potenziale collocazione giuridico - penale ben diversa[113].

A tal proposito è interessante citare quanto riportato dal Dipartimento americano della Difesa in un documento del 2011 e visionabile sul sito web del National Security Cyber Space Institute in cui, a livello terminologico, si definisce l'attacco cyber come "*un attacco ostile perpetrato utilizzando computer, sistemi o network collegati e finalizzato a interdire e/o distruggere le risorse o le funzioni critiche dei sistemi cibernetici di un avversario. Gli effetti attesi di un attacco non sono necessariamente limitati ai computer scelti come bersaglio, o ai dati stessi – ad esempio, gli attacchi volti a inibire o distruggere l'infrastruttura di comando e controllo*"[114].

Una definizione interessante in quanto qualifica il danno non solo con l'infrastruttura ma anche con le capacità del target, nell'esempio identificate con il dispositivo di comando e controllo di uno Stato Maggiore di forza armata.

Interessante integrazione al discorso può essere fatta riprendendo quanto riportato dalla Shangai Cooperation Organization (SCO)[115] in tema di guerra di informazione ed in

---

[113] AA.VV., The Law of Cyber Attack, Berkeley university, 2012, p. 824

[114] A tal proposito: CARTWRIGHT J. E., Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories: Joint Terminology for Cyberspace Operations, Washington (DC), 2010, disponibile su https://info.publicintelligence.net/DoD-JointCyberTerms.pdf

[115] SCO, Shanghai Cooperation Organisation, organizzazione finalizzata ad iniziative di cooperazione politica, economica e di sicurezza formato

particolare sul tema della coesione sociale portando all'attenzione il peso che le informazioni presenti in rete possono avere, ad esempio, nel rapporto tra la popolazione ed un governo.

Il riferimento chiaramente va alle attività di propaganda e contropropaganda perpetrate in particolare in paesi particolarmente ermetici come, ad esempio, la Corea del Nord.

Si potrebbe inoltre definire l'attacco cyber come un'azione finalizzata a minare le funzioni di una rete informatica per finalità politiche o di sicurezza nazionale[116].

Dunque, alla luce delle definizioni riportate, ritengo che una analisi efficace di un evento cibernetico offensivo debba obbligatoriamente considerare in primis azione e obiettivo:

- l'azione deve essere volontariamente perpetrata per causare danno anche se tale danno derivi dalle cosiddette difese "attive" escludendo invece tutto quanto sia avvenuto per errore o a causa di imprevisto.
- l'obiettivo è altresì l'elemento che forse maggiormente deve far testo in un'analisi. Colpire con un drone una batteria contraerea non è un attacco cyber quanto piuttosto l'utilizzo di un'arma convenzionale molto sofisticata. Diverso è il caso del missile che colpisce una dorsale portante di dati andando ad inibire la comunicazione classificata di una componente della Difesa nemica.

Un altro elemento da non sottovalutare è l'effetto dell'attacco. Se nell'attacco cinetico avviene la distruzione fisica dell'obiettivo, nel cibernetico il fine è la compromissione delle capacità avversarie, indipendentemente dalla distruzione fisica. Come già riportato, possiamo avere un attacco di tipo semantico, che non

---

attualmente da China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, Uzbekistan. http://eng.sectsco.org/

[116] AA.VV., The Law of Cyber Attack, Berkeley university, 2012, p. 826.

tocca l'hardware ma la modalità di processamento delle informazioni, di tipo sintattico, che provoca danni a sistemi operativi comportando il non funzionamento ed infine fisico, l'hardware.
Va infine considerata la finalità dell'attacco cyber, tipicamente politica.

Riprendendo le definizioni proposte, nel momento in cui il mandante dovesse essere pubblico, la finalità sarà sicuramente di carattere politico. In caso invece ci si trovi in presenza di attore privato andrà valutato se lo stesso sia stato assoldato da un'organizzazione statale o semplicemente abbia agito in autonomia. In tal caso non parleremo più di war-scene ma di azione criminale.

Va infatti compreso che esistono tre tipologie di attività che, seppur cyber, non possono accademicamente essere considerate nel novero della cyber warfare:

- il *Cyber crime*[117], atto illecito privato per fini di lucro rientrante nell'ambito del diritto penale;
- il *Cyber terrorismo*, atto di derivazione privata non per forza guidato da fini personali ma anche ideologici e per questo non annoverabile nella guerra;
- la *Cyber protesta,* realizzata da attivisti con finalità principalmente propagandistiche e considerata da molti come "soft cyber warfare", anche perché nel momento in cui scadesse in azioni violente fuoriuscirebbe definitivamente dall'ambito cibernetico finendo in quello cinetico.

Esistono infine tre tipi di attività facenti parte del cyberspazio per le quali si fatica a trovare una classificazione nella cyber warfare, per le motivazioni di seguito riportate,:

[117] WALL D. S., Cybercrime. The Transformation of Crime in the Information Age, Cambridge, 2007

- il *Cyber spionaggio*, con il quale si entra nel sistema avversario per acquisire informazioni in maniera non autorizzata. Può essere finalizzato alla raccolta di informazioni da offrire al decisore per formulare una strategia o alla raccolta di segreti industriali come anche di software o database. L'attività di spionaggio non viene inserita nel novero della cyber war comportando una compromissione dell'integrità altrui ma senza danno fisico. Per questo motivo, a livello internazionale, non esiste un vero e proprio divieto allo spionaggio;
- la *soft Cyber Warfare*, attività finalizzata alla compromissione senza distruzione. È quello in cui ricadono le cosiddette psycological operations (psy-ops), come la propaganda, il cui fine è modificare credenze e condotta dell'avversario. Trattandosi di metodi non legati ad atti fisici non può essere considerato uso della forza. Al Qaeda si dotò di un vero e proprio mensile divulgato a livello globale, "*Inspire*".

In conclusione, parlare di Cyber non vuol dire parlare automaticamente di attacco occulto. Va valutato chi utilizza i mezzi, quali mezzi utilizza e soprattutto per quali finalità.

In ogni caso, un attacco cibernetico vero e proprio può avere differenti scopi, quali ad esempio l'esercitare pressione verso decisioni strategiche di un altro paese, sventare specifici rischi o rispondere in forma di rappresaglia.

4. Cyber non-state actors (CNSA)

I Cyber Non State Actors (CNSA) sono figure di estrazione privata operanti nel Cyber spazio per interessi che spaziano dai finanziari ai politico/ideologici.

In considerazione dell' importanza dello spazio cibernetico nelle dinamiche contemporanee e della globalizzazione delle

informazioni, gli attori non statali (NSA) hanno assunto un ruolo fondamentale anche nell'influenzare le decisioni dei governi al punto di essere spesso sponsorizzati dagli stessi.

A causa della fluidità dei confini e delle sempre più sofisticate tecniche di penetrazione informatica, i NSA sono diventati un punto chiave nelle agende politiche in tema di sicurezza nazionale, soprattutto in considerazione della mancanza di un quadro giuridico univoco a livello internazionale e del fatto che il cyber spazio è ad oggi un'arena estremamente attraente sia per gli attori pubblici che per quelli privati.

Ulteriore punto di grande interesse è la sempre più alta partecipazione nei teatri di crisi mondiale.

Le attività svolte spaziano dal danno finanziario, come l'estorsione, allo spionaggio, fino all'attacco di infrastrutture governative nemiche. Le imponenti capacità, oltre l'eterogeneità degli operatori, portano gli Stati a rapportarsi con queste forze occulte, spesso di estrazione criminale, tollerandole o addirittura utilizzandole al fine di moltiplicare le capacità intelligence nazionali.

Si manifesta dunque o un controllo diretto o uno scambio reciproco vantaggioso che vede da un lato la fornitura di informazioni preziose a danno di altri paesi e dall'altro denaro o immunità. Accanto ad un interesse privato di tipo finanziario capita dunque che conviva una strategia statuale che beneficia degli introiti illeciti degli stessi hacker.

Altre frange di tipo autonomo prevedono invece scopi ideologici o religiosi in aperto contrasto con il cosiddetto sistema.

Al fine di meglio comprendere il ventaglio di operazioni messe in atto quotidianamente, è utile tentare una classificazione dei CNSA. Verranno a tal proposito presi in considerazione riferimenti

quali la motivazione, il tipo di organizzazione e il rapporto con lo Stato di provenienza.

Primo raggruppamento in esame è quello dei *cyber crime groups*, o in generale della criminalità informatica, che l'FBI, attraverso i suoi report annuali, stima come la terza economia mondiale dopo Stati Uniti e Cina.

Il bureau americano, nel rapporto 2021, ha valutato un danno all'economia mondiale previsto in 10,4 trilioni di dollari entro il 2025 con perdite nell'ordine dei 4 miliardi di dollari e un aumento esponenziale delle denunce[118].

Lo stato dell'arte attuale del cyber crimine è il Cybercrime-as-a-service (C-A-A-S) ovvero l'arruolamento a fini di lucro di singoli o gruppi che, agendo come privati, agevolano l'occultamento del mandante. È leggerissima, infatti, la linea di demarcazione tra "*Advanced Persistent Threat Groups*", operanti per conto degli Stati e criminali a titolo privato secondo il modello C-A-A-S che possono essere coinvolti in operazioni spot rendendo impossibile tracciamento e previsione[119].

Inutile ripetere che, anche se individuati, sia poi praticamente impossibile trovare un collegamento con lo Stato mandante e dunque valutare una possibile sanzione su base internazionale.

Altra tipologia di hacker è quella dei cosiddetti "*hacktivisti" o "patriottici",* attori individuali con forte motivazione politica o ideologica. Trattasi di lupi solitari o di collettivi multinazionali, detti transnazionali decentralizzati, caratterizzati dalla mancanza di una struttura centrale e dalla diffusione puntiforme. Gli hacker

[118] Federal bureau of Investigation (FBI), Internet Crime Complaint Center (IC3), https://www.ic3.gov/Home/AnnualReports

[119] In questo senso emblematica la partecipazione del Russian Business Network, una delle organizzazioni criminali più potenti e strutturate, alle operazioni contro la Georgia del 2008 come anche i noti gruppi Conti e Stormous a sostegno dell'"operazione speciale" in Ucraina e attualmente in attività.

patriottici, differentemente dagli *hacktivists*, sono nello specifico guidati da forte motivazione patriottica a favore del proprio Stato[120].

Diverso è il caso dei "*mercenari",* esperti IT assoldati per condurre sofisticate operazioni informatiche finalizzate all'*information gathering*[121]*, al network exploitation*[122] come al supporto alle attività intelligence nazionali.

Quello che questi gruppi abitualmente fanno, al pari dei "contractors" tradizionali sul campo, è lavorare in parallelo con la struttura militare ufficiale fornendo supporto durante un attacco attraverso ad esempio il monitoraggio delle attività dei server classificati o delle reti intranet nemiche.

Come meglio spiegato nei paragrafi successivi, ci sono paesi, come l'Italia, in cui l'attività offensiva o difensiva attiva ancora trova difficile collocazione negli ordinamenti nazionali anche se piccoli passi si sono in fatti sia a livello Difesa, con la costituzione del Comando per le Operazioni in rete, sia intelligence con la costituzione della Agenzia per la *Cybersicurezza* nazionale (ACN).

È comunque giusto ribadire che ad oggi, in Italia, non è contemplata l'iniziativa offensiva di tipo informatico.

Il vantaggio, si ripete, sta nel fatto che ufficialmente non sarà mai possibile provare questa forma di contratto rimanendo, in superficie, un'attività di carattere privato. È oltremodo interessante e chiarificatore contestualizzare quanto elencato nell'attuale scenario del conflitto russo-ucraino dove sia da una parte che dall'altra avvengono intense attività di sabotaggio

---

[120] Si prenda in considerazione alcune frange, anche se poco strutturate, correlate agli eventi di Capitol Hill e più in generale al complottismo collegato, suo malgrado, all'ex presidente Trump.
[121] Spionaggio attraverso raccolta di dati da server
[122] Il "bucare" le reti attraverso virus Trojan per mettere a disposizione dello Stato ospitante gli accessi.

informatico, di spionaggio, di propaganda e contropropaganda. Nello specifico conflitto le aree di competenza di attori statali e non sono di difficile individuazione come osservabile dai monitoraggi indipendenti[123] effettuati sul cyberspace che mostrano come, da entrambe le parti, siano attivi collettivi o singoli, tra cui il noto "Anonymous". Nel merito della crisi degna di nota è stata la formazione dell'Ukraine IT Army (esercito informatico ucraino) costituito da volontari esperti IT coordinati dallo stesso governo il quale, attraverso il Ministero per la trasformazione Digitale ed il suo ministro Mykhaylo Fedorov, ha invitato all'attacco verso la Russia.

Esperti a tutti i livelli si sono interrogati sulla collocazione giuridica di questi elementi non puramente statuali in considerazione del fatto che un collettivo come Anonymous, quando impegnato a sostegno di uno Stato, rappresenta un formidabile moltiplicatore di forza anche a danno di infrastrutture strategiche fisiche. All'atto pratico trattasi di muovere guerra a uno Stato attraverso l'utilizzo di formazioni che ufficialmente non hanno territorio fisico specifico e di conseguenza sovranità territoriale.

Ci si chiede inevitabilmente come si possa mai applicare il diritto internazionale su questi presupposti come anche poter far intervenire la diplomazia ufficiale.

È dunque possibile per un terzo, ad esempio l'ONU, tentare di portare la pace o evitare un'escalation a seguito di attacco subito da un CNSA?

La tendenza culturale a non considerare il Cyber spazio come dominio fondamentale di guerra porta a non considerare che un

[123] Su tutti l'attività a mezzo Twitter e del sito web di cyberknown, consultabile su https://cyberknow.medium.com/update-23-2023-russia-ukraine-war-cybertracker-may-03-efeb21056713

CNSA, se ben organizzato, può arrivare a minare la sicurezza non solo di strutture strategiche, come centrali elettriche o nucleari, ma anche il sostegno del popolo al proprio governo con conseguenze sociali devastanti[124].

In conclusione ad oggi sembrerebbe ancora irrisolto il dilemma giuridico circa la possibilità di risposta immediata attraverso canali ufficiali ad offensive cibernetiche, in particolar modo verso elementi che apparentemente non risultano collegati all'apparato statuale.

A similitudine di quanto affermato, ed anticipando le problematiche di attuazione della legittima difesa in contesto cibernetico che verranno più approfonditamente analizzate nel successivo capitolo, il tempo che si necessiterebbe per individuare, attribuire con certezza un attacco e oltretutto valutare sanzioni è all'atto pratico incompatibile con le tradizionali tempistiche internazionali. Anche avendo volontà di reagire ufficialmente va sempre considerato che i CNSA, non facendo organicamente parte del Governo di turno e soprattutto avendo spesso motivazioni differenti dal mandante, potrebbero istantaneamente spostare il punto di partenza degli attacchi in un altro stato complice vanificando in pochi istanti gli sforzi della Comunità internazionale.

L'unica via percorribile, che si tratti di non-state actors come in generale di cyber warfare, è non solo dare culturalmente la giusta importanza ad un contesto ibrido ma estremamente pervasivo ma anche fissare una solida base normativa ed operativa da applicare in particolar modo alla c.d. cyber defence tentando oltretutto di modificare l'atteggiamento tradizionalmente

[124] Si pensi alle primavere arabe e l'escalation di partecipazione avvenuta a mezzo social

passivo che contraddistingue le nostre politiche in materia, come meglio spiegato successivamente.

Va prioritariamente compreso però cosa si intenda per *defence* e *security* in ambito cyber e quali siano le differenze.

5. Difesa e sicurezza cibernetica

Dopo aver provato a dare una definizione di cyber space, la seconda grande sfida è quella di darne una a sicurezza e difesa nello spazio virtuale.

I termini che entrano in gioco, dunque, sono in particolare due: "*cyber security*" e "*cyber defence*". L'importanza di un sistema organizzato di difesa deriva dal fatto che lo sviluppo del traffico di dati a livello mondiale in termini economici e di informazioni ha coinciso con quello della criminalità informatica

L'Agenzia dell'Unione europea per la cybersicurezza (Enisa)[125], già una decina di anni fa spingeva per la creazione, all'interno di ogni Stato, di un sistema o strategia di cybersicurezza[126] e questo per non trovarsi impreparati ad attacchi cibernetici che, come da regola 30 del primo Tallin Manual, venivano definiti: "*…a cyber-operation, wheter offensive or defensive that is expected to cause injury or death to persons or damage or destructions to objects*[127]"

L'Enisa ha tentato di trovare punti comuni nelle strategie dei vari Stati, lavoro non banale in considerazione del fatto che la sicurezza nazionale è materia prettamente politica o comunque statale, dunque soggetta a variabili dipendenti dai governi di

[125] Fino al 2019 Agenzia Europea per la sicurezza delle reti e dell'informazione, nome sostituito con Regolamento UE 2019/881. https://www.enisa.europa.eu/
[126] 86 ENISA, 2012, National Cyber Security Strategies: setting the course for national efforts to strengthen security in cyberspace. Disponibile su https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[127] SCHMITT, M. N., Tallinn Manual on the international law applicable to cyber warfare, Cambridge, 2013, p. 91.

turno. Ancora una volta trovare una visione unitaria della *cybersicurezza* risulta pressoché utopico.

6. Le strategie di sicurezza nazionale nel mondo

Avere un piano strategico avrebbe comportato, secondo l'Enisa, il miglioramento della sicurezza come anche della resilienza in caso di attacco e questo poteva avvenire solo stabilendo una serie di obiettivi da raggiungere in tempi stabiliti, naturalmente a patto che cyber-defence e cyber-security finissero nelle priorità delle agende politiche governative.

Anche se al giorno d'oggi siamo abituati a queste terminologie, fino a circa 20 anni fa la cybersicurezza non era materia considerata prioritaria. Fu l'evento delle torri gemelle e la conseguente presa di coscienza circa la mancanza di coordinamento nella comunità intelligence americana, come evidenziato nel rapporto finale della Commissione nazionale d'inchiesta sull'11 settembre[128], a far scaturire, nel 2003, il primo vero piano di cybersicurezza nazionale negli Stati Uniti[129]. Venne in quella occasione considerato il Cyberspazio come elemento nevralgico e venne altresì introdotta, nel 2011, la "*international strategy for cyber-space*"[130], aggiornata nel 2018 dall'ex presidente USA Trump con la "*National cyber Strategy of the*

[128] National Commission on Terrorist Attacks Upon the United States, Finale report (o 9/11 Commission Report), 2004, disponbile su http://www.9-11commission.gov/report/911Report.pdf.
[129] United Nations CISA. (2003). *National Strategy to Secure Cyberspace*. Consultato da https://www.cisa.gov/national-strategy-secure-cyberspace
[130] National Security Council (U.S.), & United States. Executive Office of the President. (2011). International strategy for cyberspace: Prosperity, security, and openness in a networked world. [Washington, D.C.]: Executive Office of the President of the United States, [National Security Council. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

United States of America" e per ultimo, a marzo 2023, dall'attuale amministrazione Biden[131].

Nell'edizione Trump del 2018, su un orizzonte temporale di 15 anni, vennero valutati come strategici per la sicurezza nazionale alcuni punti cardine quali la protezione delle reti, l'economia digitale, la capacità di punire coerentemente gli illeciti informatici. Altri paesi seguirono l'esempio americano del 2003 come la Germania *con* il "*national plan for information infrastructure protection*" del 2005[132] e il "cyber security strategy for Germany"[133] del 2016, l'Estonia, paese leader e pioniere in materia con piani strategici prima nel 2008 e poi nel 2019[134] aventi anche focus di tenore sociale quali il riconoscimento e la protezione di libertà fondamentali anche nello spazio cibernetico, bilanciamento e simbiosi tra innovazione e sicurezza, cooperazione internazionale.

È comunque il 2008 l'anno spartiacque nella percezione circa la necessità di un piano strategico in materia di sicurezza informatica e ad oggi sono 31 i paesi dotati di strategie di sicurezza con 219 organizzazioni coinvolte e 21 macro obiettivi tra cui, su tutti, la cooperazione internazionale, la capacità di risposta

---

[131] Executive Office of the President of the United States of America, National Cyber Strategy of the United States of America, Washington, D.C., 2023. Disponibile su https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[132] Federal Ministry of the Interior, 2005,. National Plan for Information Infrastructure Protection. Disponibile su https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/EN/BSI/Kritis/National_Plan_for_Information_Infrastructure_Protection.pdf?__blob=publicationFile

[133] ENISA, *German National Cyber Security Strategy, 2016, disponibile* su https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Germany

[134] Ministry of Economic Affairs and Communications, Cybersecurity Strategy 2019-2022: Republic of Estonia, Estonia, 2019, *disponibile* su https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Estonia

agli incidenti, il monitoraggio del cyber crime ed il rafforzamento di programmi educativi in materia[135].

Al di là delle lettere di intenti dei singoli paesi anche a livello extraeuropeo, con casi pregevoli come quello canadese, ancora una volta ben si comprende quanto sia difficile trovare una visione univoca in tema di esigenze strategiche, operative o tattiche complice anche la tradizionale gelosia nella condivisione delle informazioni.

7. La strategia nazionale di cybersicurezza italiana

Nell'alveo dell'Agenzia per la cybersicurezza nazionale istituita nel 2021 e per la quale seguirà un approfondimento nel prosieguo, anche l'Italia si è dotata di una strategia nazionale di *cybersicurezza*. Il 18 maggio 2022 infatti il Comitato Interministeriale per la *Cybersicurezza* (CIC), istituito assieme all'agenzia con d.l. 82/2021[136], ha approvato la Strategia Nazionale di Cybersicurezza consistente in 82 misure da realizzare in un orizzonte temporale andante dal 2022 al 2026[137].

Tale strategia, e l'annesso piano di implementazione, ha mirato in sintesi ad un rafforzamento della resilienza in particolar modo in relazione alla tanto agognata transizione digitale, al conseguimento di una autonomia strategica, al gestire da una parte l'evoluzione della minaccia cibernetica, dall'altra le crisi nel medesimo ambito.

---

[135] ENISA, National Cyber Security Strategies - Interactive Map, disponibile su https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

[136] Decreto-legge 14 giugno 2021, n. 82, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", convertito con modificazioni dalla L. 4 agosto 2021, n. 109, in Gazzetta ufficiale n. 185 del 4 agosto 2021, art. 4.

[137] Agenzia per la Cybersicurezza nazionale, Strategia Nazionale di Cybersicurezza 2022-2026 disponibile su https://www.acn.gov.it/strategia/strategia-nazionale-cybersicurezza

L'intera strategia venne basata su quattro pilastri tecnico-operativi: Cybersicurezza e resilienza, Prevenzione e contrasto della criminalità informatica, Difesa e sicurezza militare del paese, ricerca ed elaborazione informativa, il tutto reso possibile grazie alla sinergia tra strutture dello Stato, come Forze di polizia e Forze armate per mezzo del Comando per le operazioni in rete[138], e organismi facenti parte del Sistema per la sicurezza della Repubblica[139].

Il piano di implementazione, allegato al documento di strategia, prevedeva 82 misure operative. Tra queste si diede fondamentale risalto al tema delle certificazioni con misure riguardanti il "r*afforzare il sistema di scrutinio tecnologico nazionale a supporto della sicurezza della supply chain e l'adozione di schemi di certificazione europea di cybersecurity, anche mediante l'accreditamento di laboratori di valutazione pubblico/privati*"[140] e lo "*sviluppare le capacità dei Centri di Valutazione del Ministero dell'Interno e del Ministero della Difesa accreditati dall'ACN, quali organismi di valutazione della conformità, per i sistemi di rispettiva competenza*"[141].

Tra gli obiettivi chiave l'accrescimento delle competenze e delle conoscenze cyber come da misure 12 e 13, riportanti il "c*ontinuare ad accrescere le capacità nazionali di difesa, resilienza, contrasto al crimine e cyber intelligence, rafforzando ulteriormente la situational awareness mediante il monitoraggio*

---

[138] Comando per le operazioni in rete (COR), dipendente dal Comando Operativo di Vertice Interforze, si occupa della condotta delle operazioni nel dominio cibernetico e della gestione di tutti i sistemi IT della Difesa. Disponibile su https://www.acn.gov.it /SMD_/COR/Pagine/default.aspx

[139] Dipartimento delle Informazioni per la Sicurezza (DIS), Agenzia informazioni e sicurezza esterna (AISE), Agenzia informazioni e sicurezza interna (AISI).

[140] ACN, Piano di implementazione Strategia nazionale di Cybersicurezza 2022-2026, misura #1, pag. 4, disponibile su https://www.acn.gov.it/ACN_Implementazione.pdf.

[141] *Ibidem*, misura #4

continuo e l'analisi di minacce, vulnerabilità e attacchi, secondo gli specifici ambiti di competenza" e il "r*ealizzare un servizio di monitoraggio del rischio cyber nazionale a favore delle organizzazioni e del pubblico in generale, al fine di comunicare l'effettivo livello della minaccia, nonché di informare adeguatamente i processi decisionali*".

Si è valutata inoltre la creazione di un sistema di supporto per PA e aziende[142] e di un "parco nazionale della cybersicurezza"[143] per ricerca e sviluppo.

In tema di investimenti venne deciso di destinare l'1,2% degli investimenti nazionali lordi per il finanziamento di progetti specifici finalizzati al raggiungimento di una autonomia tecnologica e l'innalzamento della sicurezza cibernetica nel sistemi informativi nazionali[144].

Sulla scia e ad integrazione di quanto sopra, in data 22 giugno 2023, di concerto con il Sottosegretario di Stato con delega alla Sicurezza e soprattutto con il Ministero dell'Università e della Ricerca (MUR), è stata promossa l'"*Agenda di Ricerca e Innovazione per la Cybersicurezza"* con lo scopo di "*far emergere, stimolare e governare gli investimenti in ricerca e innovazione nel delicato settore della cybersecurity, monitorarli nel tempo e valutarne le ricadute sulla protezione del Paese con l'obiettivo di proteggerlo e rafforzarne l'autonomia strategica*"[145].

L'innovativo progetto nasce in attuazione della già citata Strategia nazionale ed è volto ad individuare con ancora più precisione i temi prioritari di ricerca con orizzonte temporale al

---

[142] *Ibidem*, misura #33, pag. 11
[143] *Ibidem*, misura #49, pag. 15
[144] https://shorturl.at/iBFIL
[145] ACN, Agenda di Ricerca e Innovazione per la Cybersicurezza, 2023, disponibile su https://www.acn.gov.it/notizie/contenuti/l-italia-raccoglie-la-sfida-delle-tecnologie-emergenti

2026, identificando sei macro aree tematiche quali la sicurezza dei dati e della privacy, la gestione delle minacce cibernetiche, la sicurezza dei software e delle Piattaforme, la sicurezza delle infrastrutture digitali, aspetti della Società e aspetti di Governo.

Nell'intendimento dell'ACN, l'Agenda doveva tenere in considerazione l'evoluzione continua delle cosiddette Emerging and Disruptive Technology (EDT) mettendole in correlazione con le sopra riportate aree di studio ed includendo, a titolo esemplificativo, argomenti attuali quali il 5G, l' Internet of things (IOT), l'automazione, la robotica, i sistemi satellitari e la realtà virtuale mettendoli a sistema con le problematiche in esame e stimolando discussioni programmatiche[146].

8. Difesa cibernetica nazionale ed evoluzione normativa

Per ben comprendere come sia oggi strutturata l'organizzazione difensiva militare e civile in campo cibernetico nel nostro paese, ritengo sia utile fare un excursus storico della normativa nazionale in materia.

Prima di ciò va considerato che il tema della sicurezza informatica ha guadagnato la corretta attenzione solo in tempi relativamente recenti. In tema di Pubblica amministrazione, ad esempio, solo a partire dal 16 gennaio 2022, con la Direttiva del Presidente del Consiglio dei ministri recante la "Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali"[147], le informazioni trattate attraverso i sistemi informativi pubblici sono state qualificate come "risorse di valore strategico" richiedendo una adeguata protezione al fine di "*prevenire possibili alterazioni sul significato intrinseco delle*

[146] https://www.acn.gov.it/documents/agenda/it/Relazioni%20EDT%20RI.pdf
[147] Pubblicata sulla Gazzetta Ufficiale - Serie Generale n. 69 del 22 marzo 2022, disponibile su https://shorturl.at/AJZ14

informazioni stesse". La citata direttiva ha comportato, da parte della PA, un allineamento allo stato dell'arte in tema ICT imponendo l'attivazione di tutte le misure necessarie a raggiungere un livello di sicurezza tale da consentire, eventualmente, anche una progettualità convincente in tal senso.

A tale documento si è pervenuti attraverso un percorso normativo non facile composto da numerosi interventi alcuni dei quali particolarmente importanti e che verranno ora meglio descritti:

8.1 D.p.c.m. 24 gennaio 2013, "Decreto Monti".

Solo dal 2010, con la Relazione annuale al Parlamento sulla politica dell'informazione e della sicurezza[148], si è cominciato a sottolineare con fermezza il potenziale impatto della minaccia cibernetica sulla sicurezza nazionale[149]. Questa accresciuta sensibilità ha portato alla creazione di un quadro normativo ritenuto idoneo, a partire dalle modifiche alla legge 3 agosto 2007, n. 124 apportate con legge 7 agosto 2012, n. 133.

Da quel momento l'art. 1, co. 3-bis, della L. 124/2007 ha disposto che "*il Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), adotti apposite direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali*".

La stessa legge così modificata con l'art. 4, co. 3, lett. d-bis, affidava al Dipartimento delle informazioni per la sicurezza (DIS),

---

[148] Le relazioni annuali al Parlamento sono disponibili su http://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html

[149] Cfr. Mele S., I principi strategici delle politiche di cybersecurity, 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-dellepolitiche-di-cyber-security.html

il coordinamento dell'attività informativa al fine di meglio organizzare e rafforzare la protezione cibernetica a livello nazionale.

Il c.d. "Decreto Monti", d.p.c.m. 24 gennaio 2013[150], ha successivamente dato avvio alla strutturazione della difesa cibernetica attraverso l'attribuzione di funzioni e compiti tra specifici soggetti con l'obiettivo di aumentare le capacità di prevenzione, risposta e sanzione in caso di eventi dannosi. Sempre nel 2013, in applicazione dello stesso d.p.c.m., sono stati approvati il Quadro Strategico nazionale per la sicurezza dello spazio cibernetico ed il Piano Nazionale per la protezione cibernetica e la sicurezza informatica.

Tale dettato normativo, nel complesso, ha delineato finalmente in maniera organica i compiti delle articolazioni statali, fornendo specifica disciplina di dettaglio in merito alle procedure finalizzate alla riduzione delle vulnerabilità, alla prevenzione dei rischi, alla risposta tempestiva ed al ripristino immediato dei sistemi in caso di aggressione cibernetica[151].

L'infrastruttura, come organizzata, vedeva il potere decisionale incentrato nella figura del Presidente del Consiglio e dei ministri facenti parte del Comitato interministeriale per la sicurezza della Repubblica (CISR)[152]. Al CISR veniva dato il compito di elaborare la strategia nazionale in tema di

---

[150] Decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, direttiva recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", pubblicato in Gazzetta Ufficiale 19 marzo 2013, n. 66

[151] Art. 1, comma 1, del d.p.c.m. 24 gennaio 2013.

[152] Il Comitato interministeriale per la sicurezza della Repubblica è stato istituito con Legge 124/2007 art. 5, con funzioni di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza. Tale Comitato si trova presso la Presidenza del Consiglio dei ministri, presieduto dal Presidente del Consiglio con una composizione che vede la presenza del Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della Difesa, dal Ministro della Giustizia, Ministro dell'economia e delle finanze e dal Ministro dello sviluppo economico.

cybersecurity nonché definire gli indirizzi generali operativi e individuare lacune normative.

A supporto del CISR venne affiancato, ex. art. 5, il c.d. "CISR tecnico", un organismo collegiale di coordinamento presieduto dal Direttore del DIS, che si doveva occupare, tra le altre cose, della verifica dell'attuazione degli interventi previsti dal Piano nazionale per la scurezza dello spazio cibernetico come anche della formulazione di indicazioni circa le misure di sicurezza. Il d.p.c.m. istituiva inoltre presso l'ufficio del Consigliere militare del Presidente del Consiglio[153], il "Nucleo per la sicurezza cibernetica", composto da rappresentanti del DIS e delle due Agenzie operative dello stesso[154], del Ministero degli affari esteri, del Ministero dell'interno, della Difesa, dello Sviluppo economico, economia e finanze, del Dipartimento della Protezione Civile e dell'Agenzia per l'Italia digitale (AGID[155]).

Il fine di tale Nucleo era quello di supportare il Presidente del Consiglio in caso di crisi nonché di accentrare la gestione degli eventi dannosi nell'ipotesi risultassero non più gestibili dalle singole amministrazioni. Poteva, in tal caso, essere dichiarata la "*crisi cibernetica*" attraverso l'attivazione di un tavolo tecnico per la gestione della stessa con il supporto del Nucleo interministeriale di situazione e pianificazione (NISP[156]), costituito presso la

[153] Decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, direttiva recante "indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", pubblicato in Gazzetta Ufficiale 19 marzo 2013, n. 66, Art. 8, comma 1.
[154] Agenzia informazioni e sicurezza esterna (AISE) e Agenzia informazioni sicurezza interna (AISI).
[155] Agenzia per l'Italia Digitale (AGID), agenzia istituita con D.lgs. 7 marzo 2005, n. 82, art. 14-bis, "Codice dell'amministrazione digitale", pubblicato in GU n.112 del 16-05-2005 - Suppl. Ordinario n. 93.
[156] Decreto del Presidente del Consiglio dei ministri 5 maggio 2010, recante l' "Organizzazione nazionale per la gestione di crisi", pubblicato in G.U. n. 139 del 17 giugno 2010, art. 5

Presidenza del Consiglio dei ministri, competente per il supporto al Comitato Politico Strategico (CoPS[157]).

Suddetto tavolo tecnico avrebbe dovuto assicurare il coordinamento ed il corretto svolgimento delle attività di "reazione e stabilizzazione" previste per le varie amministrazioni avvalendosi a sua volta del Computer Emergency Response Team (CERT) sito presso il Ministero dello sviluppo economico.

In attuazione dell'art. 3, comma 1, del d.p.c.m. 24 gennaio 2013, con decreti del Presidente del Consiglio dei ministri del 27 gennaio 2014, sono stati successivamente adottati il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" e il "Piano nazionale per la protezione cibernetica e la sicurezza informatica".

A tal proposito il Quadro strategico venne elaborato dal Tavolo Tecnico Cyber (TTC), istituito in seno al CISR tecnico, costituito da rappresentati di vari ministeri interessati prevedendo linee strategiche di livello nazionale e orizzonte temporale di medio lungo termine, volte a fare innanzitutto un punto delle principali minacce esistenti relativamente a criminalità informatica, sfruttamento a fini terroristici delle tecnologie ICT, allo spionaggio nel cyberspazio, al c.d. "hacktivismo", al sabotaggio ed ai conflitti nella cd. "quinta dimensione".

Il documento inoltre cristallizzava sei indirizzi strategici ed undici operativi focalizzandosi sul miglioramento delle capacità tecnologiche, operative e di analisi delle istituzioni, sul potenziamento delle infrastrutture critiche nazionali, sull'incentivazione della cooperazione tra istituzioni ed imprese, sulla promozione e diffusione della cultura della sicurezza cibernetica, sul contrasto alla diffusione di contenuti illegali in rete

[157] Istituito dall'art. 4 del Decreto del Presidente del Consiglio dei ministri del 5 maggio 2010.

e sul rafforzamento della cooperazione in tema di sicurezza cibernetica.

A livello più specificatamente operativo venne posto un focus sulle capacità intelligence nazionali, sulla costituzione di una Autorità nazionale di Network and Information Security (NIS), sulla partnership tra pubblico e privato sul miglioramento dei CERT sia nazionale che della PA (CERT-PA) presso i vari dicasteri. Venne inoltre implementato il sistema integrato di Information Risk Management (IRM) per il monitoraggio e la prevenzione di crisi occorrenti su assetti strategici.

Il Piano Nazionale 2013 per la protezione cibernetica e la sicurezza informatica nazionale, allora sviluppato per il biennio 2014-2015, sviluppò gli obiettivi operativi sopra riportati nonché le relative linee d'azione marcando dunque un solco paradigmatico per il nostro paese andando a strutturare le fondamenta della difesa cibernetica nazionale.

Lo stesso non fu esente da implementazioni. Il d.l. 18 maggio 2018, N. 65, recependola, ha dato attuazione alla Direttiva UE9 2016/1148 del Parlamento europeo e del Consiglio, direttiva NIS, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi dell'Unione[158].

Con l'art. 8 del d.l. 65/2018, inoltre, venne istituito, presso la Presidenza del Consiglio dei ministri, il Computer Security Incident

[158] La direttiva NIS (Network and Information Security), indirizzata fortemente agli operatori dei servizi essenziali (OSE) quali Acqua potabile, Energia, Infrastrutture digitali, Infrastrutture del mercato bancario e finanziario, Salute e Trasporti e ai Fornitori di Servizi Digitali (FSD) come ad esempio Motori di ricerca, Servizi di cloud computing o piattaforme di commercio elettronico, fu a tutti gli effetti il primo passo della strategia europea in tema di Cybersecurity con obiettivo di rafforzare sicurezza e resilienza informativa continentale. https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148

Response Team (Csirt) assumendo compiti e competenze dei preesistenti CERT nazionale e CERT-PA.[159].

Infine il Libro Bianco per la sicurezza internazionale e la difesa, pubblicato nel 2015 dal Ministero della Difesa[160], ha evidenziato l'improrogabile necessità di dedicare capacità operative in termini difensivi al dominio cibernetico per la preservazione del "Sistema Paese" e delle strutture politiche, economiche e sociali. A tal proposito il paragrafo 32 dello stesso cita la "*particolare dipendenza dell'Occidente da un sistema di reti informatiche che sia funzionante, sicure e resiliente*".

8.2 D.p.c.m. 17 febbraio 2017, "Decreto Gentiloni".

Nel febbraio del 2017, allo scopo di razionalizzare l'architettura elaborata nel precedente decreto del 2013 e assicurare un più efficace collegamento con il CISR, viene pubblicato un nuovo d.p.c.m., il c.d. "Decreto Gentiloni"[161], al cui interno viene emanata una nuova direttiva finalizzata all'aggiornamento delle architetture istituzionali di sicurezza cibernetica e di protezione delle infrastrutture critiche.

In particolare, viene ulteriormente rafforzato il ruolo del Presidente del consiglio dei ministri[162] quale responsabile della politica generale del Governo e di vertice del Sistema di

[159] La direttiva NIS verrà successivamente aggiornata con la Direttiva europea n. 2555/2022 (direttiva NIS 2), approvata il 14 dicembre 2022 ed entrata in vigore il 17 gennaio 2023. Tale aggiornamento si è reso necessario per strutturali problemi di individuazione dei cd. servizi essenziali in fase di recepimento a livello nazionale e soprattutto a seguito della "lesson learned" durante la pandemia.
[160] Ministero della Difesa, Libro Bianco per la sicurezza internazionale e la difesa , 2015, https://www.analisidifesa.it/wp-content/uploads/2015/04/Libro-Bianco-2015.pdf
[161] Decreto del Presidente del Consiglio dei ministri 17 febbraio 2017, Pubblicato in GU n. 87 del 13 aprile 2017, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali".
[162] *Ibidem* 17 febbraio 2017, art. 3, comma 1

Informazione per la sicurezza della Repubblica (SISR) anche nello spazio cibernetico. Il CISR, in occasione di una crisi, avrebbe avuto funzione di consulenza e proposta in materia di sicurezza nazionale[163] come nel precedente decreto del 2013 ma la nuova normativa, in ossequio alla riconfigurazione avvenuta nel già citato d.l. 174/2015[164], innovò circa le peculiari funzioni di deliberazione nei casi di crisi che raggiunga una soglia di pericolo per la sicurezza nazionale.

In merito al SISR, il suo vertice, nella persona del Direttore generale, ha ora competenza nell'"*adottare le iniziative idonee a definire le necessarie linee di azione per innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti, perseguendo, in particolare, l'individuazione e la disponibilità dei più adeguati e avanzati supporti tecnologici in funzione della preparazione alle azioni di prevenzione, contrasto e risposta in caso di crisi cibernetica*" [165].

Presso il Dipartimento da lui diretto, e dunque non più presso l'Ufficio del Consigliere militare, è ora ubicato oltre al CISR[166] anche il Nucleo per la sicurezza cibernetica[167].

La ridislocazione di queste articolazioni segue l'intendimento della nuova direttiva nel trovare un maggiore coordinamento con le strutture istituzionali previste nel nuovo quadro strategico.

---

[163] *Ibidem*, art. 4, comma 1, let. a)
[164] Decreto-legge 30 ottobre 2015, n. 174, convertito con modificazioni, dalla legge di conversione 11 dicembre 2015, n. 198 "Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione", pubblicato nella G.U. n. 253 del 30 ottobre 2015.
[165] *Ibidem*, art. 6
[166] in seguito alla nuova dislocazione, il Consigliere militare del Presidente del Consiglio non partecipa più alle riunioni di CISR e CISR tecnico, come invece previsto dal precedente "decreto Monti".
[167] *Ibidem*, art. 8

Nello specifico il Nucleo in caso di crisi non attiva più il NISP, ma, una volta attivate le azioni di raccordo e coordinamento, supporta tempestivamente il Presidente del consiglio circa le competenze dello stesso ex. art. 7-bis, comma 5, del d.l. 174/2015[168].

In generale il Tavolo interministeriale di crisi cibernetica, come da previsione del decreto "Monti", termina di essere identificato presso il NISP e la gestione delle crisi di carattere cibernetico rimangono completamente affidate al Nucleo che viene altresì integrato da rappresentati del Ministero della Salute, del Infrastrutture e dei trasporti, del Dipartimento dei Vigili del fuoco, del soccorso pubblico e della difesa civile, della Commissione interministeriale tecnica di difesa civile (CITDC). Possono partecipare, in considerazione dell'evento dannoso occorso, oltre ai rappresentanti dell'Ufficio del consigliere militare, anche altre amministrazioni o enti locali che vengono autorizzati ad assumere decisioni per le amministrazioni di competenza, nonché' operatori privati eventualmente interessati[169].

Il Nucleo per la sicurezza cibernetica riceve e dirama inoltre eventuali segnalazioni estere e valuta la sostenibilità degli attacchi da parte delle singole amministrazioni intervenendo, su esigenza, a livello interministeriale e provvede ad informare il Presidente del Consiglio, per il tramite del Direttore generale del DIS, sulla gestione dell'eventuale crisi in atto. Si evidenzia, come già visto,

---

[168] d.l. 174/2015, art. 7-bis "disposizioni in materia di intelligence".

[169] Circa gli operatori privati ammessi alle riunioni del NISP viene fatta descrizione all'art. 11 del Decreto: "operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di servizi digitali (di cui alla direttiva NIS) quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici"

una maggiore presenza del Dipartimento delle Informazioni per la sicurezza, nel flusso di coordinamento.

Successivamente, con d.p.c.m. del 31 marzo 2017, viene emanato un nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica nel quale vengono rivisti gli obiettivi operativi, tra cui in particolar modo il potenziamento delle capacità intelligence, di polizia e difesa sia civile che militare e l'operatività delle strutture di incident prevention, response e remediation.

A livello militare il piano ha istituito il Comando Interforze per le operazioni Cibernetiche (CIOC), Comando, di spettro interforze, specializzato nel mondo Cyber. Tale comando da subito ha acquisito competenza circa la protezione delle reti della Difesa e per l'innovativa realizzazione di un poligono virtuale nazionale presso la Scuola telecomunicazioni delle Forze Armate di Chiavari (GE)[170] divenuta polo formativo Cyber dello Stato Maggiore della Difesa.

8.3 D.l. 21 settembre 2019, n. 105, perimetro di sicurezza cibernetica

Il Decreto-legge 21 settembre 2019, n. 105[171] ha ulteriormente rivisto l'assetto strutturale della sicurezza cibernetica andando ad adottare il cosiddetto "*perimetro di sicurezza cibernetica*", oggetto dello stesso Decreto. Il decreto va a toccare un ampio spettro di materie quali il tema del

[170] https://www.difesa.it/SMD_/EntiMI/STELMILIT/Pagine/UNAVOX.aspx
[171] Decreto-legge 21 settembre 2019, n. 105 recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito con modificazioni dalla L. 18 novembre 2019, n. 133, pubblicato in G.U. 20/11/2019, n. 272

procurement, del c.d. "golden power"[172], e le infrastrutture reputate strategiche.

Per "perimetro" si intende, ex. art. 1, comma 1, l'insieme "*delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, può derivare un pregiudizio per la sicurezza nazionale*".

Per garantire la sicurezza vengono seguite due direttrici principali: da una parte reti, sistemi informativi e servizi informatici da censire annualmente in base ad indicatori definiti dal CISR tecnico[173], dall'altra l'adozione di misure che garantiscano livelli elevati di sicurezza[174] sulla base di politiche di sicurezza, struttura organizzativa e gestione del rischio, gestione e prevenzione degli incidenti, protezione logica e fisica dei dati, integrità delle reti, continuità del servizio, test e controlli, formazione e consapevolezza, definizione di caratteristiche generali per l'affidamento di forniture di beni e servizi ICT.

Interessante, inoltre, il fatto che l'art. 5 del decreto preveda la possibilità da parte del Presidente del consiglio di disporre, su deliberazione del CISR, la disattivazione, totale o parziale, di uno

---

[172] esercizio di poteri speciali come da previsione di cui al d.l. 15 marzo 2012, n. 21

[173] Decreto-legge 21 settembre 2019, n. 105 recante "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito con modificazioni dalla L. 18 novembre 2019, n. 133, pubblicato in G.U. 20/11/2019, n. 272, art. 1, comma 2, let. b)

[174] *Ibidem*, art. 1, comma 3, let. b)

o più elementi impiegati nelle reti, nei sistemi o per l'espletamento dei servizi[175].

I presupposti per l'attivazione di un tale dispositivo sono il trovarsi in un "*rischio grave e imminente per la sicurezza nazionale*", che il provvedimento sia temporalmente limitato a quanto "*strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione*" e che risponda al criterio di proporzionalità.

Ponendo le previsioni descritte in relazione con l'istituto della legittima difesa, appare curioso il fatto che, come evidenziato da alcuni esperti, nonostante la disattivazione di un apparato di rete sia una tipica misura di difesa "passiva", la citazione del criterio della proporzionalità sembrerebbe consentire un possibile contrattacco. L'art. 5 viene infatti giudicato come "*impeccabile sotto il punto di vista della tecnica di redazione normativa*" riuscendo sia a specificare il campo d'azione sia a lasciare spazio ad ogni eventuale possibilità, anche attiva[176].

8.4 D.l. 14 giugno 2021, n. 82: istituzione dell'ACN.

Uno degli eventi più importanti per l'infrastruttura difensiva nazionale in tema di sicurezza cibernetica è avvenuto nel 2021 con l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN) a mezzo decreto-legge 14 giugno 2021, n. 82, convertito con modificazioni nella legge 4 agosto 2021, n. 10[177].

---

[175] *Ibidem*, art. 5.

[176] cfr. MELE S., Sicurezza nazionale ICT, perché il decreto sul Perimetro farà la differenza, in Agenda digitale, 2019 disponibile su https://www.agendadigitale.eu/sicurezza/sicurezza-nazionale-ict-perche-il-decreto-sul-perimetro-fara-la-differenza/

[177] Legge 4 agosto 2021, n. 109, recante "Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale", pubblicata in G.U. del 4 agosto 2021, n. 185, disponibile su https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2021-08-04;109

L'istituzione dell'Agenzia deriva in particolar modo da quanto recepito nel 2018[178] con direttiva (UE) 2016/1148, in merito alle misure da adottare per garantire la sicurezza di reti e soggetti competenti.

Dopo l'istituzione del perimetro di sicurezza nazionale, con decreto-legge 105 del 2019[179], la sicurezza cibernetica ha trovato forte attenzione anche nel Piano nazionale di ripresa e resilienza (PNRR) del 2021, nell'ambito della digitalizzazione della pubblica amministrazione, andando a formare uno dei 7 punti cardine degli investimenti in tal senso[180].

Quanto sopra al fine di garantire un rafforzamento delle infrastrutture difensive strategiche nazionali, obiettivo che ha visto l'apice nell'art. 5 del Decreto-legge 82/2021 istituente l'Agenzia per la cybersicurezza nazionale "*a tutela degli interessi nazionali nel campo della cybersicurezza, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico*". Il decreto ha previsto inoltre l'onere, per il Presidente del Consiglio dei ministri, di trasmettere al Parlamento due relazioni annuali sull'attività dell'Agenzia: la prima entro il 30 aprile per l'attività svolta specificatamente in materia di cybersicurezza, la seconda entro il 30 giugno al COPASIR[181] per le attività svolte in raccordo con il SISR.

---

[178] d.l. 18 maggio 2018, n. 65, attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione. Disponibile su https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-05-18;65

[179] Integrato dal d.l. 162 del 2019 relativamente a proroga dei termini e disposizioni per la P.A..

[180] La digitalizzazione della PA è stata prevista dal PNRR nella Componente 1 (Digitalizzazione, innovazione e sicurezza nella PA) della Missione 1 (Digitalizzazione, innovazione, competitività, cultura e turismo).
https://www.governo.it/it/approfondimento/digitalizzazione-innovazione-competitivit-e-cultura/16701

[181] COPASIR, Comitato parlamentare per la sicurezza della Repubblica, organo del Parlamento deputato al controllo sull'operato degli organismi informativi

A tal proposito va specificato che nonostante l'Agenzia sia *de facto* braccio operativo del Sistema di informazione per la Sicurezza e ricada nelle competenze del Presidente del Consiglio, non è ad oggi parte del Sistema stesso, rimanendo invariata la struttura prevista dalla L. 124/2007.

Possiamo infatti affermare che l'operato dell'Agenzia risulta assimilabile a quanto previsto al secondo comma dell'art. 8 della legge stessa per il II reparto dello Stato Maggiore della Difesa[182]. Nel complesso l'ACN, a mente dell'art. 7 del d.l. istitutivo, esercita le funzioni di Autorità nazionale in materia di cybersecurity, sviluppa le capacità di prevenzione, monitoraggio, rilevamento e mitigazione degli incidenti di sicurezza informatica, contribuisce all'innalzamento della sicurezza dei sistemi utilizzati dai facenti parte del perimetro di sicurezza nazionale cibernetica (tra cui operatori OSE e fornitori FSD), supporta lo sviluppo di competenze industriali, tecnologiche e scientifiche, è interlocutore unico a livello nazionale, per pubblico e privato, in materia di sicurezza delle reti.

In data 1° settembre 2022, con decreto del Presidente del Consiglio dei ministri, ex art. 7., comma 1, lettera m) del d.l. 82/2021[183], l'Agenzia assume tutti i compiti ex art. 51 del Codice

---

facenti parte del sistema di informazione per la sicurezza della Repubblica, come da previsione normativa della L. 3 agosto 2007, n. 124, legge di riforma degli apparati intelligence nazionali e del segreto di stato.

[182] Ai sensi dell'articolo 8, comma 2, della legge 3 agosto 2007, n. 124 "Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto" riporta che "il Reparto informazioni e sicurezza dello Stato maggiore della difesa (RIS) svolge esclusivamente compiti di carattere tecnico militare e di polizia militare, e in particolare ogni attività informativa utile al fine della tutela dei presidi e delle attività delle Forze armate all'estero, e non è parte del Sistema di informazione per la sicurezza".

[183] "*assume tutte le funzioni in materia di cybersicurezza già attribuite all'Agenzia per l'Italia digitale dalle disposizioni vigenti e, in particolare, quelle di cui all'articolo 51 del decreto legislativo 7 marzo 2005, n. 82, nonché' quelle in materia di adozione di linee guida contenenti regole tecniche di*

dell'Amministrazione digitale (CAD)[184], adottando le linee guida contenenti le regole tecniche ex. art 71 del CAD, qualificando i servizi cloud della PA, subentrando all'AgID ed assumendo le funzioni attribuite alla Presidenza del Consiglio in materia di perimetro di sicurezza nazionale cibernetica[185].

8.5 D.l. 9 agosto 2022, n. 115

Ultima importante evoluzione in materia è rappresentata dal Decreto-legge 9 agosto 2022, n. 115, recante "Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali"[186]. L'articolo 37 ha inserito nel Decreto-legge 30 ottobre 2015[187] di proroga delle missioni internazionali delle Forze armate e di polizia, l'articolo 7-ter specifico per l'ambito cibernetico riportando che "*Il Presidente del Consiglio dei ministri, acquisito il parere del Comitato interministeriale per la sicurezza della Repubblica e sentito il Comitato parlamentare per la sicurezza della Repubblica, emana, ai sensi dell'articolo 1,*

---

cybersicurezza ai sensi dell'articolo 71 del medesimo decreto legislativo. L'Agenzia assume, altresì, i compiti di cui all'articolo 33-septies, comma 4, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, già attribuiti all'Agenzia per l'Italia digitale".

[184] Decreto-legislativo 7 marzo 2005, n. 82, Codice dell'amministrazione digitale, aggiornato da ultimo dal d.l. 24 febbraio 2023, n. 13 convertito con modificazioni con L. 21 aprile 2023, n. 41, in G.U. del21 aprile 2023, n. 94

[185] decreto-legge 14 giugno 2021, n. 82, recante Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, in G.U. del 4 agosto 2021, n. 185, art. 7, comma 1, lettera h)

[186] Decreto-legge 9 agosto 2022, n. 115, convertito con modificazioni dalla l. 21 settembre 2022, n. 142, recante "Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali", in G.U. del 09 agosto 2022 n. 185, disponibile su https://www.normattiva.it/urires/N2Ls?urn:nir:stato:decreto.legge:2022-08-09;115

[187] Decreto-legge 30 ottobre 2015 n. 174, recante la "Proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione", in. G.U. del 30 ottobre 2015 n. 253, disponibile su https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2015-10-30;174

comma 3, della legge 3 agosto 2007, n. 124, disposizioni per l'adozione di misure di intelligence di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale".

Il comma 2 conferma ad ogni modo che le misure eventualmente adottate in difesa degli interessi di cui all'art. 17, comma 2, della legge 124/2007, vengono prese "*secondo criteri di necessità e proporzionalità*".

Molto importante inoltre quanto confermato ai commi 1 e 5 in merito alla cooperazione con il Ministero della difesa, la cui architettura cyber verrà meglio dettagliata nel prossimo paragrafo, e soprattutto in merito alle garanzie funzionali del personale impiegato, aspetto caratterizzato da una storica mancanza di copertura normativa fatte salve le previsioni per il personale facente parte del Sistema di informazione per la sicurezza della Repubblica[188].

9. Architettura militare cyber nazionale

Nel corso del Summit tenutosi a Varsavia nel mese di luglio 2016, la Nato ha ufficialmente riconosciuto lo spazio cibernetico quale dominio nel quale difendersi con la stessa efficacia con cui ci si difende in aria, sulla terraferma ed in mare[189]. Sembrerebbe

[188] art. 37, comma 5 del Decreto-legge 9 agosto 2022, n. 115,: "Al personale delle Forze armate impiegato nell'attuazione delle attività di cui al presente articolo si applicano le disposizioni di cui all'articolo 19 della legge 21 luglio 2016, n. 145, e, ove ne ricorrano i presupposti, all'articolo 17, comma 7, della legge n. 124 del 2007".

[189] NATO, Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016, 9 July 2016, § 70: «[…] we reaffirm Nato's defensive mandate and recognise cyberspace as a domain of operations in which Nato must defend itself as effectively as it does in the air, on land, and at sea».

dunque confermata la prassi di definire come quinto dominio di operazioni lo spazio cibernetico successivo a quello spaziale. In verità, nonostante sia ormai di uso comune, non è ancora possibile definire militarmente lo spazio come dominio. Ciò che infatti caratterizza un dominio, militarmente inteso, è la disponibilità di capacità militari specifiche per operarvi.

Già nel 2014, nel precedente Summit del Galles[190] era stata approvata l'"*Enhanced Cyber Defence Policy*" in base alla quale la NATO riconosceva l'applicabilità del diritto internazionale, come anche del diritto internazionale umanitario e della Carta ONU, allo spazio cibernetico nonché la difesa cibernetica come "core task" della difesa collettiva dell'Alleanza. Concetti oltremodo ribaditi nel 2018 durante il Summit Nato di Bruxelles dell'11 e 12 luglio[191].

Quanto sopra per delineare l'alveo in cui conseguentemente si è mosso il nostro Ministero della Difesa in tema di difesa cibernetica.

Seppur né nel Codice dell'ordinamento militare[192] né nel successivo Libro Bianco[193] del 2015 si parla di specifici compiti di protezione del Cyberspazio[194], già nel Quadro Strategico nazionale cyber del 2013 vengono attribuiti alla Difesa compiti di difesa e coordinamento in tal senso, conduzione di *Computer Network*

---

[190] NATO, Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014, § 72-73, disponibile su https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[191]Nato, Brussels Summit Declaration, § 20.

[192] Decreto-legislativo 15 marzo 2010, n. 66

[193] Nel Libro Bianco, ed. 2015, al § 81 vengono delineati, da parte del Capo di Stato Maggiore della Difesa, quattro specifiche missioni per le forze armate quali la difesa dello Stato, degli spazi euro-atlantici ed euro-mediterranei, il contributo alla realizzazione della pace e della sicurezza internazionali, i concorsi e compiti specifici delle FF.AA. in relazione anche ad esigenze particolari quali calamità o eventi straordinari.

[194] Cosa che sembrerebbe non combaciare con quanto previsto dal legislatore che con l. 133/2012, di modifica della L. 124/2007, ha attribuito al SISR, nel DIS in primis, specifiche funzioni di protezione cyber.

Operations (CNO) e apporto informativo verso gli organismi intelligence ex. L. 124/2007.

In ogni caso il citato Libro Bianco, al paragrafo 68, riporta il progetto di "*sviluppare, in piena armonia con la strategia nazionale sulla protezione informatica, le possibilità di difesa contro attacchi di natura cibernetica che dovessero eccedere le capacità predisposte dalle agenzie civili*".

Si può affermare che l'architettura cibernetica militare in Italia sia incentrata in uno specifico luogo: il Comando per le Operazioni in Rete (COR)[195]. Strutturato in tre divisioni principali (C4, Security e Cyber Defence, *Cyber-operations*), dipende direttamente dal Capo di Stato Maggiore della Difesa ed è deputato alla condotta delle operazioni nel dominio cibernetico, la gestione tecnico-operativa in sicurezza di tutti i sistemi ICT/C4 della Difesa, l'armonizzazione e la distribuzione dei flussi informativi derivanti dai sistemi di comando e controllo, computing e per Intelligence, Surveìllance & Reconnaisance (ISR), la gestione unica della rete Difesa. È inoltre deputato alla difesa di tale rete attraverso il CERT del dicastero e i dipendenti Security Operation Center (SOC), Network Operation Center (NOC) e Infrastructure Operation Center (IOC).

Nato nel 2020 dall'aggregazione di due preesistenti comandi quali il C4 Difesa ed il Comando per le Operazioni Cibernetiche (CIOC), a seguito del Gruppo di Progetto C5ISR "Riorganizzazione e razionalizzazione del settore Cyber", dal luglio 2021 è stato posto alle dipendenze, assieme al Comando per le Operazioni delle Forze Speciali e al Comando delle operazioni Spaziali, del Comando Operativo di Vertice Interforze (COVI).

[195] Comando per le operazioni in Rete (COR), https://www.difesa.it/SMD_/COR/Pagine/default.aspx

Già come in precedenza il CIOC[196], il COR si relaziona con AISE e AISI, per il tramite del II Reparto Informazioni e Sicurezza dello SMD[197], per supporto di tipo tecnico-militare.

In caso di incidente cibernetico le forze armate colpite, che dispongono di Security Operation Center (SOC) "proprietari" e di propri Computer Incident Response Team (CIRT), hanno competenza autonoma di reazione mentre nel caso di incidenti cosiddetti "cross-domain" interviene il COR che assume controllo e il coordinamento.

L'incidente viene comunicato all'autorità giudiziaria che può a sua volta delegare le indagini alla forza armata interessata o alla Polizia di Stato per il tramite del Cnaipic[198]. Successivamente il CERT Difesa, presso il COR, informa il Nucleo di sicurezza cibernetica presso il DIS che, in casi particolarmente critici, attiva CISR e CISR tecnico.

Va specificato che, come già previsto dal d.p.c.m. Gentiloni del 2017[199], la componente militare non ha competenza su reti private, civili o di altre amministrazioni pubbliche o ancora degli operatori o fornitori di servizi essenziali, come da direttiva NIS e ora NIS 2.

---

[196] Il CIOC, successivamente inglobato nel COR, era stato nel 2019 oggetto di un protocollo d'intesa tra il comparto intelligence e la Difesa al fine di meglio armonizzare i flussi informativi in tal senso (cfr. Camera dei Deputati, Documentazione e ricerche n. 83, Dominio cibernetico, nuove tecnologie e politiche di sicurezza e difesa cyber, 24 settembre 2019, p. 68).

[197] Il quale come da art. 8, c.2 della l. 124/2007 si occupa delle attività informative utili al fine della tutela dei presidi e delle attività delle forze armate all'estero, in stretto collegamento con l'AISE pur non facendo parte del SISR.

[198] Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC), unità specializzata della Polizia Postale e delle comunicazioni istituita nel 2005 per prevenzione e la repressione dei crimini informatici diretti alle infrastrutture critiche nazionali. https://www.interno.gov.it/it/temi/sicurezza/crimine-informatico/centro-nazionale-anticrimine-informatico-protezione-infrastrutture-critiche-cnaipic

[199] Decreto del Presidente del Consiglio dei ministri del 31 marzo 2017 con cui viene adottato il Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, disponibile su https://www.governo.it/sites/governo.it/files/DPCM_20170317_2.pdf.

In ogni caso, giuridicamente parlando, la difesa cibernetica militare viene limitata alla componente ICT colpita non essendo possibile ai sensi dell'art. 615-ter del Codice penale[200] introdursi in un sistema informatico protetto, contro la volontà del titolare.

A tal proposito, in ottica di poter fare di più, giova evidenziare come già tra il 2016 e il 2017, dunque antecedentemente il successivo sviluppo dell'articolazione militare in materia, la IV Commissione Difesa della Camera dei Deputati, ha esperito una indagine conoscitiva sulla sicurezza dello spazio cibernetico riportando, come risultato finale, che al fine di far fronte ad attacchi cibernetici potenzialmente distruttivi andasse sviluppata una capacità CNO (computer network operations) "oriented" da basare su una "triplice articolazione di operazioni di difesa attiva (computer network defence o CND), raccolta informativa (Computer Network Exploitation o CNE) e attacco (Computer Network Attack o CNA)"[201] da supportare con un adeguato tappeto normativo che possa legittimare operazioni con baricentro spostato verso un atteggiamento attivo.

È viva dunque la consapevolezza della necessità di un regime di deroga a protezione legale delle CNO e specificatamente per le

---

[200] Codice Penale, art. 615 ter: "accesso abusivo ad un sistema informatico o telematico": "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni" e "Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni."

[201] Cfr. proposta di documento conclusivo dell'indagine conoscitiva sulla sicurezza e la difesa nello spazio cibernetico allegata al resoconto stenografico della seduta del dicembre 2017, p. 36, disponibile su http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/pdf/04/indag/c04_cibernetico/2017/12/20/leg.17.stencomm.data20171220.U1.com04.indag.c04_cibernetico.0010.pdf

CNA andando possibilmente a definire chiare "regole d'ingaggio"[202].

Ulteriore aspetto meritevole di valutazione è l'attribuzione di funzioni specificatamente cyber a favore della componente militare oggetto di innumerevoli discussioni e di disegni di legge. Gli unici documenti in tal senso sono quelli che presentati nel corso della XVII legislatura dal 2013 al 2018.

Il primo disegno di legge[203] prevedeva la costituzione di uno specifico Comando cibernetico (il Comando Operativo Cibernetico Interforze (COCI), alle dirette dipendenze dello Stato Maggiore della Difesa e dedicava un capo alle contromisure cibernetiche definite quali "*azioni mirate alla risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale, effettuate al fine di eliminare la situazione di crisi*" [204].

Il disegno di legge collocava le contromisure al di fuori dello stato di guerra e le sottoponeva al rispetto dei principi ex art. 11 Cost., del diritto internazionale generale, del diritto internazionale umanitario e del diritto internazionale penale.

L'art. 22 del disegno di legge prevedeva anche di estendere le garanzie funzionali tipiche del personale del SISR[205] agli operatori che si fossero trovati ad adottare misure, comunque, di volta in volta autorizzate.

Si trattava dunque di applicare al personale in forza allo Stato Maggiore della Difesa le c.d. "speciali cause di giustificazione" per condotte normalmente previste come reato ad eccezione delle

---

[202] *Ibidem*, p. 37
[203] Proposta di legge A.C. 3544, a firma Artini, presentata il 19 gennaio 2016 alla Camera e poi ritirata il 12 settembre 2017, disponibile su https://www.camera.it/leg17/126?idDocumento=3544
[204] *Ibidem*, art. 2, co. 1, let. i)
[205] Come previsto dall'art. 17, L. 124/2007

casistiche previste dagli artt. 5 e seg. del trattato istitutivo della Corte penale internazionale[206].

Un successivo disegno di legge[207] definì ogni attacco "*volto a minacciare il funzionamento e l'integrità della rete informatica e delle infrastrutture informatizzate critiche di interesse nazionale*" oggetto di interesse militare[208].

Veniva previsto inoltre che nella relazione annuale al Parlamento il Ministro includesse anche "*l'evoluzione e le prospettive della minaccia cibernetica alla sicurezza nazionale*"[209]. Un ulteriore tentativo avvenne con proposta di legge A.C. 4633[210], concernente l'istituzione del Comando interforze operazioni cibernetiche (CIOC), e l'autorizzazione, a favore delle FF.AA., circa l'"*uso e alla gestione delle contromisure cibernetiche*" nonché' lo "*sviluppare programmi di contromisure cibernetiche finalizzati alla verifica della funzionalità dei sistemi di difesa cibernetica*" confermando ancora una volta l'attenzione per il tema delle garanzie funzionali.

A tal proposito è interessante segnalare come anche in Francia sia stata prevista una "*excuse penale*"[211] per il personale militare impegnato in operazioni informatiche. Tale scriminante risulta essere posta in "positivo" essendo limitata solo ai reati connessi all'accesso a sistemi di terzi a differenza della nostra legge 124/2007 che prevede, all'art. 17, scriminate tutte le condotte tranne quelle vietate dalla legge stessa, dunque una impostazione

[206] Genocidio, crimini contro l'umanità, crimini di guerra, crimini di aggressione.
[207] Progetto di legge A.C. 3677, "Norme in materia di difesa dello spazio cibernetico e istituzione del sistema nazionale di sicurezza cibernetica", a firma Artini, presentato il 15 marzo 2016 ed avviato alla Commissione Difesa nel 2017.
[208] *Ibidem*, art. 1, comma 2.
[209] *Ibidem*, art. 8
[210] Proposta di legge 4633, a firma Artini ed altri, presentata il 7 settembre 2017, concernente l'"Istituzione del sistema nazionale di sicurezza cibernetica".
[211] Emendamento al Code de le defense del 2005, avvenuto grazie all'art. 35 della Loi de programmation militaire 2019-2025.

"in negativo" [212]. La formulazione italiana non ha mancato di sollevare dubbi circa l'eccessiva portata della copertura legale, anche in memoria dei c.d. "servizi deviati".

Nella prospettiva di dare definizione ad una base normativa che consenta agli operatori cibernetici di operare in serenità anche nel caso di una difesa più attiva, sarebbe forse preferibile adottare la linea francese al fine di meglio definire il perimetro di copertura entro cui operare, sposare la tassatività e la determinatezza tipici dell'ordinamento penale ed evitare ataviche polemiche andando dunque ad indicare, in positivo, le fattispecie di reato ritenute da scriminare.

Tale ipotesi, in considerazione del ventaglio di casistiche diverse potenzialmente occorrenti nonché dalla necessità di un intervento in difesa che sia il più tempestivo possibile, risulta comunque difficilmente realizzabile. Ad oggi la soluzione utilizzata in caso di specifiche operazioni rimane quella di assorbire, temporaneamente, il personale militare presso le Agenzie di intelligence garantendo pro tempore la copertura ex l. 124/2007.

10. Cyberspazio e organizzazioni internazionali

Le organizzazioni internazionali hanno da sempre cercato il raggiungimento di obiettivi di interesse comune difficilmente ottenibili in autonomia dai singoli Stati, anche in cambio di una devoluzione di sovranità degli stessi. Gli obiettivi tipici di queste realtà, come la pace, sono stati adattati alle nuove esigenze o attraverso la creazione di nuove organizzazioni, o tramite l'aggiornamento dello statuto originario o tramite la creazione di organi interni specializzati.

---

[212] AMATO G., Le garanzie funzionali per gli 'operatori' di Intelligence (1a parte), in Gnosis, Vol. 3, 2011, disponibile su http://gnosis.aisi.gov.it/gnosis/Rivista28.nsf/ServNavig/11.

Non stupisce il fatto che come la rete abbia avuto una evoluzione come mai nessun altro fenomeno nella storia, allo stesso tempo le minacce cibernetiche hanno avuto la stessa capacità evolutiva conservando però la necessità di non avere una prevedibilità al fine di non affievolire l'impatto dannoso.

In quest'ottica va compreso come si siano mosse negli anni le organizzazioni internazionali alla luce del problema *cybersicurezza*.

L'Organizzazione delle Nazioni Unite, in questo senso, è stata pionieristica pur dovendo segnalare che ancora oggi sembrerebbe mancare una visione unitaria in materia[213]. Il termine più corretto è sicuramente "frammentazione", fenomeno dovuto al numero di organizzazioni esistenti e, all'interno di ognuna di esse, della stratificazione di uffici.

Tralasciando la cybersicurezza ed andando più in generale nel mondo della sicurezza e dell'informazione ritengo sia esplicativo ricordare l'atavica gelosia dei paesi, anche alleati, in ambito intelligence, cosa che ha sempre comportato l'impossibilità di creare una reale struttura di intelligence europea.

Allo stesso modo la cyber eredita nel DNA la medesima diffidenza nello scambiare informazioni come anche procedure in particolar modo in ambito NATO.

L'Organizzazione delle Nazioni Unite si è principalmente espressa attraverso risoluzioni approvate dall'Assemblea Generale ma non dal Consiglio di Sicurezza portando a documenti non vincolanti. Fra questi possiamo citare la A/RES/53/70 "*Developments in the field of information and telecommunications*

[213] MAURER T., Cyber norm emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security, Cambridge (MA), 2016, disponibile su https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security

in the context of international security"[214] del dicembre del 1998, adottata su iniziativa della Federazione Russa al fine di una più proficua collaborazione in riferimento al cyberspazio. Sulla falsariga di quest'ultima il tema del cyber crime, come quello dell'uso illecito di tecnologie ICT, è stato più volte ripreso[215] al punto da portare tre comitati dell'Assemblea Generale, il Comitato per il Disarmo e la sicurezza internazionale[216], il comitato Economico e finanziario[217] ed il comitato sociale, umanitario e culturale[218] a studiare possibili risoluzioni in tema di cyber security.

In particolar modo il Comitato per il Disarmo e la sicurezza internazionale ha visto una forte partecipazione di attori quali Stati Uniti ma anche Cina e Russia.

Accanto alle formazioni internazionali quali ONU, NATO o Enisa, che verranno meglio descritte nei paragrafi successivi, giova citare alcune specifiche realtà a conferma della già citata eterogeneità' organizzativa.

Si cita, ad esempio, la "*Association of southeast Asian Nations*" (Asean)[219] istituita negli anni 60 del secolo scorso, con una formazione attuale di 10 stati membri[220] e l'intento di

---

[214] Assemblea generale, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/53/70 del 4 gennaio 1999, disponibile su https://digitallibrary.un.org/record/265311#record-files-collapse-header

[215] Assemblea generale, Combating the criminal misuse of information technologies, UN Doc. A/RES/55/63 del 22 gennaio 2021, disponibile su https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[216] Assemblea generale, Disarmament and International Security (First Committee), disponibile su https://www.un.org/en/ga/first/index.shtml.

[217] Assemblea generale, Economic and Financial Committee (Second Committee), disponibile su https://www.un.org/en/ga/second/index.shtml

[218] Assemblea generale, Social, Humanitarian & Cultural Issues (Third Committee), disponibile su https://www.un.org/en/ga/third/index.shtml.

[219] https://asean.org/

[220] Singapore, Filippine, Indonesia, Malesia, Thailandia, Brunei, Vietnam, Birmania, Laos, Cambogia

mantenere la stabilità pacifica nell'area di competenza degli stessi stati.

Va detto che tale associazione è stata pionieristica in materia andando già verso la fine degli anni 90 ad affrontare le tematiche del cyber spazio e più specificatamente del crimine in ambito cibernetico e transnazionale. In particolar modo, in seno all'ASEAN, degno di nota è l'ASEAN REGIONAL FORUM (ARF) di cadenza annuale con partecipazione estesa a Stati Uniti, Russia, Cina come anche l'Unione Europea stessa[221]

Tra le varie organizzazioni facenti parte del bacino NATO ritengo interessante citare la "Shanghai Cooperation Organisation" (SCO) istituita nel 2001 e particolarmente sensibile in materia di sicurezza delle informazioni nonché importante osservatorio nei confronti della Russia in considerazione dell'impronta sovietica nel controllo del comportamento e delle informazioni[222], tornata attuale nel cyberspazio e già preannunciata, in toni allarmistici, in pubblicazioni di più di 10 anni fa[223].

A tal proposito la Russia è da sempre stata oggetto di studio in materia di strategia comunicativa forte della storica impronta sovietica. La Russia più che di cyberspace fa riferimento all'Information-Space, uno spazio comprendente sia l'informatica che l'elaborazione delle informazioni umane ovvero un dominio antico quanto attuale e che per certi versi viene richiamato

[221] v. https://ccdcoe.org/incyder-articles/asean-regional-forum-reaffirming-the-commitment-to-fight-cyber-crime/
[222] A proposito di controllo sociale storico ed in particolar modo del modus operandi della Germania Est e della STASI, v. GARTON T. A., il dossier, 2017
[223] GILES K., Russia's Public Stance on Cyberspace Issues, Oxford UK, 2012, disponibile su https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf

nell'approccio di tipo multi dominio del nostro ministero della Difesa[224].

A tal proposito risulta interessante considerare che la sfera cognitiva dell'information warfare russa è assolutamente attuale quanto storica. Attuale nella forma di propaganda e contropropaganda a mezzo social, storica nel concetto sovietico del "*reflexive control"* o controllo della reazione di origine marxista-leninista secondo cui "*la cognizione risulta dal riflesso del mondo materiale nella mente umana, che determina la coscienza sociale. L'intelligenza dell'uomo ed i processi cognitivi dipendono dalla sua conoscenza sensoriale del mondo esterno, che a sua volta determina il contenuto e le dimensioni della sua consapevolezza*"[225].

Altra organizzazione regionale residente a livello occidentale con intensa produzione in tema di sicurezza cyber è l'Organizzazione degli Stati Americani (OAS), nata a margine del secondo conflitto mondiale[226]. Tale organizzazione per il tramite del Comitato Interamericano contro il terrorismo (Cicte), con l'adozione del cyber security program si è impegnata nell'implementazione delle agende politiche in tema di sicurezza informatica[227].

Va compreso come in ambito ONU sia forte la sensibilità nella difesa delle proprie strutture informative anche in considerazione del fatto che un suo membro permanente, quindi con capacità di

---

[224] MINISTERO DELLA DIFESA - Stato Maggiore della Difesa Titolo: "Approccio della Difesa alle Operazioni Multidominio", Roma, 2022, disponibile su https://www.difesa.it/SMD_/Staff/Sottocapo/UGID/Documents/Concetto_Approccio_Difesa_alle_Operazioni_Multidominio_2022.pdf

[225] CRISTADORO N., La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea, 2022

[226] Organization of American States (OAS), disponibile su http://www.oas.org/en/about/who_we_are.asp

[227] https://www.oas.org/en/topics/cyber_security.asp

penetrazione dall'interno, si sia reso protagonista di una crisi inedita quale quella russo ucraina.

10.1 Unione europea

L'Unione europea nel suo complesso ha molto lavorato sulla sicurezza di reti ed informazioni nonché sulla criminalità informatica. Obiettivi dell'Unione sono la resilienza informatica, la salvaguardia delle comunicazioni e la sicurezza on line. Nel solco della volontà di produrre una normativa atta a creare una base giuridica comune, è possibile elencare una serie di interventi in tal senso.

Pubblicata per la prima volta nel 2013, nel 2020 la Commissione europea e l'alto rappresentante per gli affari esteri e la politica di sicurezza, hanno presentato[228] la nuova edizione della S*trategia UE in materia di cybersicurezza*, aggiornata anche a seguito dell'esperienza maturata con la pandemia da COVID-19[229].

Il documento rinnovato, facendo tesoro della continua evoluzione tecnologica, è stato incentrato sulla sicurezza nella navigazione sia per la salvaguardia delle comunicazioni e dei dati che dei diritti fondamentali. Il documento contiene proposte da realizzare attraverso tre strumenti principali quali normative, investimenti e iniziative di carattere politico.

Tali strumenti dovranno avere come obiettivo comune alcune aree di interesse quali resilienza, sovranità tecnologica e leadership, capacità operativa di prevenire, scoraggiare e rispondere, cooperazione per un cyberspazio globale e aperto.

---

[228] Come da comunicato stampa del 16 dicembre 2020, disponibile su https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

[229] Commissione europea, "the EU's Cybersecurity strategy for the Digital Decade" disponibile suhttps://digital-strategy.ec.europa.eu/it/node/435

L'orizzonte temporale previsto è quello di sette anni con una quadruplicazione degli investimenti rispetto alle precedenti strategie in materia.

Sempre in ambito Unione europea, la direttiva NIS, sulla sicurezza delle reti e dei sistemi informativi del 2016, pensata per un elevato livello di sicurezza delle reti e dei sistemi di informazione a livello europeo, è stata sottoposta ad un importante processo di riesame arrivando alla pubblicazione della direttiva NIS 2 in Gazzetta Ufficiale dell'Unione europea nel dicembre 2022 con entrata in vigore il 16 gennaio 2023 e tempo massimo al 18 ottobre 2024 per l'introduzione negli ordinamenti. Va inoltre citato:

- Il *cyber security act*[230], che istituisce certificazioni per prodotti e servizi sotto il controllo dell'ENISA, l'agenzia per la *cybersicurezza* europea, ora molto rafforzata nel suo campo d'azione a livello europeo[231].
- il Cyber Resilience Act[232], proposta di legge in ambito europeo volto alla sicurezza informatica dei dispositivi connessi. In data 19 luglio 2023 la Commissione per l'industria del Parlamento europeo

---

[230] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32019R0881&qid=1694642868084 .

[231] Con Proposta di regolamento del Parlamento europeo e del Consiglio del 18 aprile 2023 che modifica il regolamento (UE) 2019/881 per quanto riguarda i servizi di sicurezza gestiti, la Commissione ha proposto una modifica sul cyber security act mirata alla certificazione anche dei "servizi di sicurezza gestiti", in aggiunta ai prodotti, ai servizi ed ai processi ICT già inclusi precedentemente. Disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52023PC0208

[232] Proposta di regolamento del Parlamento europeo e del Consiglio del 15 settembre 2022, relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020, disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52022PC0454.

ha dato il via libera a tale proposta portando il testo alla sessione plenaria del Parlamento al fine di confermare l'avvio dei negoziati inter-istituzionali con Commissione e Consiglio UE (cd. Trilogo), per la stesura definitiva del testo;

- La proposta, del 18 aprile 2023, da parte della Commissione per la "EU cyber solidarity act" o atto di solidarietà cibernetica, finalizzata ad una migliore risposta alle minacce informatiche a livello totale europeo attraverso un cosiddetto scudo europeo di *cybersicurezza* ed un meccanismo unico in caso di emergenza;
- La Digital Operational Resilience Act (DORA), regolamento (UE) n. 2022/2554[233], entrata in vigore dal 16 gennaio 2023, mirata alla sicurezza cibernetica nel settore finanziario.

La Commissione sta inoltre lavorando ad un quadro di certificazione a livello Unione, la EU cybersecurity certification framework, frutto del lavoro del "Gruppo europeo di certificazione della cybersicurezza (ECCG, European Cybersecurity Certification Group[234]) e avente come fulcro l'Enisa.

L'Unione europea gode di una vera e propria comunità Cyber formata da diverse realtà quali:

- L'Accademia UE per le competenze in materia di cybersicurezza (Cybersecurity Skills Academy)[235], ospitata sulla piattaforma per l'occupazione e le competenze della Commissione, riunendo iniziative pubbliche e private finalizzate alla forza lavoro in questo ambito;

---

[233] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011. Disponibile su https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R2554

[234] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group

[235] https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

- I Centri di Condivisione e Analisi delle Informazioni (ISAC) finalizzati alla collaborazione di diverse comunità di materia in settori diversi;
- Il Centro Comune di Ricerca (CCR o JRC, joint research center[236]) che tra le altre cose ha prodotto nel 2022 il JRC Cybersecurity Taxonomy al fine di standardizzare il linguaggio cyber a livello europeo[237];
- I CSIRT (Squadre di risposta agli incidenti informatici) o CERT (squadre di pronto intervento informatico) presenti negli stati membri come già da direttiva NIS. I Teams citati hanno compito di monitorare gli incidenti, fornire allarme rapido, reagire agli incidenti, analizzare l'accaduto e partecipare alla rete europea delle strutture dei paesi membri. In Italia il CSIRT nazionale[238] è ubicato presso l'Agenzia Nazionale per la Cybersicurezza (ACN).
- L'Organizzazione Europea per la Cybersicurezza (ECSO), creata nel 2016 come partenariato pubblico-privato di livello contrattuale-industriale.

Per concludere l'excursus comunitario in materia di cybersicurezza possiamo riassumere affermando che la politica UE in materia si basa su quattro pilastri: l'azione comune, la protezione dell'ecosistema della difesa, investimento, il partenariato. l'UE coopera, inoltre, con paesi terzi al fine di rafforzare le capacità di difesa cibernetica. A tal proposito vanno citati i programmi di cybersicurezza nei Balcani occidentali e nei

[236] https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/joint-research-centre_en
[237] European Commission, Joint Research Centre (JRC) (2021): JRC CYBERSECURITY TAXONOMY. European Commission, Joint Research Centre (JRC) [Dataset] PID: http://data.europa.eu/89h/d2f56334-a0df-485b-8dc8-2c0039d31122
[238] https://www.csirt.gov.it/

sei paesi del partenariato orientale[239], portati avanti dal Dipartimento della Cooperazione internazionale e dello sviluppo.

10.2 ONU

L'Organizzazione delle Nazioni Unite, nonostante disaccordi che non hanno consentito il raggiungimento dei risultati sperati, ha messo in atto diverse iniziative finalizzate alla sicurezza informatica. Tra tutte il GGE[240], Gruppo di esperti governativi sugli sviluppo nel campo delle tecnologie dell'informazione e della comunicazione nel contesto della sicurezza internazionale. A tal proposito il GGE ha prodotto una serie di report tra cui:

- l'A/72/327: Report sulla risoluzione dell'Assemblea generale 70/237 sugli sviluppi ICT in relazione alla sicurezza internazionale, 2017[241]; l'A/68/98: Report di raccomandazione sulle norme di comportamento on line e lo scambio di informazioni, del 22 luglio 2015[242]; l'A/65/201: misure di cooperazione e raccomandazioni per ridurre il rischio di incomprensioni[243].

Più in generale l'Organizzazione ha prodotto report e studi sulla prevenzione del crimine[244], sullo sfruttamento e abuso

[239] Eastern Partnership (EAP), lanciata nel 2009 per rafforzare i rapporti tra partner extra unione quali Armenia, Azerbaijan, Bielorussia, Georgia, Moldavia, Ucraina.
[240] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
[241] https://undocs.org/A/72/327
[242] https://undocs.org/A/68/98
[243] https://undocs.org/A/65/201
[244] Assemblea generale, Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity, report of the Secretary general, 2022, disponibile su https://www.unodc.org/documents/treaties/a_res_57/153e.pdf;

dei bambini[245], sui sistemi di sanzione, sui problemi legati all'uso della rete[246] e sull'uso terroristico delle tecnologie ICT[247].

A livello di regolamentazione sono state prodotte diverse risoluzioni in tema di disarmo correlato al problema della sicurezza informatica[248], protezione di infrastrutture di informazione critiche[249], sulla diffusione della cultura della sicurezza cibernetica ed educazione all'uso delle ICT[250]. Molto importanti le attività di cooperazione quali l'Annual Cyber Stability Conference, il World Summit on the Information Society (WSIS), L'Arria-Formula Meeting, riunione informale dei membri del Consiglio di Sicurezza ONU convocata di volta in volta da un membro dello stesso[251], il Gruppo OEWG (Open-Ended Working Group[252]), gruppo di lavoro creato con risoluzione 73/27 del 2018 aperto a tutti gli stati con lo

[245] Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, disponibile su https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

[246] The Mapping of International Internet Public Policy Issues, disponibile su https://unctad.org/meetings/en/SessionalDocuments/CSTD_2014_Mapping_Internet_en.pdf

[247] Countering the Use of the Internet for Terrorist Purposes - Legal and Technical
Aspects, Working Group Compendium, consultabile a https://www.un.org/es/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

[248] Resolutions and Reports on Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/ict-security/

[249] Assemblea generale, seconda Commissione, Resolution on the Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, UN Doc. A/RES/64/211 del 17 marzo 2010, disponibile su https://undocs.org/A/RES/64/211

[250] Assemblea generale, Resolution on the Creation of a global culture of cybersecurity, UN Doc. A/RES/57/239 del 31 gennaio 2003, disponibile su https://undocs.org/A/RES/57/239

[251] Ultimo incontro avvenuto nel mese di maggio 2023 intitolata "The Responsibility and Responsiveness of States to Cyberattacks on Critical Infrastructure", disponibile su https://www.securitycouncilreport.org/whatsinblue/2023/05/arria-formula-meeting-on-the-responsibility-and-responsiveness-of-states-to-cyberattacks-on-critical-infrastructure.php

[252] https://disarmament.unoda.org/open-ended-working-group/

scopo di valutare gli sviluppi ICT correlati alla sicurezza internazionale[253].

Meritano specifica citazione i "Digital blue helmets", presso l'Ufficio per le Informazioni e le comunicazioni tecnologiche (OICT). Il "Digital Blue Helmets Program" non è un classico organo operativo con funzioni di peacekeeping tradizionalmente inteso ma viene definito, attraverso una brochure[254], come team di professionisti informatici, specializzati nel monitoraggio di eventi, test ambientali, analisi forense e operazioni informatiche.

La nascita del programma deriva dalla sempre accresciuta esigenza di sicurezza informatica per i siti istituzionali su più livelli, da quello fisico delle infrastrutture a quello economico attraverso il furto di dati bancari o ancora a quello dei dati sensibili degli utenti.

Più nello specifico una delle esigenze massime per il team di esperti è stato quello del monitoraggio delle attività illegali nel dark web, dal traffico di stupefacenti, delle armi, come anche degli esseri umani creando quello che viene definito, in contrapposizione, un "light web".

Le agenzie afferenti all'ONU che conducono attività correlate più o meno direttamente alla sicurezza cibernetica sono la United Nations Office for Disarmament Affairs[255], la International Telecommunications Union (ITU)[256], la United Nations Institute for

---

[253] OEWG, developments in the field of ICTs in the context of international security, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement

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

[255] Dipartimento con core business nello smantellamento delle armi, in particolari di distruzione di massa. Ha un occhio particolarmente agli equilibri in ambito ICT https://www.un.org/disarmament/ict-security

[256] Storica organizzazione interessata agli standard di comunicazione con responsabilità di difesa cibernetica nelle reti di comunicazione, https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

Disarmament Research (UNIDR)[257], lo United Nations Office on Drugs and Crime (UNODOC)[258] specializzato in crimine con settori specifici dedicati al monitoraggio del cyber-crime, l'Office of Information and Communications Technology (OICT)[259], deputato al monitoraggio dei programmi ICT dell'Organizzazione.

10.3 NATO

Il North Atlantic Treaty Organisation (NATO), in virtù della sua indole operativa e militare, ha posto il Cyberspazio e la difesa dello stesso come uno dei task principali da perseguire anche a seguito del vertice di Lisbona del 2010[260], del vertice di Varsavia del 2016 in cui il Cyberspazio è stato riconosciuto come reale dominio di operazioni e della decisione di creare un Cyber Operation Center presso lo SHAPE[261].

A livello di Cyber policy la Nato, durante il Wales Summit del 2014, ha adottato l'"*Enhanced Cyber Defence Policy*"[262], documento finalizzato alla cooperazione in tema di cyber difesa, mutua assistenza tra i membri, sviluppo di capacità e creazione di partnership.

Nel 2018 inoltre, a margine del summit di Bruxelles, è stata formulata una dichiarazione, al cui punto 20 vengono considerate

[257] https://unidir.org/about/the-institute
[258] https://www.unodc.org/unodc/en/cybercrime/index.html
[259] https://unite.un.org/information-security
[260] In cui la Cyber Defence è stata inclusa nel Concetto strategico della Nato, a tal proposito vedasi http://www.comitatoatlantico.it/COMIT/documenti/concetto-strategico-2010/
[261] https://shape.nato.int/about/aco-capabilities2/cyber-defence
[262] NATO, Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 2014, disponibile su https://www.nato.int/cps/en/natohq/official_texts_112964.htm

le minacce cibernetiche, riaffermando la necessità di sviluppo di capacità in tal senso[263].

Va inoltre citato il Tallin Manual, redatto dal CCDCOE[264], meglio descritto successivamente, contenente indicazioni per i cyber incidenti nelle formulazioni del 2013, del 2017 (Tallin Manual 2.0) e divenuto assoluto riferimento in relazione all'applicazione del diritto internazionale agli incidenti cibernetici. Risulta, tra l'altro, già allo studio la terza versione del manuale a cura del Professor Michael Schmitt storico direttore delle precedenti edizioni[265].

Le agenzie della Nato interessate alla difesa cibernetica sono:

- La NATO Communications and Information Agency (NCIA), deputata alla protezione dei sistemi di comunicazione della componente militare[266];
- Il North Atlantic Council (NAC), la maggiore autorità in ambito cyber defence e gestione delle crisi informatiche[267]
- Il Nato Cyber Defence Committee[268];
- Il Nato Cyber Defence Management Board, per la coordinazione CIMIC, ovvero dei settori militari e civili, in ambito cyber[269];
- L' Allied Command Transformations, responsabile tra le altre cose di una esercitazione cyber a cadenza annuale, la Cyber Coalition Exercise;

---

[263] NATO, Brussels Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels
11 12 July 2018, disponibile a https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[264] Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/
[265] A tal proposito v. https://ccdcoe.org/research/tallinn-manual/
[266] https://www.ncia.nato.int/what-we-do.html
[267] https://www.nato.int/cps/en/natohq/topics_78170.htm?selected.l.ocale=en
[268] *Ibidem*
[269] *Ibidem*

- Il Nato Cooperative Cyber Defence Centre of Excellence (CCDCOE), organizzazione di esperti provenienti da 25 nazioni con scopo di ricerca e supporto in ambito Nato.

Va evidenziato inoltre il fitto programma di esercitazioni e cooperazione internazionale in ambito cyber defence attuato dalla Nato:

- il Nato Information Assurance Symposium (NIAS)[270]
- l'Annual Cyber Coalition Exercise[271], la più grande esercitazione in materia in ambito Nato con più di 700 attori militari e civili.
- l'International Conference on Cyber Conflict[272];
- la Locked Shields[273];
- il progetto Nato-Moldova[274], Estonia/Nato-Japan[275], Cooperation Agreement EU-Nato[276], Nato-Kuwait ICI Regional Center activities[277], Nato-Lithuania[278], Nato-Bosnia and Herzegovina[279], il dialogo Morocco-Nato[280], ed i MOU (memorandum of understanding) con la Bulgaria[281], Repubblica Ceca[282], Romania[283] e Lithuania[284].

---

[270] https://nias19.com/
[271] https://www.nato.int/cps/en/natohq/news_160898.htm
[272] https://ccdcoe.org/cycon/
[273] https://ccdcoe.org/exercises/locked-shields/
[274] https://www.nato.int/cps/en/natohq/news_152364.htm?selected.l.ocale=en
[275] https://ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn/
[276] https://www.nato.int/cps/en/natohq/news_149848.htm
[277] https://www.nato.int/cps/ic/natohq/news_147010.htm
[278] https://kam.lt/lt/titulinis_1220.html
[279] https://www.nato.int/cps/en/natohq/news_144045.htm
[280] https://northafricapost.com/17912-morocco-nato-cooperate-countering-cyber-security-risks.html
[281] https://www.nato.int/cps/en/natohq/news_137069.htm
[282] https://www.govcert.cz/en/info/events/2444-nsa-director-sign-memorandum-with-nato/
[283] https://nato.mae.ro/local-news/487
[284] https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_LITHUANIA_092015.pdf

Va senza dubbio considerato inoltre il dispiegamento e rafforzamento sul "fronte est" in considerazione della crisi Russo-Ucraina, con interessamento sia su suolo italiano che in Teatro operativo del nostro Comando Operazioni in Rete dello Stato Maggiore della Difesa.

10.4 Consiglio d'Europa

Il Consiglio d'Europa, o Council of Europe (CoE), organizzazione intergovernativa specializzata nella difesa dei diritti umani, con la Convenzione di Budapest sulla criminalità informatica del 2001[285], ha posto in atto una significativa iniziativa nell'ambito della sicurezza informatica producendo una linea guida per quei paesi che devono ancora sviluppare le legislazioni nazionali in tema di criminalità informatica.

Attraverso il CoE, il 17 aprile 1989[286], è stato istituito un sistema di protezione dei dati personali e la figura del Commissario della protezione dei dati, responsabile della supervisione del rispetto di tali norme.

Circa la cooperazione internazionale il CoE è coinvolto nel "*GLACY+*"[287], progetto congiunto di Unione Europea e Consiglio d'Europa in materia di protezione dalla criminalità informatica a supporto di 15 paesi[288].

---

[285] Consiglio d'Europa, Convenzione sulla criminalità informatica Budapest 23/11/2001, attualmente ratificato da 68 paesi, con l'eccezione di Irlanda e Sud Africa che hanno firmato ma non ratificato. Disponibile su https://www.coe.int/it/web/portal/coe-action-against-cybercrime

[286] Consiglio d'Europa, Secretary General's Regulation of 17 April 1989 instituting a system of data protection for personal data files at the Council of Europe,
disponibile su https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680684608.

[287] Global Action on Cybercrime Extended (GLACY)+, disponibile su https://www.coe.int/en/web/cybercrime/glacyplus.

[288] Benin, Burkina Faso, Capo Verde, Cile, Costa Rica, Repubblica Domenicana, Ghana, Mauritius, Marocco, Nigeria, Paraguay, Filippine, Senegal, Sri Lanka e Tonga

Il Consiglio d'Europa, a seguito di un Memorandum con la Romania, ha istituito nel 2013 il Cybercrime Program Office a Bucarest[289] con l'obiettivo di creare una solida base nella lotta al cyber crime.

10.5 Altre organizzazioni internazionali

Vengono di seguito sinteticamente elencate altre organizzazioni di diversa tipologia e le relative strutture operative interne dedicate o interessate al cyberspazio. Tale elenco, sicuramente non esaustivo, vuole far comprendere come indipendentemente dalla locazione geografica mondiale, il tema della sicurezza informatica è sempre presente anche con il supporto, fisico o di linea guida, di strutture già consolidate in tal senso come Unione Europea o ONU: il Commonwealth con il Commonwealth Telecommunications Organization (CTO)[290] e la Commission on Sciences and Technology for Sustainable Development in South (Comstas)[291]; l' Economic Community of West African States (Ecowas)[292] che ha prodotto l' Ecowas ICT Policy[293] e l' Ecowas Cyber Security and Cyber-crime Strategy[294]; l' Organisation of American States (OAS)[295] con l' Inter-American

[289] Cybercrime Program Office (C PROC), disponibile su https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-
[290] https://thecommonwealth.org/organisation/commonwealth-telecommunications-organisation-cto
[291] https://thecommonwealth.org/organisation/commission-science-and-technology-sustainable-development-south-comsats
[292] ECOWAS, Organizzazione molto attiva in Africa nel settore della sicurezza informatica composta da Benin, Burkina Faso, Capo Verde, Costa d'Avorio, Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Senegal e Togo, http://www.ecowas.int/
[293] https://www.ecowas.int/ecowas-sectors/ict/
[294] https://www.ecowas.int/regional-technical-committee-validates-ecowas-cyber-security-and-cybercrime-strategy/
[295] Organisation of American States (OAS), organizzazione regionale formata dai 35 parsi americani. L'OAS ha aiutato l'America latina a sviluppare strategie di sicurezza informatica. http://www.oas.org

Committee against Terrorism (Cicte)[296], l' Inter-American Telecommunication Commission (Citel)[297] ed il Group of Governmental Experts, Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (Remja)[298]; l'Organisation for Economic Co-operation and Development (OECD)[299] con due direttorati, il Directorate for Sciences e il Directorate for Technology and Innovations[300].

Abbiamo inoltre le sotto elencate organizzazioni e le rispettive attività in materia:

L' Organisation for Security and Co-operation in Europe (OSCE)[301] con il Regional Cybercrime Training[302], ed il Capacity building in Kosovo[303];

L' African Union (AU) con l'Africa Cybersecurity Collaboration and Coordination Committee (Acs3c), l'African Union Cyber Security Expert Group (Aucseg)[304] e lo Specialized Technical Committee on Communication and ICT (STC CICT)[305];

L' Association of Southeast Asian Nations (Asean) con i National Security Operations Centres (SOC)[306].

Questo elenco, se da un lato ci illustra una atavica stratificazione a livello organizzativo internazionale, ci aiuta allo

[296] http://www.oas.org/en/sms/cicte/
[297] https://www.citel.oas.org/en/Pages/default.aspx
[298] http://www.oas.org/en/sla/d.l.c/remja/
[299] http://www.oecd.org/
[300] https://www.oecd.org/sti/
[301] https://www.osce.org/
[302] https://polis.osce.org/node/1083
[303] https://www.osce.org/mission-in-kosovo/cyber-ict-security
[304] https://au.int/en/announcements/20180920/call-experts-african-union-cyber-security-expert-group
[305] https://au.int/en/stc
[306] Composto da 10 stati membri dell'ASEAN per la creazione di una piattaforma di scambio informativo "orizzontale" utilizzata anche per early warning in caso di minaccia cibernetica, https://acioa.com/

stesso tempo a comprendere quanto, a partire dagli anni 70[307] fino ai 2000 con la nascita della cyberwarfare intesa come uso volutamente malevolo di strumenti informatici a fini di attacco, il problema della sicurezza ICT e della comunione di sforzi sia divenuto punto cardine nelle policy internazionalistiche degli Stati.

Nonostante le dichiarazioni di intenti, rimane comunque irrisolto, come meglio vedremo nel terzo capitolo, il tentativo di trovare una visione univoca nell'adattamento del diritto internazionale preesistente classico ai fenomeni cibernetici che gli Stati di vota in volta si trovano ad affrontare singolarmente o insie me.

[307] Seppur già teorizzato dal John von Neumann negli anni 50, il primo esempio di programma replicante e autoinstallante risale al 1971 con la creazione di "Creeper", scritto da Bob Thomas, ingegnere informatico americano. Fu il primo caso di "worm" ma soprattutto la prima volta in cui ci si pose domande sul controllo di questi fenomeni.

Capitolo 3 – Legittima difesa e cyber warfare

Dopo aver descritto i fondamenti del diritto internazionale in tema di uso della forza e legittima difesa ed aver illustrato il concetto, fino ad ora teorico, di cyberspazio, l'intento del terzo capitolo è quello di tratteggiare in una summa teorico-pratica dei primi due capitoli, gli ostacoli che nel dibattito dottrinale continuano ad emergere nel tentativo di conciliare le due realtà dovendo obbligatoriamente considerare temi imprescindibili quali l'attribuzione della colpa ad un determinato Stato, la responsabilità internazionale e soprattutto la proporzionalità nella risposta.

Il capitolo verrà aperto illustrando alcuni casi scuola avvenuti negli anni 2000, anni che segnarono il passaggio dalla sperimentazione benevola di programmi autoinstallanti tipica degli anni Ottanta alla nascita della cyberwarfare vera e propria, caratterizzata da un uso strategico ed operativo di mezzi informatici a finalità offensive.

Fatto tesoro dei casi studio proposti verranno infine analizzate le principali problematiche di applicazione degli istituti internazionali.

1. Attacchi cibernetici, alcuni casi studio

Il Piano nazionale per la protezione cibernetica e la sicurezza informatica e l'annesso Piano d'azione, sono stati il culmine di un periodo che ha visto numerosi eventi accaduti nel cyberspace, nuova arena della rivalità multinazionale. Tra questi ci sono stati alcuni casi scuola che hanno di fatto segnato il passaggio da una generica attività informatica alla guerra cibernetica vera e propria.

Si vuole dunque riportare alcuni di questi eventi rimasti storici non solo per l'innovativa portata tecnica ma anche e soprattutto per le problematiche di volta in volta affrontate e che di fatto non hanno consentito una proporzionata risposta da parte degli Stati lesi o dalla Comunità internazionale.

1.1 Estonia, 2007

L'Estonia è ad oggi uno dei paesi informaticamente più avanzati al mondo. Nonostante le modeste dimensioni geografiche è a tutti gli effetti punto di riferimento nella Cybersecurity.

Prima di arrivare al caso di specie giova brevemente ricordare che nel 1991, ottenuta l'indipendenza dall'Unione Sovietica, uno degli obiettivi governativi fu quello della costruzione da zero di una infrastruttura tecnologica tale da consentire l'avvicinamento all'occidente nel più breve tempo possibile.

Venne a tal proposito varato nel 1996 il progetto "Tiger Leap", in estone Tiigrihüpe, "salto della tigre", un epocale programma di sviluppo tecnologico di tutto il paese con particolare riguardo all'istruzione e all'accesso alla rete internet in tutte le scuole. Ad oggi il progetto di digitalizzazione più avanzato al mondo porta il nome di e-Estonia[308] e spazia nei più disparati campi come ad esempio la realizzazione del primo veicolo autonomo ad idrogeno nel 2021.

Al di là della spinta verso il progresso ciò che però rese il paese riferimento in tema di sicurezza fu un cyber attacco di enormi proporzioni subito nel 2007.

L'evento scatenante fu la decisione da parte del governo estone di rimuovere la statua di bronzo, corrispettivo del nostro milite ignoto, installata nel 1947 dall'Unione Sovietica per

[308] https://e-estonia.com/story/

commemorare i caduti dopo la cacciata dei tedeschi nella seconda guerra mondiale. L'asportazione del monumento voleva rappresentare il rafforzamento dell'orgoglio nazionale a detrimento della compagine filorussa presente nel paese.

Immediatamente si scatenò un'ondata di manifestazioni da parte della comunità estone di lingua russa che comportò un morto e l'arresto di 1300 persone.

Contemporaneamente, dalla serata del 27 aprile, una serie di attacchi cyber colpirono alcuni siti governativi andando ad incrementare costantemente la complessità offensiva e la portata degli eventi malevoli. Si iniziò con attacchi ping[309] per passare ben presto all'utilizzo di Botnet in un sistema di volta in volta più strutturato.

Il culmine avvenne il 9 maggio, anniversario della vittoria sovietica sul nazismo. Solo in quella giornata furono messi fuori gioco ben 58 siti statali ed i servizi digitali della principale banca del paese[310]. Vennero nel complesso utilizzati 85.000 computer in modalità botnet nell'arco di tre settimane rendendo chiaro che una capacità cyber offensiva di questa portata non potesse avere natura completamente privata come neanche derivare da Stati poco avanzati tecnologicamente.

Il Ministro della Difesa estone accusò apertamente la Russia vantando prove documentali, tesi successivamente smentita dalle indagini NATO e della Commissione Europea che non riuscirono a provare la matrice russa, lasciando insoluta più che l'identificazione degli operatori, l'attribuzione dell'attacco. Non si poté infatti con certezza addebitare il danno alla Russia

[309] Attacco tipicamente DDOS a mezzo invio di pacchetti "ICMP ECHO REQUEST" comportanti la saturazione della banda sia in ingresso che in uscita.
[310] AA.VV., International Cyber Incidents, legal consideration, Tallinn, 2010, p. 20.

nonostante determinati accadimenti favorissero l'attribuzione in tal senso. Fra questi la riscontrata pianificazione antecedente le manifestazioni riguardanti sia Tallin che l'ambasciata estone a Mosca[311], la presenza nei sistemi estoni di botnets collegabili ad organizzazioni filo-russe nelle settimane precedenti gli scontri,[312] la strutturazione delle proteste della comunità filo-russa assimilabile quella della dottrina del "rally round the flag effect" posta spesso in essere dal Cremlino per le minoranze di lingua russa[313] e consistente, come osservabile anche nell'attuale conflitto ucraino, nel paventare minacce alla propria integrità al fine di generare maggiore coesione e sostegno ad un leader spesso anche senza basi razionali. Diversi attivisti russi, inoltre, nonché' un parlamentare della Duma, si attribuirono gli attacchi.

Analizzando l'evento e tentando una collocazione giuridica nelle classificazioni tipiche del diritto internazionale, bisogna innanzitutto chiedersi se gli accadimenti estoni possano essere considerati effettivamente un attacco armato, un attacco di guerra o un "semplice" atto di terrorismo di matrice ideologica. Non pochi esponenti estoni, a partire dal Ministro della difesa illo tempore, dichiararono che la natura degli attacchi fosse di tipo terroristico e nello specifico di tipo psicologico volto cioè a screditare l'organizzazione statale estone e a minare la fiducia nelle istituzioni.

---

311 BLANK S., Web War I: Is Europe's First Information War a New Kind of War? In Comparative Strategy, Vol. 27, No. 3, 2008, pp. 227-247, disponibile su https://doi.org/10.1080/01495930802185312

312 RID T., Cyber War Will Not Take Place, in Journal of Strategic Studies, London, UK, 2011, p. 12, disponibile su https://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf

313 GIUSTI S, La Proiezione Esterna della Federazione Russa, Pisa, 2012;

Lato NATO, nel timore di una escalation, il tutto venne qualificato come sommossa informatica[314], tesi sostenuta anche dagli esperti del Manuale di Tallin i quali ritennero l'episodio estone non elevabile al grado di attacco armato in considerazione di dimensione ed effetti[315]. Le autorità estoni, inoltre, considerarono l'incidente un atto di cyber crime interno e dunque non di interesse internazionale andando unicamente ad attivare i meccanismi del diritto penale nazionale .

Le investigazioni a valle di quanto sopra esposto soffrirono inoltre di alcune limitazioni. In primis per i limiti alla possibilità di raccogliere dati imposti dall'allora legislazione estone[316] che non consentirono l'opportuna libertà di manovra per l'identificazione degli autori. Il secondo ostacolo, che ritengo di interesse circa l'oggetto del presente lavoro, fu rappresentato dalla rogatoria internazionale inviata dal Procuratore Generale estone verso la Russia finalizzata al recepimento di indirizzi IP dei potenziali attaccanti[317] ed alla quale venne data risposta negativa addirittura un anno dopo.

Questo ci pone all'attenzione uno dei problemi principali circa l'applicazione delle sanzioni a livello internazionale in questo ambito ovvero quanto una mancanza di cooperazione internazionale in un contesto, quello cibernetico, che sfugge ai tipici meccanismi di tempo e luogo degli attacchi tradizionali, possa vanificare qualsiasi tipo di individuazione o attribuzione.

---

[314] SHACKLEFORD S. J., From Nuclear War to Net War. Analogizing Cyber Attacks in International Law, in Berkeley Journal of International Law, Vol. 27, No. 1, 2009, p. 209,

[315] SCHMITT, M. N., Tallinn Manual on the international law applicable to cyber warfare, Cambridge, 2013, Rule 13, punto 13

[316] Codice Penale Estone, § 137 "Unauthorised surveillance", disponibile su https://www.riigiteataja.ee/en/eli/522012015002/consolide e Codice di Procedura Penale Estone, Divisione 8, § 110-112.

[317] Come da accordo di mutua assistenza legale del 1993.

L'unico incriminato fu Dimitri Galushkevich, estone ma della minoranza russofona, incolpato di aver lanciato attacchi durante la prima fase "ping" verso il Partito Riformatore Estone comportando un danno di 2.820 euro[318]. Al di là delle conseguenze penali, l'evento del 2007 fece prendere coscienza, non solo all'Estonia, della fragilità difensiva, sul piano tecnico come quello giuridico, nel contesto cibernetico portando il paese colpito a divenire il centro globale della cybersecurity nonché' sede, a Tallin, del Centro di eccellenza per la difesa informatica cooperativa della Nato (CCDCOE), struttura attraverso la quale sono stati prodotti i noti manuali divenuti rifermento dottrinale in materia.

1.2 Stuxnet, 2009

Il primo vero esempio di cyber war fu Stuxnet (2009), un attacco ai danni della centrale nucleare di Natanz in Iran. Il fatto che esso sia un passaggio unico nel suo genere va ricercato negli elementi evinti a posteriori[319] quali il target, il tipo di azione, i danni prodotti e la motivazione. L'evento iraniano fu considerato a tutti gli effetti il primo caso di uso di un dispositivo digitale capace di causare danni fisici, a persone o cose.

Fino a quel momento i malware venivano utilizzati per estorcere denaro, rubare informazioni o "bucare" barriere istituzionali senza comunque superare la barriera del danno virtuale. Stuxnet, come venne etichettato dagli esperti forensi, riuscì invece a conseguire un obiettivo di massimo livello strategico: compromettere 1.000 su 8.000 centrifughe nel sito di

[318] Sentenza della Corte della contea di Harju numero 1-07-15185 (Galushkevich) del 13 dicembre 2007

[319] A tal proposito vedasi GORI U. e GERMANI L. S., Information Warfare. Le nuove minacce provenienti dal cyber spazio alla sicurezza nazionale italiana, Milano, 2011

Natanz, a 250 chilometri a sud di Teheran, arrivando a ritardare il programma nucleare iraniano.

Stuxnet ancora oggi viene riconosciuto come il cyber attacco più complesso mai realizzato di tipo one spot ovvero non correlato ad altre operazioni militari in corso con un periodo di azione, benché scoperto nel 2010, risalente alla fine del 2007[320] e costituito da tre ondate offensive attuate nell'estate del 2009 e nel marzo e nella primavera del 2010. Si ritiene comunque che solo la prima ondata abbia causato danni reali[321].

La porta di accesso venne individuata in una vulnerabilità presente in un software prodotto dalla Siemens, il SIMATIC STEP7[322], utilizzato nella centrale di Natanz. Il virus venne introdotto attraverso un'unità USB consentendo così l'attivazione dall'interno, elemento fondamentale in considerazione del fatto che i sistemi della centrale non fossero accessibili dall'esterno. L'apparato da colpire presentava, dal punto di vista dell'attaccante, delle complicazioni in quanto questo genere di sistemi non dispone né di periferiche di input, quali mouse o tastiere, né di output, come schermi o stampanti. Chi programma o aggiorna questo tipo di sistemi (fondamentalmente delle scatole) si connette tramite un computer portatile, solitamente di produzione Siemens, dotato di sistema operativo Windows.

Il virus, dunque, venne inoculato o consapevolmente o, più facilmente, da un agente inconsapevole[323].

---

[320] LANGNER R., What STUXNET is All About, 2011, disponibile su http://www.langner.com/en/2011/01/10/what-stuxnet-is-all-about/.

[321] LINDSAY J. R., Stuxnet and the Limits of Cyber Warfare, in "Security Studies", Vol. 22, No. 3, 2013, disponibile su https://doi.org/10.1080/09636412.2013.816122

[322] Software di automazione industriale PLC, Controllore Logico Programmabile, utilizzato per automatizzare un processo, una funzione specifica o addirittura un'intera linea industriale.

[323] Nel 2010 vennero arrestate alcune persone con l'accusa di spionaggio ma non si dispongono di notizie certe circa la reale colpevolezza. Si pensa infatti

Uno dei motivi per cui Stuxnet viene ancora considerato a distanza di più di un decennio estremamente sofisticato è la capacità di rimanere occulto durante il contagio. Viene stimato che alla fine del 2010 fossero 100.000 i terminali infettati, dei quali il 40% fuori dall'Iran[324].

Tecnicamente il virus sfruttò una vulnerabilità "zero-day" di Windows, dunque non risolvibile per lo stato dell'arte del periodo, ed era dotato di certificati digitali Realtek e Lmicron che gli consentirono di installare i rootkit[325]. Stuxnet era inoltre programmato per comunicare, nonostante il sistema "air gap", in modalità peer-to-peer via internet con specifici server dedicati all'operazione potendo dunque inviare informazioni verso l'esterno e creando la porta per eventuali nuove istruzioni. Ogni terminale infettato diventava a tutti gli effetti un terminale "zombie" da tramutare in worm per la ricerca dell'obiettivo successivo.

Raggiunto l'obiettivo dei controller logici Siemens 6ES7-315-2 e 6ES7-417, che controllavano turbine e centrifughe dei reattori di Busheher e Natanz[326], il virus andò a manipolare la frequenza del converter del rotore della centrifuga passando dai canonici 1,064 H_z a valori differenti nell'arco di più giorni.

Per rendere l'attacco difficile da rilevare, la frequenza venne incrementata e diminuita ad intervalli di 27 giorni e, per questo, i tecnici inizialmente ritennero che il tracollo delle centrifughe fosse

---

che l'arresto fosse dovuto alla ricerca di un capro espiatorio. A tal proposito v. YONG W., Iran Says It Arrested Computer Worm Suspects, su nytimes.com, 2010, disponibile su https://www.nytimes.com/2010/10/03/world/middleeast/03iran.html

[324] AA.VV., *W32. Stuxnet Dossier*, versione 1.4, 2011, pp. 5-7, disponibile su https://nsarchive.gwu.edu/document/21440-document-44.

[325] Insieme di software tipicamente malevoli realizzati per accedere ad un computer.

[326] RID T., Cyber War Will Not Take Place, in Journal of Strategic Studies, London, UK, 2011, p. 12, disponibile su https://www.csl.army.mil/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf, p. 18.

dipeso da un errore umano commesso al momento della scoperta più che da un virus inoculato molto tempo prima. La frequenza venne portata a 1,410 H_z per 15 minuti al giorno per poi essere abbassata per 50 minuti in modo da rendere la turbina non efficiente per l'arricchimento dell'uranio. La stessa, successivamente, tornava a regime normale. Tale azione venne pensata non tanto per una rottura definitiva ma per un indebolimento strutturale diffuso nel tempo, attraverso un affaticamento delle parti meccaniche. Agli operatori, inoltre, venivano restituiti report falsati indicanti il normale funzionamento delle centrifughe non destando, dunque, alcun sospetto da parte degli addetti al controllo.

Le conseguenze dell'azione si palesarono in più ambiti. A livello informatico fu l'inizio dell'era degli attacchi informatici capaci di portare danno fisico ha rivoluzionato il modus operandi degli analisti cambiando anche la programmazione dei sistemi di automazione industriale PLC, di colpo non considerati inviolabili in quanto isolati dal mondo esterno.

Altro aspetto da considerare è stato il rallentamento del programma nucleare iraniano di circa un anno fatto che ha sancito il successo strategico dell'operazione Stuxnet. Attaccare cineticamente un reattore nucleare avrebbe costituito, oltre un danno ambientale e sociale devastante, un atto di guerra legittimante una azione di legittima difesa da parte iraniana. L'opzione diplomatica non avrebbe inoltre ottenuto la medesima capacità di rallentamento.

Riagganciandoci all'analisi del caso estone, anche in questa occasione non fu ufficialmente possibile attribuire la responsabilità dell'attacco nonostante i sospetti fossero rivolti verso Stati Uniti ed Israele. È possibile comunque considerare che lo sviluppo di un virus del genere ha probabilmente richiesto dai sei mesi all'anno

di lavoro[327]. Un codice di tale sofisticatezza non poteva inoltre che essere stato scritto da decine di ingegneri informatici e nucleari avvantaggiati presumibilmente da informazioni fornite da apparati intelligence[328]. Non da ultimo i costi di realizzazione sono stati valutati in cento milioni di dollari se non oltre. Tutte capacità nelle disponibilità facilmente di in una superpotenza.

Fatto tesoro di quanto illustrato nel primo capitolo, possiamo tentare di valutare se Stuxnet fosse stato un uso della forza, un attacco armato o un atto di aggressione.

Per gli autori del Manuale di Tallin l'azione, a differenza dell'evento estone, andrebbe configurato come attacco armato se non addirittura come atto di aggressione e questo per una serie di elementi: il danno fisico conseguente all'azione, la reiterazione, l'intenzionalità aggressiva, il danno strategico.

È anche vero però che nel diritto internazionale risulta fondamentale osservare l'atteggiamento degli Stati al fine di capirne le prassi. Nel caso Stuxnet tutte le principali potenze non diedero rilievo all'accaduto e, cosa fondamentale, neanche l'Iran stesso.

Questo perché, al tempo, il non ritenere il cyberspazio quale dominio di azione tutelabile dal diritto internazionale classico portò ad avere criteri per la valutazione dell'aggressione o dell'uso della forza diversi, non ancora ben definiti. Questo oltretutto non solo per impreparazione storica ma tipicamente per un motivo ben preciso che ancora oggi caratterizza le decisioni in tal senso: il non voler disciplinare definitivamente la materia per lasciarsi la libertà di azione nella risposta. La reazione iraniana infatti, da

---

[327] AA.VV., *W32. Stuxnet Dossier*, versione 1.4, 2011, p. 5, disponibile su https://nsarchive.gwu.edu/document/21440-document-44
[328] *Ibidem*, p. 3

quello che sembra, sarebbe avvenuta a distanza di ben due anni[329].

1.3 Sony, 2015

Alla fine del 2014 è avvenuto quello che per molti è stato considerato un unicum storico. Un attacco condotto non nei confronti non di un altro Stato ma di una multinazionale.

Nella ricostruzione dei fatti sembrerebbe che la Corea del Nord abbia attaccato la Sony per un film in uscita in quel periodo[330] al cui interno sarebbe stato raffigurato l'assassinio del leader coreano Kim Jong-Un. L'attacco, durato circa una settimana, ha non solo reso inoperativa la sede americana di Sony ma anche l'intero sistema Hollywoodiano. Vennero infatti trafugati circa 100 terabyte di dati tra email riservate, dati personali, programmi futuri non ancora presentati delle case cinematografiche e film non ancora usciti nelle sale[331].

Le dinamiche iniziali dell'attacco si manifestarono attraverso un sistema spearphishing, dunque tramite l'individuazione di bersagli con tecniche di social engineering, procedendo alla successiva creazione di mail verosimili, nelle quali veniva indicato un link considerabile affidabile dalla vittima. Nel caso di specie si ritiene che il primo target fosse una persona in possesso di elevati privilegi di rete[332]. Una volta entrati, si passò ad una fase

---

[329] NAKASHIMA E., Iran blamed for cyberattacks on U.S. banks and companies, su washingtonpost.com, 2012, disponibile su https://www.washingtonpost.com /world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

[330] "The interview".

[331] Un esempio fu "Fury", di Brad Pitt, scaricato più di 2,3 milioni di volte prima di entrare per la prima volta in una sala cinematografica. PAGLIERY J., 'Sonypocalypse': Why the Sony hack is one of the worst hacks ever, su CNN Money, 2014, disponibile su http://money.cnn.com/2014/12/04/technology/security/sony-hack/.

[332] GILBERT D, NSA monitored North Korean hackers since 2010 but were unable to prevent Sony hack, su ibtimes.co.uk, 2015, disponibile su

bimestrale di osservazione e ricerca vulnerabilità prodromica all'azione vera e propria.

Il 24 novembre del 2014, all'accensione dei pc, più di 7000 dipendenti trovarono un fotomontaggio raffigurante Michael Lynton, all'epoca amministratore delegato, decapitato assieme ad una rivendicazione firmata da tali "guardians of peace" (GOP) nella quale si minacciava la pubblicazione di tutti i dati raccolti nei sistemi Sony se non fossero state esaudite determinate richieste[333].

Come contromisura nell'immediato Sony decise di porre off-line tutto il proprio sistema comportando di fatto un ritorno alla preistoria informatica. I dipendenti dovettero utilizzare carta e penna nonché vennero recuperati device blackberry in disuso[334].

Successivamente, il 27 novembre, i GOP divulgarono alcuni titoli non ancora usciti nelle sale, avvertendo i giornalisti del settore. Fu a quel punto che venne riportata alla luce una dichiarazione di qualche mese prima del portavoce del ministero degli esteri nord coreano in cui veniva annunciato che se Sony non avesse ritirato la pellicola "*the interview*" ci sarebbero state contromisure impietose.

Quando il primo dicembre vennero pubblicati gli stipendi di alcuni dirigenti e di più di 6000 dipendenti della Sony, il governo americano decise di intervenire per il tramite dell'FBI avendo Sony Pictures Entertainment sede negli Stati Uniti. Al Bureau

---

http://www.ibtimes.co.uk/nsa-monitored-north-koreanhackers-since-2010-were-unable-prevent-sony-hack-1484021.

[333] GRIFFIN A, Sony hack: who are the Guardians of Peace, and is North Korea really behind the attack?, in Independent.com, 2014, disponibile su https://www.independent.co.uk/tech/sony-hack-who-are-the-guardians-of-peace-and-is-north-korea-really-behind-the-attack-9931282.html

[334] GILBLOM K., Old BlackBerrys Came to Sony's Rescue After Systems Hacked, su Bloomberg, 2014, disponibile su https://www.bloomberg.com/news/articles/2014-12-31/old-blackberrys-came-to-the-rescue-after-sonys-systems-hacked?utm_source=website&utm_medium=share&utm_campaign=copy.

quantificarono la portata del danno ricevuto con il 75% dei server colpiti resi inagibili, con data center completamente cancellati e dati personali, dalle email ai numeri di previdenza sociale del personale, divenuti di dominio pubblico[335].

Sony, inizialmente reticente ad assecondare le richieste, decise di ritirare il film dalle sale[336] facendo al contempo percepire pubblicamente la sottomissione alle rivendicazioni dei terroristi.

La decisione del ritiro venne valutata dallo stesso Presidente Obama come un grave errore aggiungendo che in considerazione dei danni causati su suolo americano e dell'aver agito contro la libertà d'espressione dei cittadini americani[337], l'America avrebbe risposto in modo proporzionato.

Il Presidente dava per scontata la provenienza Nord-coreana dell'attacco, supportato in questo dalla stessa FBI. Venne a tal proposito ritenuto che un'attribuzione straordinariamente veloce come quella presidenziale, sottintendesse il possesso di più informazioni di quanto pubblicamente comunicato[338] anche in considerazione di quanto emerso da un'operazione intelligence del 2010 che consentì il tracciamento del Bureau121, l'unità elite di cyber spionaggio di Pyongyang[339]. L'FBI, nella persona del

---

[335] CIEPLY M., BROOKS B., Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm, su nytimes.com, 2014, disponibile su https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

[336] KASTRENAKES J., Sony cancels The Interview release after theaters pull out, su theverge.com, 2014, disponibile su http://www.theverge.com/2014/12/17/7412393/sony-cancels-theinterview-release-after-theaters-pull-out

[337] ALLEN Nick, Sony hack: Obama considers 'proportional response' against North Korea, su telegraph.co.uk, 2014, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11302590/Sonyhack-Obama-considers-proportional-response-against-North-Korea.html.

[338] SANGER D., FACKLER M., NSA breached north korean networks before sony attack, officials say, su newyorktimes.com, 2015, disponibile su https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

[339] In particolar modo dal suo ufficio più importante, il Reconnaisance General Bureau, https://irp.fas.org/world/dprk/index.html

Direttore James Comey, non riteneva, oltretutto, ci fosse pericolo di false flag e questo sulla base di materiale in loro possesso[340].

Dalle indagini dell'agenzia federale emerse che il malware utilizzato fosse del tipo wiper, ovvero un software in grado di cancellare i dati dei sistemi, strumento tra l'altro già utilizzato dalla Corea del Nord.

Il malware venne lanciato attraverso computer presenti in vari paesi, tra cui anche l'Italia, per poi trovare una falla nel Windows Management Instrumentation, un gestore di reti aziendali di Windows.

In particolare il malware era in grado di cancellare le informazioni utili all'avvio del sistema operativo rendendo impossibile di fatto l'accensione del terminale infetto.

Il grado di sofisticazione del software ha portato molti esperti a valutare la presenza di un "insider" in Sony anche se la versione governativa ufficiale ha sempre protetto l'integrità americana dando sempre esclusiva colpa alla Nord Corea.

In conclusione analizzando il caso di specie è possibile osservare come vi siano state due fasi principali, una in cui Sony ha tentato di risolvere autonomamente il problema ed una segnata dall'intervento del Governo americano, fase in cui l'attacco ha interessato la sicurezza nazionale oltre l' aziendale.

Nella prima fase sono individuabili due errori fondamentali commessi dalla Sony: il voler sminuire la portata dell'attacco ed il voler gestire esclusivamente a livello interno la crisi.

Va notato infatti che senza l'intervento governativo anche un colosso come Sony non sarebbe stato in grado di respingere un attacco di quelle dimensioni sottolineando l'importanza della

[340] HESSELDAHL A., Details Emerge on Malware Used in Sony Hacking Attack, in vox.com, 2014, disponibile su https://www.vox.com/2014/12/2/11633426/details-emerge-on-malware-used-in-sony-hacking-attack.

cooperazione multilivello. Il caso di specie narra infatti di una cooperazione tra pubblico e privato e di un pubblico che ha consentito l'ingresso dell'interesse nazionale portando scontro e difesa, ad un livello molto più alto.

Rimane anche in questo caso l'apparente insormontabilità dell'attribuzione seppur decantata a toni sicuri dall'amministrazione americana nonostante la mancanza di indagini terze. La mancanza di una attribuzione internazionalmente condivisa comportò, a catena, che la Corea del nord non fu nelle condizioni di qualificare ufficialmente la "risposta proporzionata" americana scagliata sulle reti di Pyongyang tra il 21 e il 22 dicembre dello stesso anno[341].

Quanto sopra, unitamente ai casi precedenti, ben ci fa capire quanto nel cyberspazio non esista una prassi consolidata.

In ognuno dei tre casi esposti vi è stata una qualificazione differente dell'azione: cyber sabotaggio nel caso iraniano, cyber sommossa nel caso estone, cyber spionaggio nel caso americano. Allo stesso modo diverse sono state diverse le reazioni: cyber rappresaglia nel caso iraniano, ricerca di maggiore cooperazione Nato in Estonia, un mix di sanzioni e rappresaglia da parte del governo americano.

Appare dunque chiaro quanto sostenuto da molti studiosi di diritto internazionale ovvero che nell'ambito del cyberspazio, vuoi anche per la giovane età dello stesso, la mancanza di episodi e discendenti reazioni ripetute costantemente nel tempo non consentono la formazione di uno dei cardini del diritto

[341] L'ex presidente americano Obama, a seguito dell'attacco, forte di una provata attribuzione, ha decretato sanzioni nei confronti della Corea del Nord ed una richiesta al Congresso di aggiornamento della legislazione in materia di sicurezza sull'esperienza del caso Sony. FISHER M., North Korea's internet appears to be under mass cyber attack, su Vox.com, 2014, disponibile su http://www.vox.com/2014/12/22/7433873/north-korea-internet-down.

internazionale, la consuetudine. Inoltre la poca trasparenza degli Stati in merito alle procedure messe in atto e la gelosia informativa, difficilmente può consentire una previsione scritta che faccia riferimento.

1.4 Hamas, 2019

Il 2019 ha visto accadere un ulteriore evento di portata storica, dopo quelli iraniano, estone e americano.

Israele, infatti, a seguito di un attacco informatico palestinese, ha risposto abbattendo fisicamente il quartier generale informatico di Hamas. Il contrattacco missilistico ha rappresentato dunque il primo caso di reazione cinetica ad un'offesa cibernetica[342].

Il contrattacco ha avuto il duplice scopo di abbattere una struttura strategica della controparte e quello di limitare la capacità informatica della stessa. L'inedito avvenimento ha stimolato il dibattito circa la legittimità di un conflitto ibrido. L'esercito israeliano (IDF), ha operato con il supporto di un team composto da unità intelligence d'elite[343] e dello Shin Bet[344] provvedendo prima ad alzare gli scudi contro l'attacco informatico e successivamente a bombardare il sito di provenienza dello stesso, localizzato nel quartier generale informatico di Hamas.

Seppur alcuni paesi, Stati Uniti in primis, abbiano incluso nelle loro policy la possibilità di rispondere cineticamente ad un attacco cibernetico, risulta questa la prima attuazione pratica in tal senso

[342] SCALERA L., I missili in risposta a un attacco cyber: così Israele riscrive la cyberwar, su agenda digitale.eu, 2019, disponibile su https://www.agendadigitale.eu/sicurezza/i-missili-in-risposta-a-un-attacco-cyber-cosi-israele-riscrive-la-cyber-war/

[343] Unità 8200, unità militare delle forze armate specializzata in spionaggio SIGINT, ELINT, OSINT.

[344] Agenzia Intelligence per gli affari interni israeliani, corrispettivo del nostro AISI.

e soprattutto realizzata in tempo reale, dunque non come rappresaglia successiva.

Volendo fare il consueto tentativo di inquadramento giuridico internazionale del caso di specie[345], va innanzitutto compreso come sia configurabile l'iniziale attacco informatico di Hamas e sotto quale chiave di lettura una risposta come quella israeliana possa rientrare in quelle legittimate dall'ordinamento ONU.

Hamas, va ricordato, non è una realtà statuale risultando piuttosto essere un NSA (non-state actor). Giustificazione alla risposta israeliana potrebbe allora rinvenirsi in una responsabilità oggettiva dello stato palestinese, come sostenuto dall'Avv. Stefano Mele, presidente della Commissione sicurezza cibernetica del comitato atlantico[346]. Per Mele, al fine di far rientrare la risposta ai sensi dell'art. 51 della Carta ONU, va comunque prioritariamente valutato se l'attacco perpetrato possa essere considerato al pari di un attacco armato. In un'analisi che valuti le conseguenze, va compreso se l'attacco palestinese avrebbe potuto compromettere in maniera seria le strutture israeliane o almeno minare stabilità politica, economica o sociale legittimando in questo caso anche la risposta in assenza di danni fisici tenendo sempre a mente che, come già scritto, per la Corte internazionale di Giustizia l'uso della forza è indipendente dal mezzo utilizzato.

Circa l'elemento della proporzionalità appare chiaro che non sia stata rispettata anche se, come valutato dagli esperti, il porre l'episodio all'interno di una cornice più ampia quale il conflitto arabo-israeliano, potrebbe configurare la distruzione fisica del

[345] v. https://cyberlaw.ccdcoe.org/wiki/Israeli_attack_against_Hamas_cyber_headquarters_in_Gaza_(2019)
[346] v. MIELI R., Israele reagisce a un attacco cyber di Hamas e ne abbatte il quartier generale informatico, su formiche.net, 2019, disponibile su https://formiche.net/2019/05/israele-abbattuto-quartier-generale-cyber-hamas/

quartier generale proporzionata alla portata degli ordinari eventi occorrenti nella zona.

Con questo ennesimo caso si vuole ancora una volta evidenziare quanto la difficoltà di attribuzione e la mancanza di storico rendano difficile l'applicazione del diritto internazionale, classicamente inteso.

Verranno ora analizzate le problematiche di applicazione dei principali istituti correlati alla legittima difesa nel contesto della cyber warfare.

2. Cyber warfare come uso della forza

Nelle discussioni dottrinali, molto tempo si è speso nel tentativo di utilizzare criteri tradizionali per qualificare l'attacco cibernetico come uso della forza.

Il requisito dell'uso della forza viene riproposto più volte nelle previsioni internazionalistiche. La regola 10 del Manuale di Tallin[347] ad esempio sancisce l'illegittimità di un'operazione cibernetica che comporti minaccia o uso della forza ai danni dell'integrità territoriale o l'indipendenza politica di uno Stato. Anche Roscini ritiene che per applicare l'art. 2, § 4 della Carta ONU in occasione di un'operazione cibernetica occorrano tre condizioni[348]:

- Che sia attribuibile ad uno Stato;
- Che consista effettivamente in una "minaccia" o in un "uso della forza";
- Che avvenga in un contesto internazionale.

[347] SCHMITT M.N., Tallin Manual on the International Law Applicable to Cyber Warfare, Schmitt M.N., 2013, pag. 45

[348] ROSCINI M., Cyber operations and the use of force in international law, Oxford, 2014, p. 44-45.

In proposito la regola 11 del Manuale di Tallin riporta che "*un'operazione cibernetica costituisce un uso della forza quando la sua scala e i suoi effetti sono comparabili a quelli di operazioni non cibernetiche che raggiungono il livello di un uso della forza*"[349].

Nonostante i molteplici esempi, riuscire a valutare quando un'operazione cibernetica superi quella soglia che la faccia evolvere ad uso della forza è tutt'altro che automatico.

Pur volendo fare appello al cosiddetto criterio dell'equivalenza cinetica, utilizzato spesso in ambito cyber, le difficoltà di equiparazione rimangono. Va però considerato che essendo quello cibernetico un dominio per sua natura trasversale agli altri, è possibile utilizzare indicatori comuni a tutti i domini al fine di fissare spazio, tempo ed effetti di queste operazioni[350].

Contemporaneamente, vi sono elementi che non sembrano poter aiutare il processo di qualificazione. La presenza di una coercizione[351], ad esempio, sembra fare poco testo in quanto nel corso di una intromissione negli affari interni di un altro Stato essa risulta presente senza che venga ogni volta raggiunta la soglia grave della forza.

Anche utilizzare il fatto che sia presente una Forza armata per qualificare un uso della forza sembrerebbe essere un criterio facilmente aggirabile utilizzando un attore specificatamente ingaggiato attraverso agenzie di intelligence o privati[352].

---

[349] SCHMITT M.N., Tallin Manual on the International Law Applicable to Cyber Warfare, 2013, rule 11 pag. 47

[350] STATO MAGGIORE DELLA DIFESA, Cognitive Warfare. La competizione nella dimensione cognitiva, Ed. 2023, pag. 24, disponibile su https://www.difesa.it/SMD_/Staff/Sottocapo/UGID/Pagine/Centro_Innovazione_Difesa.aspx

[351] ROSCINI M., Cyber operations and the use of force in international law, Oxford, 2014, p. 46.

[352] SCOLART B., Il diritto all'autodifesa nel dominio cyber, Roma, 2020, pag. 41, disponibile su https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/AO_SMD_01_Scolart.aspx

In generale vengono indicati tre approcci per qualificare un atto cibernetico come uso della forza ex art. 2, § 4 della Carta ONU[353].

In primis il c.d. criterio di Schmitt, dal nome del suo ideatore nonché autore dei manuali di Tallin, che misura la vicinanza tra cinetico e non grazie ad una matrice a 8 criteri concorrenti quali "*severity*", "*immediacy*", "*directness*", "*invasiveness*", "*measurability of effects",* "*military character*", "*presumptive legitimacy*" e "*responsibility*", dove la severity è l'entità' delle conseguenze sugli interessi nazionali, l'immediacy è la velocità di manifestazione delle conseguenze, il directenss è il nesso di casualità, l'invasiveness il livello di penetrazione nei sistemi targettizzati, la presumptive legitimacy è il non essere completamente vietati dal diritto internazionale e la responsibility il coinvolgimento di uno Stato. Formato lo schema si prende un atto di riferimento qualificato come uso della forza dalla comunità internazionale e si analizza punto per punto il grado di prossimità[354].

Un secondo approccio è quello c.d. "*target-based*" che non considera gli effetti concreti ma si soddisfa nel momento in cui un'operazione viene indirizzata contro un'infrastruttura critica nazionale. Tale approccio però, focalizzandosi unicamente sull'obiettivo, parrebbe ricondurre nel divieto della Carta ONU anche le operazioni cibernetiche non comportanti danni materiali, come ad esempio quelle di matrice ideologica o degli hacktivists.

Ultimo approccio è invece quello "*instrument-based*", basato sul mezzo utilizzato e sul fatto che tale strumento debba essere

---

[353] *Ibidem*, p. 46-48.

[354] SCHMITT M.N., Computer network attack and the use of force in international law: thoughts on a normative framework, in The Columbia Journal of Transnational Law, Volume 37, 1999, p. 914-916, disponibile su https://nsarchive.gwu.edu/sites/default/files/documents/3460881/Document-04-Michael-N-Schmitt-United-States-Air.pdf

un'arma sulla base dell'intento coercitivo nell'uso della forza armata di cui all'art. 2 della Carta ONU.

In ambito informatico sulla base di questo approccio potrebbe essere qualificato anche un comune PC come arma tranne se decidessimo di adottare la valutazione contemporanea di mezzo e obiettivo. Nell'approccio instrument based infatti è il mezzo che definisce l'uso della forza ma ciò non può evidentemente bastare: lo strumento stesso dovrà prima essere qualificato in base alle conseguenze[355].

Va infine considerato che una grande difficoltà nell'inquadrare le operazioni cibernetiche risiede nell'eterogeneità delle stesse.

Come già visto nel secondo capitolo infatti viene classificata come operazione cibernetica sia l'exploitation, sia una manomissione fisica come nel caso delle centrifughe iraniane[356]. Risulta in ogni caso complesso riuscire ad etichettare un'operazione le cui conseguenze, salvo rari eventi, non comportano conseguenze significative sui servizi alla collettività. È il caso ad esempio dello spionaggio, atto illecito ma non tale da far intraprendere un'azione di risposta basata sul diritto internazionale.

Diverso è il caso in cui si abbia come conseguenza diretta o indiretta la palese neutralizzazione di un'infrastruttura critica come ad esempio è il caso dei sistemi SCADA della centrale di Natanz[357] pur non essendo, nel caso di specie, una struttura vitale per il funzionamento della società.

---

[355] ROSCINI M., Cyber operations and the use of force in international law, Oxford, 2014, p. 50
[356] *Supra*, cap. 3, § 1
[357] *Ibidem*

A tal proposito è oggetto di discussione cosa si debba intendere per infrastruttura critica[358] anche se, come detto, è opinione comune considerare critica quell'infrastruttura infungibile in termini di funzionamento della società e mantenimento della sicurezza interna[359].

Quest'ultimo aspetto è utile per comprendere quanto sia complesso qualificare anche gli obiettivi a seconda del tipo di attacco. Mentre l'obiettivo dell'attacco cinetico può essere un'infrastruttura, l'attacco cibernetico può avere come risultato atteso la compromissione della qualità della vita attraverso un rallentamento delle reti informatiche in uso in società abituate alla condivisione dei dati in tempo reale.

Risulta esemplificativo l'esempio della Borsa. Se il target nel cinetico è la sede fisica, centro nevralgico degli scambi finanziari di un Paese, il successo della missione si realizzerà all'atto della distruzione della struttura. Al contrario un attacco cibernetico, pur non distruggendo l'infrastruttura, potrebbe portare ingenti danni all'economia nazionale arrivando, magari attraverso un attacco Ddos di tipo ramsomware, a poter esercitare pressioni di tipo politico o economico. L'economia, ad esempio, se contestualizzata nell'attacco cinetico è il mezzo attraverso il quale mandare un messaggio, in quello cibernetico diventa l'obiettivo stesso.

In conclusione ad oggi manca una visione condivisa su quale operazione cibernetica possa essere qualificata in maniera tale da rientrare nel divieto ex art. 2 della Carta ONU.

I paesi sembrerebbero evitare, al momento, una classificazione definitiva limitandosi ad una valutazione dottrinale

---

[358] ZIOLKOWSKY K., Computer network operations and the law of armed conflict, in The Military Law and the Law of War Review, Vol. 49, 2010, p. 73-74, disponibile su disponibile su http://www.ismllw.org/REVIEW/2010%20ART%20Ziolkowski.php

[359] *Ibidem*.

ex post caso per caso, lasciandosi piuttosto margine di manovra "in caso d'uso" come nell'esempio della risposta cinetica israeliana all'attacco informatico di Hamas[360].

Una eventuale previsione definita per l'uso della forza in ambito cibernetico, infatti, potrebbe comportare il divieto di utilizzo della stessa come contromisura, stante quanto previsto dal "Draft Articles on Responsibility of States for Internationally Wrongful Acts"[361], un progetto di articoli sulla responsabilità degli Stati per fatti internazionalmente illeciti del 2001 a cura della Commissione di diritto internazionale delle Nazioni Unite al cui articolo 50 viene riportato il divieto di uso della forza nelle contromisure.

Ad ogni modo, facendo tesoro di quanto osservato nel conflitto ucraino, sembra essersi sviluppata la percezione della necessità di allargare le maglie delle previsioni pattizie storiche che al tempo della stipulazione non potevano immaginare gli scenari odierni, come ad esempio lo Statuto di Roma della Corte penale internazionale.

A tal proposito sembra emergere deciso un cambio di atteggiamento, da parte della Corte penale internazionale, in merito al considerare gli attacchi cibernetici non solo equiparabili in taluni casi all'uso della forza cinetica ma addirittura, sull'esperienza della citata crisi ucraina, talmente gravi da poter essere perseguiti come crimini di guerra. Questo cambio di atteggiamento giuridico verrà meglio esposto nei capitoli successivi.

---

[360] *Supra*, cap. 3, § 4.

[361] Commissione di diritto internazionale, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, disponibile su https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

3. La responsabilità internazionale, principi generali

La Commissione di diritto internazionale[362], nel citato Progetto di codificazione sulla responsabilità degli Stati per fatti internazionalmente illeciti approvato nel 2001 (ARSIWA), ha proposto i criteri per l'attribuzione delle condotte illecite a livello internazionale nonché le conseguenze per lo Stato responsabile al fine di garantire al leso la cessazione del comportamento, la riparazione del danno subito nonché il diritto alle contromisure, fatto salvo quanto già previsto dalla Carta ONU.

Il Progetto sancisce che "*ogni atto internazionalmente illecito di uno Stato comporta la responsabilità internazionale di quello Stato*"[363] e che "*un atto internazionalmente illecito è tale quando la condotta, consistente in una azione o in una omissione, in violazione di un obbligo internazionale gravante sul suo autore, è attribuibile allo Stato*"[364].

Si parla dunque specificatamente di Stato e non di un qualunque soggetto diversamente dagli artt. 4, 5 e 8 nei quali si parla di organo dello Stato o di soggetto esercitante funzione pubblica o ancora di soggetto sotto direzione o controllo di uno Stato dunque anche persone fisiche o giuridiche, entità individuali o collettive, come da intendimento della Commissione.

L'art. 4 specifica inoltre che come organo dello Stato vada inteso chi esercita la funzione esecutiva, giudiziaria o qualunque

---

[362] https://legal.un.org/ilc/

[363] Commissione di diritto internazionale, Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001, art. 1: "Responsibility of a State for its internationally wrongful acts – "Every internationally wrongful act of a State entails the international responsibility of that State", disponibile su https: //legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

[364] *Ibidem*, art. 2.

altra funzione a prescindere dalla posizione ricoperta nell'organizzazione[365].

Possono a questo punto essere incluse anche le unità militari operanti in ambito cibernetico come d'altronde risultante anche dal Manuale di Tallin 2.0 in cui, nel commento alla regola 15 "Attribution of *cyber-operations* by State organs"[366], viene citato lo US Cyber Command[367].

Se per tale organizzazione militare il legame statuale è indiscutibile diverso è il problema per gli organi de facto. Nella nota sentenza Nicaragua c. Stati Uniti d'America, la Corte Internazionale di Giustizia ha dichiarato in tal senso che ciò che deve rilevare è la realtà del rapporto.

In caso di una "*complete dependance*", prescindente dalla previsione giuridica, l'organo va considerato come agente proprio[368] e questo anche in considerazione del fatto che, diversamente, gli Stati potrebbero sfuggire alla responsabilità internazionale commissionando operazioni ad intermediari non statali.

Si parla infine di organi "parastatali" operanti in funzione di una delega ricevuta dallo Stato come ad es. i CERT nazionali[369], autorizzati alla difesa di strutture governative.

---

[365] *Ibidem*, *Article 4.*
[366] SCHMITT M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, commento alla regola 15 "Attribution of cyber operations by State organs", § 1, p. 87)
[367] Come anche il Netherlands Defence Cyber Command, dell'Agence nationale de la sécurité des systèmes d'information francese, della Estonian Defence Leagues's Cyber Unit, dell'unità cyber dell'Esercito Popolare di Liberazione cinese, e l'Unità 8200 israeliana.
[368] Corte internazionale di giustizia, case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), sentenza del 27 giugno 1986, ICJ Reports, 1986, § 110.
[369] SCHMITT M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, p. 563

Definiti i principi consuetudinari e in progetto di codifica in materia di responsabilità internazionale, ritengo utile illustrare di seguito quale sia la difficoltà pratica nell'individuare il colpevole e conseguentemente nell'attribuire la paternità dell'azione, azioni prodromiche fondamentali per decidere quale tipo di legittima difesa attivare e soprattutto verso chi.

3.1 Individuazione ed attribuzione della responsabilità

Abbiamo visto come una delle peculiarità della dimensione cibernetica è quella di poter attaccare a grande distanza chilometrica o temporale rimanendo occulti nonché di utilizzare agenti inconsapevoli in diverse nazioni.

Inoltre, in caso di danno derivante da attacco cibernetico, va valutata non solo la plausibile provenienza ma anche il tipo di attacco ricevuto al fine di definire chi sia eventualmente titolato a rispondere, nel caso ci siano i presupposti.

Si attiva dunque un complesso processo di individuazione e di attribuzione definito, dal Dipartimento della Difesa americano, "*trace back*" inteso come "*any attribution technique that begins with the defending computer and recursively steps backwards in the attack path toward the attacker"*[370] dove l'attaccante o il suo intermediario non viene però associato automaticamente ad una persona fisica ma può potenzialmente essere un account, un alias, come anche una posizione geografica o virtuale, nel caso ad esempio di un indirizzo ip.

Il processo di individuazione, fortemente prodromico all'attribuzione, è un attività di natura strettamente tecnica che,

[370] WHEELER D. A. - LARSEN G. N., Techniques for Cyber Attack Attribution, Institute for Defence Analysis, 2003, p. 1, disponibile su https://apps.dtic.mil/sti/pdfs/ADA468859.pdf

sulla base della già citata documentazione americana[371], consta di diverse tecniche quali l'honeypots, il network forensic, la malware analysis, l'intelligence-led attribution[372].

Il successivo processo di attribuzione, sembrerebbe esulare dal mero tecnicismo[373], seguendo la sottile linea rossa che collega l'ideatore alla vittima ed andando nel campo della valutazione giuridica e politica[374]. Ad ogni modo è un processo forense talmente complesso e sfuggente da risultare in un certo senso rassicurante per chi pianifica condotte illecite, come anche per quei paesi che, per aggirare i tempi burocratici dei competenti organi internazionali ed intendendo condurre operazioni difensive più spregiudicate della media a seguito di attacchi informatici pongono in essere operazioni spesso al limite di ciò che possa essere ancora considerato come difensivo-passivo. Si pensi alle covert operations preventive verso siti sospetti[375] attuate al fine di identificare nel più breve tempo possibile una minaccia imminente. Non si parla comunque di attività illecita quanto di necessità scaturente da strette tempistiche a disposizione.

Concludendo, l'essere riusciti ad identificare l'autore non significa automaticamente poter attribuire la responsabilità ad uno

---

[371] *ibidem*

[372] AA.VV., Attribution of cyber attacks on industrial control systems, in EAI endorsed transactions on industrial Networks and Intelligent System, 2016, pp. 1 15, disponibile su https://publications.eai.eu/index.php/inis/article/view/458/352

[373] ROSCINI M., Cyber operations and the use of force in international law, Oxford, 2014, p. 34.

[374] V. MELE S., audizione nell'ambito dell'esame, in sede consultiva, del d.l. 105/2019, concernente "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (C.2100), disponibile su https://webtv.camera.it/evento/15163

[375] BOEBERT W.E., A Survey of Challenges in Attribution, in National Research Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington, DC, 2010, p. 48-49, disponibile su https://doi.org/10.17226/12997

Stato mandante e forse questo rimane ancora oggi il principale nodo da dirimere.

4. Il principio di proporzionalità della legittima difesa.

Uno dei principi cardine della legittima difesa, il principio di proporzionalità, trova specifiche difficoltà applicative in ambito cibernetico.

Come già detto, una volta che l'azione, cinetica come virtuale, venga qualificata come attacco armato, in automatico viene legittimato anche il diritto di autodifesa.

A tal proposito, in ambito cibernetico forse ancor più' che in ambito tradizionale, l'attribuzione, come visto, assume enorme importanza. Attribuzione e qualificazione della natura dell'attacco sono requisiti fondamentali per l'autodifesa, in primis al fine di colpire il responsabile ma anche per decidere il tipo di contro-attività' da porre in essere al fine di non incappare in una violazione dei canoni internazionalistici.

Abbiamo a tal proposito due elementi da valutare: il responsabile, o *attaccker attribution*, e la natura dell'attacco, o *attack attribution*[376].

La rapidità di esecuzione di un attacco informatico, inoltre, come anche i tempi di valutazione ufficiale della portata dei danni, comportano spesso l'impossibilità di una qualsiasi azione preventiva sulla base di un "early warning".

Un sistema di sicurezza collettivo che consenta l'identificazione di un intento ostile già nel momento di una iniziale introduzione in un sistema strategico nazionale ed una conseguente autodifesa

[376] BRENNER S. W., At light speed: Attribution and response to cybercrime/terrorism/warfare, in Journal of Criminal Law and Criminology, 2007, disponibile su https://scholarlycommons.law.northwestern.edu/jclc/vol97/iss2/2/

immediata comporterebbe una maggiore capacità di mitigazione dell'eventuale danno. Tale visione non a caso rispecchia quella delle peace operations cooperative di cui ai Manuali di Tallin.

5. La difesa in un attacco imminente

Il concetto di "*early warning",* citato nel paragrafo precedente, ha comportato non poche discussioni in dottrina per comprendere se la legittima difesa possa essere esercitata già in caso di minaccia imminente o necessiti comunque di una valutazione post attacco. Si tenterà allora di comprendere se sia accettabile, ai sensi del diritto internazionale, la contromisura attivata sulla base di un danno non ancora subito e se il contesto cibernetico necessiti di previsioni specifiche.

L'interpretazione letterale del "*if an armed attack occurs*" nell'art. 51 della Carta sembrerebbe prevedere l'attacco avvenuto rendendo di fatto la difesa a titolo precauzionale non percorribile.

Va inoltre considerato che un contrattacco preventivo, per quanto lanciato al fine di depotenziale la minaccia, potrebbe al contrario portare ad una escalation nonché ad una paradossale inversione delle parti, dove cioè il contrattacco, derogando a necessità e soprattutto proporzionalità, diventerebbe esso stesso casus belli causante danno effettivo, finendo per consentire la legittima difesa di chi prima attaccava.

Volendo cercare una logica in questo tipo di azione va detto che è comunque irrealistico pensare che uno Stato, sapendo di essere bersaglio di un imminente attacco, decida di attendere il danno e dunque, in caso di difesa preventiva, almeno il principio di necessità potrebbe forse trovare giustificazione.

Circa la proporzionalità, per quanto sia possibile una valutazione, si potrebbe far riferimento a quanto inevitabilmente compromesso in caso di attacco avvenuto.

In ambito cibernetico l'autodifesa preventiva, intesa come capacità di arrestare un imminente attacco, è sicuramente pratica diffusa in particolar modo da quei paesi, come gli Stati Uniti, che godono di più ampi margini di azione operativa, come nel caso della comunità intelligence americana.

Si tende a distinguere in tal senso l'autodifesa "*preventiva*", quale risposta ad un plausibile attacco e l'autodifesa "*anticipatoria*" intesa come risposta ad una reale, tangibile, imminente minaccia[377].

In condizioni normali non è ad oggi accettata una difesa basata su una valutazione ex ante del danno ricevuto, restano dunque validi i principi ottocenteschi derivanti dalla cd. "dottrina Caroline"[378]. Va però detto, per completezza di informazione, che c'è stato un periodo, relativamente recente, in cui gli Stati Uniti, grazie alla c.d. dottrina Bush, tentarono di legittimare la teoria della risposta preventiva, riuscendo anche a convincere la maggioranza della Comunità internazionale.

---

[377] REISMAN M., ARMSTRONG A., The Past and Future of the Claim of Pre-emptive Self-Defense, in American Journal of International Law, Loyola university, New Orleans, 2006, p. 526, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2169416

[378] Nel 1840, il segretario di Stato americano Daniel Webster, in occasione degli eventi sopravvenuti a seguito della distruzione della Nave Caroline da parte di soldati britannici in territorio statunitense, definì il perimetro in cui fosse giustificato l'uso della forza in legittima difesa, asserendo che il governo britannico, per scagionare i propri sudditi, avrebbe dovuto dimostrare "necessity of self-defence instant, overwhelming, leaving no choice on means and no moment for deliberation". Su tale esternazione si basano ancora oggi i principi legittimanti il ricorso all'autodifesa in risposta ad un attacco armato.

5.1 La dottrina americana della risposta preventiva

Un esempio scolastico di autodifesa preventiva, dunque in relazione ad una plausibile minaccia non immediata, risiede principalmente nella cosiddetta dottrina Bush come anche in linee di condotta tenute in occasione di altri storici eventi che hanno riguardato gli Stati Uniti: in primis la lotta al terrore con l'operazione "enduring freedom" e successivamente la lotta alla proliferazione delle armi di distruzione di massa nei confronti, in particolar modo, di Iran, Iraq e Corea del Nord.

Il periodo storico riguardante l'operazione Enduring freedom rappresentò un cambio paradigmatico nella percezione del fenomeno terroristico e un caso di studio circa una concezione dell'autodifesa per alcuni versi inedita. Il consiglio di sicurezza ONU, nel 2001 con risoluzioni n. 1368 e 1373, adottate all'unanimità rispettivamente il 12 ed il 28 settembre dello stesso anno, riconobbe l'autodifesa, individuale o collettiva, come misura utilizzabile in caso di attacchi terroristici.

La legittima difesa si ritrovava dunque a non dover più discendere unicamente da un attacco subito da uno Stato. Altrettanto inusuale fu la funzione preventiva che gli Stati Uniti vollero dare all'operazione.

Lo scopo, infatti, non fu tanto una risposta diretta[379], ma un chiaro messaggio deterrente verso futuri attacchi, con un'operazione oltretutto ampiamente supportata in quel caso dalla comunità internazionale. Sulla stessa linea si pose l'Inghilterra la cui partecipazione venne finalizzata ad evitare attacchi da parte di Al Qaeda sul proprio territorio.

[379] In particolar modo non verso l'Afghanistan in quanto "*Stato*" non essendo, lo stesso, autore diretto degli attacchi

Si aggiunga che l'operazione venne qualificata come generica lotta al terrore andando a completare il quadro di una legittima difesa nuova i cui elementi di rottura erano rappresentati dall'agire ad attacco terminato, in maniera preventiva e deterrente per il futuro, verso entità non statuali e, in aggiunta, senza una precisa durata temporale.

L'approccio sopra illustrato, nonostante l'iniziale approvazione unanime, generò non poche polemiche in merito alla forte discrezionalità nella valutazione della possibilità di un futuro attacco considerando oltretutto che il punto di vista americano sembrava non reputare fondamentale una evidenza riguardante il dove e il come di un attacco che di fatto non era ancora avvenuto.

Fu l'espressione forse più generalista possibile di una legittima difesa preventiva che si accontentava della probabilità di accadimento più che dell'imminenza dello stesso. Tale discrezionalità portò ad un altro storico e controverso caso di studio ovvero la lotta alla proliferazione delle armi di distruzione di massa.

L'evento infatti che forse più di tutti caratterizzò la definizione di legittima difesa preventiva fu l'attenzione degli Stati Uniti verso il pericolo delle armi di distruzione di massa in particolar modo nei confronti di Iraq, Iran e Corea del Nord.

La nuova sensibilità verso il terrorismo e la paura di un uso improprio di armi ad alto grado di letalità da parte di organizzazioni terroristiche fecero valutare la necessità di una rivisitazione della normativa esistente in tema di legittima difesa. In particolar modo si chiedeva la valorizzazione del concetto di "attacco imminente" al fine di agevolare l'iter della difesa preventiva già sperimentata in occasione dell'attacco alle torri gemelle ma non ancora effettivamente normata in merito ai requisiti legittimanti.

A livello internazionale, questa volta, forti furono le resistenze a questa visione. Nel 2004 un Panel di esperti in materia si espresse in maniera contraria alla dottrina americana valutando non applicabile il diritto alla legittima difesa in caso di pericolo non imminente ed anche ci fossero state evidenze, non sarebbe stata giustificata una difesa di tipo soggettivo e discrezionale restando nelle mani del consiglio di sicurezza ONU ogni decisione finale in merito.

In linea di massima nonostante fosse stata sostenuta fortemente l'operazione Enduring freedom ad un più freddo esame la comunità internazionale si espresse come contraria ad una legittima difesa che non derivasse da un attacco già in corso o per lo meno imminente.

In virtù di quanto esposto e nel merito dell'ambito cyber, ritengo che nonostante possa essere auspicabile consentire una più rapida valutazione degli attacchi cibernetici in entrata, non risulta ad oggi possibile giuridicamente agire preventivamente basandosi su fattori quali, ad esempio, le astratte capacità offensive di una determinata entità.

La comprovata realtà ed imminenza di un attacco consente invece l'allertamento di tipo anticipatorio, mantenendo salde, in ogni caso, le competenze del Consiglio di sicurezza ONU.

6. Il problema della difesa attiva e l'etica dell'hacking back

Come visto, l'inesistenza di una prassi internazionale relativa alla legittima difesa in ambito cyber warfare non consente di aprire una discussione, de iure condendo, circa accordi o normative di portata internazionale in tema di responsabilità e autodifesa.

L’incertezza si ripercuote inevitabilmente anche a livello operativo nel momento in cui si debba decidere il livello della risposta e questo in particolar modo in ambito cibernetico dove il danno tipico non comporta conseguenze fisiche nell’immediato a cose o persone ma si configura comunque come un’ingerenza negli affari interni di un altro Stato.

Ci si chiede dunque se anche un evento di questa natura, in apparenza meno eclatante, sia configurabile come attacco armato degno di risposta immediata da parte dello stato vittima.

Se il poter essere legittimati alla risposta potrebbe sembrare a questo punto già un grande passo, sorgono ulteriori nodi normativi da sciogliere.

Abbiamo visto che, in particolar modo nella dottrina americana, le metodologie di difesa cibernetica vengono racchiuse sotto le Computer network operations, all’interno delle quali vengono distinte la Computer Network Defence (CND), la Computer Network Exploitation (CNE) e il Computer Network Atack (CNA). Mentre le CND comportano un atteggiamento passivo di difesa fisica o logica, con le CNE e soprattutto con le CNA si passa ad una difesa attiva, tecnicamente detta *active cyber defence*, comportante l’intrusione del sistema esterno.

Ancora più nello specifico l’exploitation è di fatto un’attività ispettiva clandestina, attività equiparata a tutti gli effetti ad una forma di spionaggio. L’attività di exploitation, che sia in risposta o meno ad un attacco, è attualmente attività internazionalmente molto praticata in quanto, grazie allo sviluppo della tecnologia e all’aumento dei dati memorizzati on line, risulta essere estremamente redditizia in termini di informazioni raccolte.

Un’exploitation finalizzata alla conoscenza delle capacità avversarie che non comporti danno e che venga eseguita al fine di calibrare la risposta ad un attacco informatico potrebbe in un

certo senso rientrare nella logica del conflitto ed essere giustificata dalla necessità di mitigare il danno. Diverso sarebbe il caso di un'attività di CNE al di fuori di questo contesto cosa che la farebbe sfociare nello spionaggio internazionale.

Per spionaggio internazionale infatti si intende l'esplorazione delle intenzioni e delle azioni politiche, economiche e militari del nemico, nel suo territorio, per riferirne ai propri connazionali, con l'intento di nuocere[380]. Essendo attività tipicamente occulta non viene tra l'altro considerata spia chi svolge attività di ricerca informativa in uniforme o chi risiede sul territorio avversario salvo agire sotto falsi pretesti[381].

A tal proposito è interessante riportare le diverse definizioni date allo spionaggio, attività praticata fin dagli albori dei conflitti bellici, per comprendere, se mai ce ne fosse bisogno, come nella comunità internazionale, anche tra storici alleati, manchino vocabolari comuni. Il Sistema italiano di informazioni per la sicurezza parla infatti di "*attività condotte da agenzie intelligence straniere nonché da individui od organizzazioni operanti in modo autonomo ovvero in collegamento con servizi di informazione esteri al fine di acquisire notizie in danno della sicurezza nazionale*"[382], nozione che sembrerebbe non considerare l'elemento della clandestinità.

Il Dipartimento della difesa americano parla invece di "*act of obtaining, delivering, transmitting, communicating, or receiving*

[380] PRETO P., Le parole dello spionaggio, in Per Aspera ad Veritatem, 1996, disponibile su https://gnosis.aisi.gov.it/sito/rivista6.nsf/servnavig/5

[381] Protocollo I addizionale alle convenzioni di Ginevra del 12 agosto 1949, relativo alla protezione delle vittime di conflitti armati internazionali, 1977, entrato in vigore il 7 dicembre 1978, art. 46 disponibile su https://unipd-centrodirittiumani.it/it/strumenti_internazionali/Protocollo-I-addizionale-alle-convenzioni-di-Ginevra-del-12-agosto-1949-relativo-alla-protezione-delle-vittime-dei-conflitti-armati-internazionali/135.

[382] Il linguaggio degli organismi informativi. Glossario intelligence, 2013, disponibile su https://www.sicurezzanazionale.gov.it/sisr.nsf/wpcontent/uploads/2013/12/Glossario-intelligence-2013.pdf

information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation»[383], concentrandosi più sulla Difesa stessa che sulla sicurezza nazionale.

Da quanto sopra esposto si comprende quanto sia complicato ricevere una copertura legittimante e dunque non essere imputabili di reato nel momento in cui un operatore cyber si trovi a dover operare in un contesto tipicamente clandestino e caratterizzato dall'intrusione nei sistemi altrui.

Ancora più eclatante è il caso delle attività successive l'Exploitation ovvero quelle configurabili a tutti gli effetti come attacco in considerazione in particolar modo del problema della proporzionalità.

Mettendo il caso che un paese vittima sia riuscito ad identificare, attribuire e valutare la portata dell'attacco nonché' ricevere legitimizzazione internazionale per la difesa, dovrà rispondere in maniera proporzionata a quanto subito secondo i tipici canoni internazionalistici.

Sforare quel limite, ricordando che nel cyberspazio azioni e danni possono essere visibili anche in maniera differita nel tempo, comporterebbe però passare nella veste di attaccante, con tutti i già citati pericoli di escalation internazionale.

È oltremodo complicato, nel cyberspazio, fare una preventiva distinzione tra spionaggio e attacco, distinzione che nel mondo "fisico"[384] è decisamente più agevole. In tal senso basti pensare

---

[383] U.S. Department of Defense, Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms, 2010, p. 80, disponibile su https://irp.fas.org/doddir/dod/jp1_02.pdf

[384] BROWN G., Spying and fighting in cyberspace: what is which?, in Journal of National Security Law & Policy, Vol. 8, 2016, p. 624-625, disponibile su

che lo scoprire un accesso non autorizzato ad un sistema informatico protetto non ci consente di sapere in anticipo se tale accesso serva unicamente allo studio della rete, ad un'esfiltrazione di informazioni o paradossalmente alla predisposizione di un blocco successivo della rete stessa in grado di causare danni fisici.

La vera differenza tra spionaggio e attacco cibernetico viene in evidenza nella fase di danneggiamento che nello spionaggio consiste nel reperimento di informazioni compromettenti la sicurezza nazionale avversaria e nell'attacco nella compromissione di sistemi informatici come anche nel danneggiamento fisico di sistemi industriali strategici, come nel caso della centrale nucleare di Natanz.

Il problema che in questa sede rileva è quello del rispetto della proporzionalità nella c.d. attività di hack back. L' hack back consiste in un attacco proporzionato ad un altro ricevuto e che si attiva solo in tale situazione. Dunque una forma difensiva che non si limita ad assorbire il colpo ma provvede ad assestarne un altro in risposta. È però di fondamentale importanza avere sempre ben visibile la sottile linea rossa esistente tra difesa passiva, difesa attiva e attacco.

Dorothy Denning, uno dei massimi esperti americani di cybersicurezza, definisce la difesa attiva cyber come un'azione difensiva posta in essere per distruggere, annullare e ridurre la quantità di minacce cibernetiche contro assetti e forze amiche[385].

---

https://jnslp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf

[385] DENNING D.E. - STRAWSER B.J., Active Cyber Defense: Applying Air Defense to the Cyber Domain, in Carnegie Endowment for International Peace, 2016, disponibile su https://carnegieendowment.org/2017/10/16/active-cyber-defense-applying-air-defense-to-cyber-domain-pub-73416

Denning, in un parallelo cinetico, spiega che mentre inviare missili nello spazio altrui è un attacco, monitorare gli stessi è una difesa passiva mentre abbatterli è una difesa attiva[386]. Da qui si comprende inoltre il perché la citata attività di exploitation finalizzata alla conoscenza può risultare approvabile nella logica delle operazioni belliche.

Sempre Denning evidenzia l'importanza di non confondere, come spesso accade, la difesa attiva con la tecnica di hacking back (HB). L'HB consiste a tutti gli effetti in un'intromissione di sistema altrui e qualora effettuato senza legittimazione ufficiale, come nel caso di un'azienda privata sotto attacco, ben facilmente si configura come fattispecie penalmente sanzionabile.

Forme di difesa attiva aggressiva vengono spesso equiparate all'hacking back ma la differenza risulta molto sottile in quanto in generale l'attività di hackeraggio finalizzato a tutto ciò che vada oltre il semplice monitoraggio della capacità avversaria, dunque anche il danneggiamento dei sistemi altrui, è fondamentalmente considerato illegale.

Un esempio chiarificatore fu quello dell'hacker russo che inoculò malwares in computer governativi della Georgia. Il malware agì cercando nei sistemi documentazione attraverso una ricerca semantica di termini come "USA" e "Nato", esfiltrando la documentazione di interesse su un server dedicato. Il governo Georgiano agì in risposta inserendo, nei propri sistemi compromessi, uno spyware in un file nominato "Georgian Nato Agreement". L'hacker russo sulla base della presenza del termine Nato portò il file sul proprio server e una volta trasferito lo

[386] BERINATO S., Active Defense and "Hacking Back": A Primer, in Harward business review, 2018, disponibile su https://hbr.org/2018/05/active-defense-and-hacking-back-a-primer

spyware attivò la webcam consentendo di avere la prova del furto nonché' le generalità fisiche dell'autore[387].

L'attività posta in essere dalla Georgia, in difesa di un attacco in corso, non può essere considerata come hack back ma come difesa attiva. Innanzitutto la Georgia ha inserito lo spyware nei propri sistemi, non andando a introdursi in una rete esterna. Si trattò ad ogni modo di una risposta governativa e non privata.

In questo senso è interessante come si parli spesso di etica dell'hacking back. Gli esperti ritengono che tecniche di difesa aggressiva poste in essere senza autorizzazione legale o cooperazione governativa che vadano a sfociare in un attacco siano antietiche in particolar modo al di fuori dei propri confini. Sono operazioni oltretutto difficili da legittimare ex post. È anche questo uno dei motivi che non consente la velocità di risposta che lo spazio cibernetico richiederebbe.

È risaputo che l'attività di hacking back viene effettuata soprattutto da paesi più spregiudicati in materia rimanendo un problema invece in paesi come il nostro nel quale i confini della legittima difesa sono di forte derivazione costituzionale, connotati dall'inderogabile ripudio della guerra.

In Italia l'azione aggressiva di difesa cibernetica desta non poche ritrosie a livello giuridico in quanto ritenuta pericolosa e potenzialmente dannosa in particolar modo per il potenziale coinvolgimento di attori inconsapevoli. Si pensi ad un attacco Ddos che, essendo per sua natura distribuito, arrivi a coinvolgere computer di privati cittadini o server di ospedali[388].

---

[387] ANDERSON N., How Georgia doxed a Russian hacker (and why it matters), in Ars Technica, 2012, disponibile su https://arstechnica.com/tech-policy/2012/11/how-georgia-doxed-a-russian-hacker-and-why-it-matters/

[388] Nel 2014 Microsoft ha preso il controllo di 23 domini internet dell'azienda Vitalwerks reputata erroneamente complice di un'organizzazione hacker. L'errore, poi riconosciuto, ha comportato le scuse pubbliche di Microsoft,

Non a caso gli esperti, nazionali ed esteri[389], consigliano alle grandi aziende che siano potenziali bersagli internazionali, di porre in essere unicamente atti di difesa passiva senza intraprendere, ad esempio attraverso società private, attacchi in risposta. A tal proposito spesso si sottovaluta il senso di giustizia che porta ad operare autonomamente, in particolar modo a seguito di attacchi ramsomware[390].

La reazione, perpetrata fuori dall'autorizzazione governativa, nel momento in cui fuoriesce dal canone della proporzionalità, è ad oggi penalmente incriminabile, nel nostro paese ex artt. 615 ter e quater del Codice penale ed a livello internazionale in nome del divieto di ingerenza negli affari interni altrui.

Ad oggi, inoltre, risulta complesso far valere la violazione di norme di diritto internazionale in particolar modo nei casi, come quello georgiano, in cui la soglia del danno non raggiunga l'uso della forza o si faccia fatica a dimostrare l'ingerenza negli affari interni o comunque una compromissione della sovranità. Una più attenta analisi in tal senso verrà effettuata nei capitoli successivi.

7. La legittima difesa cibernetica in forma collettiva

Se già possa sembrare complesso ravvedere gli estremi legittimanti un'eccezione al divieto all'uso della forza ai sensi della Carta delle Nazioni Unite, forse ancora più sfidante è riscontrare tali presupposti in caso di un intervento collettivo a difesa di un paese attaccato.

---

https://blogs.microsoft.com/blog/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption/

[389] a tal proposito l'Australia nelle parole del capo dell' Australian Signals Directorate nel 2018 ha espresso un interessante punto di vista circa l'opportunità di non rispondere personalmente ad attacchi hacker, disponibile su https://www.cybersecurity.it/hack-back-laustralia-dice-no-alla-legittima-cyber-difesa/

[390] V. a tal proposito LIN P., Ethics of Hacking Back, in U.S. National Science Foundation, 2016 disponibile su http://ethics.calpoly.edu/hackingback.pdf

Anche in questo caso si necessita fare un breve richiamo alla casistica cinetica.

È bene ricordare che l'art. 51 della Carta ONU prevede, oltre la difesa individuale, anche quella collettiva attraverso Stati terzi che si attivano in supporto di uno Stato colpito.

Ad integrazione dei presupposti previsti per la legittima difesa individuale, la collettiva, come specificato dalla Corte Internazionale di Giustizia nella sentenza Nicaragua vs. Stati Uniti, prevede che lo stato bersaglio, una volta che abbia dichiarato di essere vittima di quello che si configura come un attacco armato di provenienza esterna con perdita totale o parziale di controllo di una porzione di territorio, e quindi con tutte le difficoltà di equiparazione cinetica, richieda l'assistenza di atri Stati.

Oltre l'art. 51, al fine di meglio assicurare la mutua assistenza in caso di bisogno, tale dispositivo è oggetto di ulteriori trattati tra cui, esempio noto, il trattato NATO, in particolar modo all'art. 5. Sono trattati che richiedono un'interpretazione comunque conforme alla carta ONU.

Dati come assodati anche in questo caso i principi ottocenteschi di necessità, proporzionalità e immediatezza della risposta va ora compreso quali siano le difficoltà di applicazione di suddetti parametri al cyberspazio in primis per la mancanza di confini definiti dello stesso.

La questione soprariportata è tutt'altro che banale parlando di attacchi informatici in quanto, si pensi ad un attacco Ddos, al fine di perpetrare un attacco ad uno Stato membro ONU può essere, colpito, spesso inconsapevolmente dalla vittima, un sistema di

uno Stato prossimo al target, si pensi alla Svizzera in un attacco al cuore dell'Unione Europea[391].

Una volta presa coscienza dell'attacco si tratterà di aiutare lo Stato colpito applicando possibilmente in maniera estensiva, le previsioni del diritto tradizionale che benché' all'art. 51 parli esplicitamente di attacco già sferrato ad uno stato membro ONU, è opinione diffusa della dottrina che la legittima difesa possa essere fatta valere anche da non appartenenti dell'Organizzazione[392] considerando questa visione diritto internazionale generale.

È in tal senso opportuno ricordare infatti che il diritto naturale alla legittima difesa scaturisce non tanto dall'art. 51 quanto dall'art. 2, § 4, che vede il divieto di uso della forza quale diritto cogente e dunque invocabile universalmente.

In generale non sembrano esistere ad oggi previsioni di specie per l'ambito cibernetico ulteriori a quelle del mondo fisico, permanendo la condizione fondamentale che l'intervento vada svolto nell'esclusivo interesse dello Stato attaccato il quale sarà l'unico ad avere l'onere di valutare l'esistenza delle stesse condizioni previste per la fattispecie individuale e che, ad integrazione, valuti di non poter far fronte autonomamente alle minacce comunque già in corso.

Uno dei primi storici elementi di valutazione circa l'interesse ad intervenire è stato quello della contiguità geografica. Trattasi a parere dello scrivente di un elemento anacronistico in quanto di pura derivazione cinetica. In passato infatti la vicinanza territoriale offriva naturale interesse a che i propri confini non

[391] Oltre la Svizzera, si richiama il caso di Serbia e Montenegro che non hanno goduto della continuità dello status della Jugoslavia a seguito dello smembramento.
[392] LAMBERTI ZANARDI P., La Legittima difesa, cit., Milano, 1972, pagg. 290 e segg.

venissero coinvolti negli scontri. Successivamente la vicinanza territoriale è stata superata da quella politica degli stati che, seppur non facendo parte della medesima organizzazione regionale, stipulavano accordi di mutua assistenza ad hoc.

Gli esempi storicamente più evidenti sono sicuramente il Patto Atlantico ed in contrapposizione quello di Varsavia. Nel contesto cyberspaziale le componenti territoriali naturalmente non hanno più senso vista la mancanza di confini fisici che caratterizza tale dominio, ma sembra avere importanza secondaria anche l'appartenenza ad organizzazioni o patti. Viene fatta invece una valutazione caso per caso, forse anche opportunistica, in quanto, l'attacco ad un paese può risultare funzionale al raggiungimento di un altro non necessariamente perché contiguo fisicamente, politicamente o ideologicamente. Ne sono esempio gli attacchi degli hacker etici, almeno apparentemente non sotto il controllo di attori statuali, contro multinazionali o organizzazioni aventi interessi reputati, per fare un esempio, non ecologici.

L'attacco ad una multinazionale cinese con sedi sparse nel mondo può comportare ripercussioni anche al paese ospitante una di queste e che abbia messo a disposizione spazio nella dorsale informatica locale.

In generale dunque non si ravvedono ad oggi particolari adempimenti circa l'intervento in supporto di stati attaccati che non siano quelli già previsti "tradizionalmente" nella misura della richiesta di aiuto.

Il Cyberspazio è a tutti gli effetti un dominio fortemente interdipendente dove le azioni verso un paese possono avere conseguenze globali. Pur non essendo stato definito a livello internazionale il problema dell'intervento multiplo sicuramente dare un'interpretazione della legge che non consenta l'azione

collettiva comporterebbe il lasciare indifesi molti Stati non informaticamente capaci.

Ciò che rileva in ambito cyberwarfare, a parere dello scrivente, è che la capillarità delle reti può comportare che più paesi contemporaneamente siano fatti oggetto di attacco e che lo stesso non raggiunga la soglia del riconoscimento dell'attacco armato.

Poniamo dunque il caso che tutti questi paesi facciano formale richiesta di supporto. Quale potrebbe essere il discrimine per individuare uno stato "particolarmente leso" tra quelli colpiti?

La risposta è tutt'altro che scontata in primis per i tempi di valutazione del danno subito e successivamente anche per la possibilità che l'attivazione dei dispositivi offensivi non avvenga simultaneamente all'inizio dell'attacco ma in maniera differita, come nel caso dei malwares dormienti.

Si ritiene dunque che in caso di più paesi colpiti non esistano criteri oggettivi ufficialmente definiti circa la priorità di intervento quanto invece una valutazione caso per caso che tenga conto del danno già ricevuto, dei danni potenzialmente in divenire e soprattutto degli interessi strategici multinazionali a livello Stato o Organizzazione.

Sicuramente ciò che ad oggi ancora manca è una previsione unitaria, non a caso anche il Segretario Generale della Nato Jens Stoltenberg, già dal 2001, ha più volte ribadito la necessità di norme condivise circa le azioni offensive nel cyberspazio ad esempio attraverso un trattato di portata planetaria[393]. Si percepisce l'urgenza di una previsione pattizia, mancando anche quella consuetudinaria specifica in materia, anche per avere certezza di cosa debba attivare eventuali dispositivi di mutuo

[393] NATO, discorso del Segretario generale NATO Jens Stoltenberg seguito da domande e risposte al terzo "3rd German Ecumenical Church Days", 15 maggio 2021, disponibile su https://www.nato.int/cps/en/natohq/opinions_183679.htm

soccorso tra Stati, avendo a riferimento sicuramente le Carte ONU e Nato ma anche la sensibilità sulle criticità infrastrutturali delle reti mondiali post pandemia.

Allo stesso modo anche altri membri ONU, in particolar modo Cina e Russia, hanno sottolineato la necessità di definire, in forma di accordo, la governance dello spazio virtuale, pur senza superare le divergenze nelle visione della convivenza giuridica tra cyberspazio e diritto internazionale, a cui si rimanda nei paragrafi a seguire.

8. Il dibattito mondiale su diritto internazionale e cyberspazio.

Come osservato, il mondo del cyberspazio è caratterizzato dalla mancanza di norme definite nonché' dall'impossibilità, al momento, che si generi una qualsiasi forma di consuetudine.

Questo però non deve far pensare che non vi sia discussione in merito o che non venga sentita la necessità di previsioni scritte. Paesi come Cina e Russia[394], hanno avuto uno sviluppo significativo delle capacità informatiche, cosa che ha contribuito ad alimentare la discussione in merito all'applicazione del diritto internazionale in questo contesto.

È opinione comune infatti che sia necessaria una previsione pattizia che definisca specificatamente le linee di condotta e che l'interpretazione estensiva di quanto esistente non sia sufficiente per la velocità di evoluzione degli eventi.

Ciò che è certo è che l'arena cibernetica è ad oggi una zona grigia di forte competizione strategica in particolar modo da quei

[394] National Intelligence Council - U.S. Office of the Director of National Intelligence, Cyber Operations Enabling Exspansive Digital Authoritarianism, 2020, declassificato il 5 ottobre 2022, disponibile su https://www.odni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407–2022.pdf

paesi che mirano alla predominanza a livello globale in tema di sicurezza nazionale.

Come la Cina è ad oggi leader nello sfruttamento delle vulnerabilità in particolar modo nelle attività di exploitation, allo stesso modo la Russia ha nel tempo accumulato massive capacità informatiche orientate in particolar modo allo spionaggio digitale e alla guerra dell'informazione attraverso propaganda, contropropaganda e disinformazione[395].

È chiaro dunque che queste capacità siano una fortissima arma di politica estera spendibile sotto forma di minaccia anche a fini di deterrenza e mantenimento dell'equilibrio internazionale. È altrettanto chiaro quanto si necessiti una previsione univoca, meglio se a mezzo accordo, da richiamare in caso venga superato qualche labile confine.

Dopotutto le attività di ingerenza informatica sono state costantemente praticate nel tempo, una su tutte la recente azione di alcuni elementi, apparentemente affiliati al governo russo, che avrebbero colpito pesantemente il sistema elettorale americano[396].

La consapevolezza di una perpetrata ingerenza su suolo americano ha portato ad esempio l'attuale presidente Biden a sollecitare più volte la controparte russa ad un atteggiamento proattivo contro i gruppi ramsomware operanti sul proprio

---

[395] NOCETTI J., Cyber Power, Routledge Handbook of Russian Foreign Policy edited, 2018, disponibile su https://www.taylorfrancis.com/chapters/edit/10.4324/9781315536934-13/cyber-power-julien-nocetti.

[396] U.S. Senate Select Committee on Intelligence, "Russian Targeting of Election Infrastructure During the 2016 Election: Summary of Initial Findings and Recommendations", 2018, disponibile su https://www.intelligence.senate.gov/publications/russia-inquiry; U.S. Senate Select Committee on Intelligence, report "RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION", 2020, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.

territorio, non mancando di preannunciare azioni in difesa del popolo e delle infrastrutture critiche del paese sfide[397].

La presidenza americana ha inoltre adottato un atteggiamento informaticamente più aggressivo del solito in risposta a specifici attacchi della controparte quali in particolar modo i più noti solarwinds[398], Colonial Pipeline[399], REvil[400] o Republican National Commitee[401]. Questo in parte per mitigare le minacce, in parte per mandare un messaggio finalizzato alla deterrenza, in una sorta di rinnovata guerra fredda.

Osservare la provenienza delle minacce impone l'adottare un orizzonte di livello mondiale. Nel 2022 sono state infatti realizzate ben 147 operazioni offensive informatiche esterne ai paesi colpiti e ritenute rilevanti[402], provenienti, in particolar modo da Cina, Iran e Corea del Nord.

Quanto sopra per comprendere il perché della accresciuta sensibilità di tutti i paesi in tema di difesa cibernetica internazionale e del bisogno di una previsione giuridica unica che vada finalmente oltre la dottrina dei manuali di Tallin.

---

[397] The White House, Background Press Call, 2021, disponibile su https://www.whitehouse.gov/briefingroom/speeches remarks/2021/07/09/background-press-call-by-senior-administration-officials-on-president-bidens-call--with-president-putin-of-russia

[398] SCHMITT M., Top Expert Backgrounder: Russia's Solar Winds Operation and International Law, in Just Security, 2021, https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

[399] OSBORNE C., colonial pipeline ransomware attack: everything you need to know, in zdnet.com, 2021, disponibile su https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

[400] BROWNING K., Hundreds of companies, from Sweden to the United States, affected by cyberattacks, in The New York Times, 2021, disponibile su https://www.nytimes.com/2021/07/02/technology/cyberattack–businesses–ransom.html.

[401] WISE A., The Republican National Committee Was Targeted by Hackers, su NPR, 2021, disponibile su https://www.npr.org/2021/07/06/1013545363/russians-tried-to-hack-republican-national-committee.

[402] Digital and Cyberspace Policy staff, Cyber Operations Tracker, Council on Foreign Relations, 2023, disponibile su https://www.cfr.org/cyber-operation.

Ad opinione di esperti come Adam Segal[403], i principali attori dello scacchiere informatico mondiale sembrano concordare sul fatto che il riferimento debba essere sempre il diritto internazionale "tradizionale" differendo però sulla visione di alcuni aspetti relativi in particolar modo all'autodifesa ed all'uso della forza.

A tal proposito gli Stati Uniti ritengono che al cyberspazio vadano pedissequamente applicate le previsioni ONU e che in tema di sovranità cibernetica dei paesi non vadano invece posti divieti assoluti, specialmente in occasione di particolari operazioni difensive. Il discorso sottintende un desiderio tipico dei paesi operativamente più spregiudicati, ovvero quello di conservare un margine di azione, una zona grigia, in quanto il riferimento del discorso, secondo Segal, è a quelle attività di difesa particolarmente attiva che arrivando in territorio straniero rischiano di essere considerate aggressioni internazionali[404].

Resta comunque l'opinione che quelle attività informatiche che possano potenzialmente consentire il diritto naturale di autodifesa anche attiva vadano valutate nelle sedi competenti caso per caso conservando saldo in ogni caso il tradizionale principio della proporzionalità all'offesa ricevuta.

Va sottolineato che il tema della sovranità, principio che come visto è stato più volte chiamato in discussione relativamente alla possibile sussistenza in un contesto volatile come lo spazio cibernetico, rimane materia viva al punto che gli Stati Uniti stessi non hanno mai espresso una posizione definitiva circa la necessità

[403] SEGAL A., Hearing on China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States, U.S. China Economic Security Review Commission, 2022, video della testimonianza disponibile su https://www.uscc.gov/hearings/chinas-cyber-capabilities-warfare-espionage-and-implications-united-statesAdam Segal Testimony.
[404] *Ibidem*

di norme che impongano il rispetto della sovranità cyberspaziale altrui e presumibilmente per le motivazioni già espresse.

In conclusione una visione, quella americana, nella quale la legittima difesa può essere attivata per gli attacchi cibernetici come per i cinetici ed anche in maniera particolarmente attiva, conservando comunque il principio di proporzionalità.

La Cina, in contrapposizione, non concorda sull'applicabilità della legittima difesa in caso di attività cibernetiche malevoli poiché' il consentirlo a suo avviso "militarizzerebbe" il cyberspazio dando eccessiva libertà di azione agli Stati più capaci informaticamente e consentendo agli stessi di interpretare a proprio favore il diritto internazionale[405].

In sostanza la Cina invita al rispetto delle previsioni di cui all'art. 2 della Carta ONU in particolar modo riguardo al principio di uguaglianza sovrana[406] ed invita ad evitare operazioni cyber di stampo militaresco.

Il blocco russo-cinese ha inoltre evidenziato, come detto in apertura, la necessità di un trattato internazionale specifico per lo spazio cibernetico e nel 2011, con l'appoggio di Tagikistan e Uzbekistan, ha presentato all'Assemblea generale ONU una proposta di codificazione internazionale, intitolata "International Code of Conduct for Information Security", orientata alla sicurezza delle informazioni e tendente al non utilizzo delle tecnologie ICT per attività ostili, atti di aggressione, minacce alla pace o alla sicurezza internazionale nonché contro la proliferazione di

[405] BOZHKOV N., China's Cyber Diplomacy: A Primer, in EU Cyber Direct, 2020, pp. 36-37, disponibile su https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/-GXl50Cl/bozhkov-digital-dialogue-final.pdf.
[406] ONU, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, 1945, Chapter I:" Purposes and Principles", disponibile su https://www.un.org/en/about-us/un-charter/chapter-1.

armamenti di tipo informatico[407], codice riproposto[408] in sede ONU dalla Shanghai Cooperation Organization (SCO) nel 2015.

Nel complesso sembra, quello cinese, un approccio più conservativo che, a parere di molti analisti, sembra riflettere le preoccupazioni circa l'efficacia delle proprie capacità informatiche ed il timore che venga lasciata "carta bianca" in particolar modo a Stati Uniti e NATO. Il proporre un proprio modello normativo di riferimento mira in ogni caso all'indebolimento del sistema di governance americano.

E' interessante inoltre riportare che nel 2004 la Cina prese parte ai lavori del Gruppo di esperti governativi ONU (GGE) circa lo sviluppo di norme di "comportamento statale responsabile nel cyberspazio" sposando la linea americana, in particolar modo nel 2013 e 2015[409] con due rapporti di consenso in cui 15 paesi, tra cui Stati Uniti, Cina e Russia, convennero che il diritto internazionale, ed in particolare la Carta delle Nazioni Unite, si potessero applicare al cyberspazio. Nel 2017, nonostante la sottoscrizione da parte cinese e russa di alcune proposte americane, gli stessi, con Pakistan, Malesia e Bielorussia, si opposero al far riferimento all'art. 51 della carta ONU circa l'autorizzazione all'uso della forza per autodifesa contro attacco armato.

---

[407] Ministero degli Esteri della Repubblica Popolare di Cina, International Code of Conduct for Information Security, 2011, disponibile su https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201109/t20110913_679318.html

[408] U.N. General Assembly, "Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General", U.N. Doc. A/69/273 (2015), https://digitallibrary.un.org/record/786846.

[409] UN Group of Governmental Experts, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/174, 2015, disponibile su https://digitallibrary.un.org/record/799853.

Successivamente Cina e Russia proposero una risoluzione finalizzata alla creazione di un gruppo di lavoro parallelo al GGE, l' Open-Ended Working Group (OEWG), di sviluppo di norme informatiche che, nel 2021, ha prodotto rapporti fondamentalmente simili al GGE seppur con qualche aspetto lasciato non trattato in materia di diritto internazionale umanitario sempre, a detta dei partecipanti, per evitare una militarizzazione del cyberspazio[410].

Nel complesso il blocco russo-cinese, come tra l'altro ribadito nell'incontro bilaterale del febbraio 2022, ritiene ad oggi che seppur vadano rispettati i principi generali della carta ONU in tema di non uso della forza, di sovranità nazionale, di non ingerenza negli affari interni degli altri stati, non vada tanto aggiornato o adattato al cyberspazio il corpus normativo vigente quanto piuttosto vada creato un nuovo trattato multilaterale vincolante specifico sulle norme di comportamento informatiche[411].

Al contrario, come già visto, il blocco occidentale si è espresso positivamente all'applicazione del diritto internazionale al cyberspazio in particolar modo avendo a riferimento Unione Europea[412], Nato[413] e, a livello dottrinale, i manuali di Tallin[414].

---

[410] United Nations Open-Ended Working Group, Chair's Summary, 2021, disponibile su https://www.un.org/disarmament/open-ended-working-group/

[411] Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development, 2022, disponibile su http://en.kremlin.ru/supplement/5770?s=08.

[412] Council of the European Union, "Council conclusions on the development of the European Union's cyber posture", 2022, https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.

[413] NATO Standardization office, "Allied Joint Doctrine for Cyberspace Operations", Allied Joint Publication -3.20, NATO, Gennaio 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

A conferma di quanto già riportato nel concetto strategico del 2022[415], la NATO, durante il recente summit di Vilnius dell'11 e 12 luglio 2023[416], ha prodotto una dichiarazione finale (o Communiqué[417]), ai cui punti 66 e 67 sono stati trattati i due domini che forse attualmente rappresentano fonte di crescente preoccupazione da parte dei paesi parte dell'Alleanza: lo spazio extra atmosferico e cibernetico.

Nello specifico, al punto 67, il cyberspazio viene definito "teatro di contesa costante" necessitante di contrasto alle minacce anche ibride.

Il comunicato in merito alla legittima difesa, precisa che "a *single or cumulative set of malicious cyber activities could reach the level of armed attack and could lead the North Atlantic Council to invoke Article 5 of the Washington Treaty*"[418], confermando, in una valutazione caso per caso, l'equiparabilità delle attività cibernetiche all'attacco armato, attività dunque in grado di attivare il Consiglio del Nord Atlantico nella decisione sull'invocazione dell'Art. 5 e la mutua difesa collettiva, in nome dei task principali storici dell'Alleanza quali deterrenza e difesa, prevenzione e gestione delle crisi, sicurezza cooperativa.

9. Aspetti ancora non definiti

Nonostante si siano svolti molti incontri di livello internazionale tra USA e Cina ed al di là delle visioni divergenti in tema di applicabilità del diritto esistente allo spazio cibernetico, rimangono aperti, volutamente o meno, due punti fondamentali

---

[414] SCHMITT M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, febbraio 2017.
[415] https://www.nato.int/strategic-concept/
[416] https://www.nato.int/cps/en/natohq/216570.htm
[417] https://www.nato.int/cps/en/natohq/official_texts_217320.htm
[418] *Ibidem*, punto 66.

che rilevano nella definizione del tema del presente lavoro. Su tali punti sembra, per vari motivi, permanere l'incertezza normativa, cosa che, se risolta, consentirebbe una risposta legittimata agli attacchi ostili[419]:

1) la sovranità come principio applicabile anche allo spazio cibernetico;
2) la necessità di una trasparente attività di Due diligence da porre in essere verso gli attacchi informatici scagliati dal proprio territorio.

9.1 Il principio di sovranità nel cyberspazio

L'applicabilità del principio della sovranità nel cyberspazio è oggetto di discussione in particolar modo per le mancate prese di posizione da parte di paesi protagonisti nello scacchiere mondiale.

Ritengo sia importante considerare uno dei concetti che da sempre ha caratterizzato il rapporto tra Stati in relazione ad un concetto "fluido" come quello dello spazio cibernetico. Si intende cioè valutare se sia opportuno parlare di sovranità in un contesto caratterizzato, almeno in apparenza, dall'assenza di confini spazio-temporali.

È inevitabile richiamare il modello Westfphaliano del 1600 basato fortemente sulla delimitazione territoriale, sulla non ingerenza negli affari interni altrui nonché sull'eguaglianza sovrana tra Stati, principi tra l'altro fondanti della Carta ONU[420] e rinvenibili proprio nell'articolo 2 della stessa.

---

[419] SCHMITT M. N., Three International Law Rules for Responding Effectively to Hostile Cyber Operations, in Just Security, 2021, disponibile su https://www.justsecurity.org/77402/three-international-law-rules-for-respondng-effectively-to-hostile-cyber-operations/.

[420] ONU, Charter of the United Nations and Statute of the International Court of Justice, San Francisco, 1945, articolo 2 paragrafo 1 disponibile su https://unric.org/it/lo-statuto-delle-nazioni-unite/.

Partendo dalla pace di Westphalia del 1648, il principio di sovranità si è visto mettere in discussione nell'inedito confronto con lo spazio cibernetico e le pertinenti strutture fisiche afferenti ai singoli Stati, al punto da dover comprendere se fosse estensibile il concetto di esclusività territoriale a questo contesto ed in quale misura.

Gli Stati, in considerazione dell'ubiquità ottenibile grazie alle operazioni informatiche[421], hanno sentito la necessità di porre sotto la propria giurisdizione o meglio ancora sotto la propria sovranità esclusiva, le infrastrutture telematiche.

Si parla non a caso di sovranità "cyberwesphaliana"[422] ovvero della tendenza, a partire da Cina e Stati Uniti, a porre confini virtuali, coesistenti a quelli fisici, in nome della sicurezza nazionale.

L'esistenza di tali perimetri consentirebbe un maggiore controllo di quanto avviene sul proprio territorio attraverso un filtro sulle attività da e verso i paesi stessi. La Cina, infatti, ha spinto verso la creazione di una rete interna che consentisse il tracciamento delle informazioni dal mittente al destinatario, in una visione Nordcoreana o sul modello internet islamista iraniano[423]. È il cosiddetto "great firewall"[424].

Quanto sopra esposto evidenzia una tendenza all'autodifesa soggettiva in contrapposizione al concetto cooperativo internazionale. Un tale processo di regionalizzazione delle reti

---

[421] MILANOVIC M., Human Rights and Foreign Surveillance: Privacy in the Digital Age, in Harvard International Law Journal, 2015, p. 81 e ss.
[422] DEMACHAK C.C. – DOMBROWSKI P., Rise of a Cybered Westphalian Age, in Strategic Studies Quarterly, 2011, p. 45, disponibile su https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf.
[423] YANNAKOGEORGOS P.A., LOWTHER A.B., Conflict and Cooperation in Cyberspace: The Challenge to National Security, Boca Raton, FL, 2013, p. 277.
[424] SHACKERLFORD S.J., Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace, Cambridge, 2014, p. 71.

inevitabilmente si scontra con la natura globale e senza confini tipica del cyberspazio e che ha consentito nel tempo lo scambio delle informazioni in tempo reale e lo sviluppo sociale ed economico mondiale. Risulta difficile pensare che uno Stato riesca veramente ad esercitare un possesso esclusivo di una porzione di spazio cibernetico se mai identificabile.

Va inoltre considerato che il mantenere aperte le linee di comunicazione globale è interesse strategico degli Stati, in bilanciamento costante con le esigenze di sicurezza interna. Una delimitazione dello spazio cibernetico a similitudine dei confini statali risulterebbe realisticamente irrealizzabile in primis per le difficoltà tecniche ma anche per l'interesse dei paesi stessi a che i vicini rimangano osservabili.

Come già asserito, molte problematiche di inquadramento del problema nascono da posizioni ondivaghe o comunque non definite degli attori principali. Il Regno unito, ad esempio, ha criticato le operazioni cibernetiche da parte russa verso l'Ucraina sulla base di un mancato rispetto della sovranità[425] nonostante nel 2018, e nel 2021, abbia affermato che nel contesto informatico non possa esistere la regola della sovranità[426]. Di opinione differente risultano invece gli altri paesi interpellati in merito, tra cui l'Italia[427], che hanno interpretato la sovranità come principio di diritto internazionale applicabile al di là del contesto e sulla stessa

[425] UK Foreign, Commonwealth and Development Office e National Cyber Security Center, UK assesses Russian involvement in cyber attacks on Ukraine, GOV.UK, 2022, disponibile su https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine.
[426] Attorney General Jeremy Wright QC MP, "Cyber and International Law in the 21st Century", UK, 2018, disponibile su https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.
[427] Ministero degli Affari Esteri, Presidenza del Consiglio dei Ministri e Ministero della Difesa, Italian position paper on international law and cyberspace'", disponibile su https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.

linea risulta essere, in generale, la recente dottrina NATO seppur con riserva non sciolta del Regno Unito[428].

Gli Stati Uniti, dal canto loro, pur non esprimendosi esplicitamente, ritengono che la sovranità sia un principio derivante e strettamente collegato ad altri più generali come il divieto dell'uso della forza o il principio di non intervento[429] considerandolo dunque elemento autonomo ma discendente da altre prescrizioni già definite di diritto internazionale.

È certamente una posizione questa colpevole di generare non poche interpretazioni e che sicuramente non fornisce elementi utili per l'eventuale definizione di una responsabilità in caso di attacco e, di conseguenza, per la legittimazione della legittima difesa.

In generale, come affermato dal gruppo di esperti governativi nei già citati rapporti del 2013 e 2015, non esistono motivi per cui il cyberspazio debba essere escluso dall'applicazione delle norme in uso, pattizie o consuetudinarie, nel momento in cui uno Stato irrompa nelle aree di interesse altrui o alternativamente non faccia nulla per impedire un'attività offensiva generata sul proprio territorio, come meglio si vedrà circa la responsabilità oggettiva e la Due diligence.

La sovranità applicabile al cyberspazio comporterebbe la possibilità di lamentare un illecito internazionale per operazioni informatiche sia direttamente operate da organi di uno Stato, sia

---

[428] v. NATO, "Allied Joint Doctrine for Cyberspace Operations, NATO Standardization Office, 2020, disponibile su https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

[429] NEY Jr Hon. P.C., DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, Dipartimento della Difesa degli Stati Uniti, 2020, disponibile su https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

eseguite da terzi sotto istruzione o controllo effettivo dello stesso[430].

A livello dottrinale, in ogni caso, questo viene confermato con i manuali di Tallin ed in particolare alla regola 4 del Manuale di Tallin 2.0 si afferma che, indipendentemente che la struttura colpita sia governativa, "*l'attività informatica che provoca effetti sul territorio di un altro Stato può violare la sovranità*"[431] e che tale sovranità può risultare violata anche quando l'attività posta in essere interferisca con le funzioni intrinsecamente governative di un altro Stato.

In conclusione si ritiene che riconoscere la regola della sovranità nel contesto cyberspaziale comporti un passo fondamentale nella facilitazione più che del processo di identificazione, di quello di attribuzione al fine di legittimare una dichiarazione di intervento per legittima difesa. Non avere questo riconoscimento, o non dichiararlo apertamente come nel caso americano o ancora australiano, priva il processo di un tassello fondamentale in un contesto già eccessivamente vago e soggetto a discrezionalità.

9.2 Responsabilità oggettiva e due diligence

Preso atto della possibilità di risposta in legittima difesa a fronte di un evento qualificato come uso della forza, un problema fortemente discusso in dottrina è stato quello di come rispondere in caso di attacco che non raggiunga la soglia dell'uso della forza

[430] International Law Commission, "Draw articles on Responsibility of States for Internationally Wrongful Acts, with commentaries 2001", Yearbook of the International Law Commission, 2001, vol. II, Part Two, 2001, disponibile su htt ps://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.
[431] SCHMITT M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017

tradizionalmente intesa, come nel caso di attacchi perpetrati da soggetti privati o autonomi.

Uno dei problemi principali risiede negli alti criteri richiesti dal diritto internazionale al fine di attribuire con certezza l'atto ad un determinato Stato. Specificatamente nell'ambito cyberspaziale ed in particolar modo in relazione agli attacchi posti in essere da soggetti non statuali, è stata dunque suggerita la possibilità di alleggerire questi criteri per meglio collegare l'autore allo Stato da cui è partito l'attacco[432].

Per favorire questo si è prospettato un sistema di valutazione caso per caso in cui sia possibile rispondere proporzionalmente sulla base dei criteri tradizionalmente previsti in caso di attacco armato come anche attraverso misure alternative quali strumenti diplomatici o economici se tale soglia non venga raggiunta. Si è inoltre valutata la possibilità di introdurre il concetto di responsabilità' oggettiva, con attribuzione allo Stato controllante il territorio da cui è partito l'attacco stesso[433].

Per quanto questo approccio sembri dare un'ulteriore possibilità di risposta allo Stato vittima, a parere dello scrivente si ritiene che non sia un processo fortemente efficace in quanto necessitante di valutazioni principalmente ex post su natura ed effetti dell'attacco subìto andando dunque a perdere la possibilità di evitare o limitare il danno di un attacco appena scagliato.

Ad ogni modo parlare di responsabilità oggettiva impone l'introduzione di un altro dei grandi temi di discussione rimasti irrisolti ovvero la necessità di una *Due diligence*, concetto

[432] FINLAY L, PAYNE C., The Attribution Problem and Cyber Armed Attack, in Cambridge university press, 2019, p. 205, disponibile su https://doi.org/10.1017/aju.2019.35
[433] *Ibidem*, p. 206

fortemente collegato al principio di sovranità e non ancora universalmente riconosciuto nell'ambito di interesse.

La Due diligence o "dovuta diligenza", in diritto internazionale è stato un concetto, o meglio un obbligo, ribadito più volte in giurisprudenza. Si riporta a tal proposito il caso United States c. Netherlands del 1929, "Island of Palmas"[434], in cui la Corte permanente di arbitrato, nella persona del giudice Huber, affermò che la sovranità territoriale comporta l'obbligo a corollario di proteggere all'interno del territorio stesso i diritti degli altri stati in pace e guerra.

Anche la Corte Internazionale di Giustizia, nel caso riguardante il canale di Corfù[435], ha affermato l'obbligo di non permettere consapevolmente l'utilizzo del proprio territorio per atti ostili verso altri Stati. Quest'ultimo caso oltretutto rimase pietra miliare nella giurisprudenza internazionale in quanto definì con chiarezza, creando infatti un principio generalmente riconosciuto, che la responsabilità non risiedeva unicamente in forma soggettiva ma anche in forma oggettiva quando in presenza di attività poste in essere sotto la giurisdizione o comunque il controllo effettivo di uno Stato. Stesso dicasi per il caso Argentina c. Uruguay del 2010[436], in un contenzioso relativo ad uno stabilimento di polpa di cellulosa operativo dal 2007 e costruito su

[434] Corte Permanente di arbitrato, Island of Palmas Case (or Miangas), United States v Netherlands, Award, 1928 II RIAA 829, ICGJ 392 (PCA 1928): "territorial sovereignty (…) involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the territory the rights of other States, in particular their right to integrity and inviolability in peace and in war" disponibile su https://legal.un.org/riaa/cases/vol_II/829-871.pdf.

[435] Corte internazionale di giustizia, The Corfù channel case, sentenza del 9 aprile 1949, I.C.J. Reports, p. 22.

[436] Corte internazionale di giustizia, Pulp mills on the river Uruguay (Argentina v. Uruguay), sentenza del 20 aprile 2010, I.C.J. Reports 2010, p. 22, disponibile su consultabile a https://www.icj-cij.org/public/files/case-related/135/135-20100420-JUD-01-00-EN.pdf

territorio Uruguaiano al confine con l'Argentina in occasione del quale la Corte ha ribadito l'obbligo di agire con dovuta diligenza nel rispetto delle parti interessate.

Gli obblighi comporterebbero l'aver messo in opera tutte le misure necessarie al fine di evitare che avvenga un evento dannoso. Una responsabilità dunque legata alla condotta più che al risultato.

A tal proposito va infatti evidenziato che in caso di incidente, il danno intercorso non è sufficiente a poter valutare l'imputazione per responsabilità oggettiva rappresentando appunto una obbligazione di condotta e non di risultato come oltretutto affermato dalla Commissione di Diritto internazionale nel "*Draft Articles on the Law of the Non-Navigational Uses of International Watercourse sand Commentaries thereto and Resolution on Transboundary Confined Groundwater" del 1994*, dove al commentario dell'art. 7 viene riportato che "*the obligation of due diligence contained in article 7 sets the threshold for lawful State activity. It is not intended to guarantee that in utilizing an international watercourse significant harm would not occur. It is an obligation of conduct, not an obligation of result*" [437].

Preso atto a questo punto che nelle previsioni, seppur dottrinali, sia stata prevista una due diligence in ambito cyber[438] e considerato che d'altro canto, come ribadito in giurisprudenza nel già citato caso del Canale di Corfù[439], non si possa presumere che

---

[437] Come affermato dalla Commissione del diritto internazionale nel commentario all'art. 7 del Draft, disponibile su https://legal.un.org/ilc/texts/instruments/english/commentaries/8_3_1994.pdf.

[438] SCHMITT M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, art. 7: «the principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States».

Corte internazionale di giustizia, The Corfù channel case, sentenza del 9 aprile 1949, I.C.J. Reports, p. 18.

lo Stato sia a conoscenza di tutte le attività svolte sul proprio territorio, ci si deve allora chiedere se invece, nell'ambito del cyberspazio, lo Stato possa riuscire ad essere a conoscenza di tutta l'attività informatica in partenza dai propri confini o si possa al contrario interpretare estensivamente la sentenza citata.

Il voler rimanere ancorati alla giurisprudenza tradizionale comporterebbe, ai sensi di quanto inoltre espresso dalla CIG nel contenzioso Uruguay-Argentina[440], una attività di due diligence sotto forma di controllo amministrativo da applicare ad operatori pubblici e privati, dunque un massivo controllo sulle attività informatiche di tutti i propri sudditi nonché sui server posti sul proprio territorio. Una visione che, oltre ad essere tecnicamente dispendiosa in termini di uomini e mezzi da utilizzare, riporta alla memoria attività statuali anacronistiche universamente condannate in primis in nome della inviolabilità costituzionale della libertà e della segretezza della corrispondenza e che difficilmente potrebbero essere oggi conciliate in una sorta di riedizione moderna della Stasi.

In conclusione ad oggi non esiste regola pattuita né tantomeno consuetudine circa la due diligence anche se il suo utilizzo sembra godere dell'appoggio della comunità internazionale nonché' della dottrina come nel caso degli esperti del Manuale di Tallin 2.0.

Come espresso dal gruppo di esperti governativi ONU in più rapporti, tra cui quello del 2021[441], la dovuta diligenza rimane

---

[440] Pulp Mills on the River Uruguay (Argentina v. Uruguay), 2010, § 187: "«the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party"

[441] Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" (GGE), "Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security", General Assembly of the

attività non vincolante ma auspicabile quando siano in pericolo principi fondamentali quali ad esempio la sovranità altrui[442].

9.3 I cyber attacchi e lo Statuto di Roma

Un ultimo aspetto non ancora definito ma che ultimamente sembrerebbe aver guadagnato attenzione è quello del riconoscimento di talune attività informatiche come crimini di guerra dunque perseguibili dalla Corte penale internazionale ai sensi dello Statuto di Roma[443]. Il Procuratore capo della Corte penale internazionale, Karim A.A. Khan, ha infatti recentemente affermato che lo Statuto, pur chiaramente non essendosi mai occupato direttamente di cyber warfare, potrebbe essere abbastanza flessibile da consentire un'interpretazione estensiva tale da poter comprendere le attività informatiche senza necessità di andare a creare regole nuove o modificare di quelle esistenti.

Il Procuratore ha dunque preso atto delle preoccupazioni degli esperti di sicurezza in relazione al peso che le operazioni informatiche hanno avuto ultimamente nel determinare l'esito dei conflitti armati e per le quali veniva chiesta la produzione di una convenzione, a similitudine di quelle di Ginevra, specifica per il crimine cibernetico insistendo sull'errore di pensare il cyber spazio come un dominio libero da qualsiasi regolamentazione come anche della tradizionale funzione ordinatoria propria del diritto internazionale.

United Nations, 2021, disponibile su https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

[442] SCHMITT M. N., In Defense of Due Diligence in Cyberspace, in The Yale Law Journal Forum, 2015, disponibile su https://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

[443] Statuto di Roma della Corte penale internazionale, entrato in vigore il 1° luglio 2002, ratificato in Italia con l. 12 luglio 1999 n. 167, in Gazzetta ufficiale n. 167 del 19 luglio 1999, supplemento ordinario. Disponibile su https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/cc/2002/586/20151029/it/pdf-a/fedlex-data-admin-ch-eli-cc-2002-586-20151029-it-pdf-a.pdf

Il Procuratore Khan, in considerazione del numero sempre maggiore di incidenti informatici attuati in parallelo o a supporto di azioni cinetiche ed in considerazione del fatto che tali attività hanno sempre più spesso avuto ripercussioni su oggetti fisici o comunque sulla vita di persone civili, ritiene che sia arrivato il momento di equiparare, in talune circostanze, le azioni perpetrate nel cyberspazio ai crimini di guerra, ai crimini contro l'umanità ed a tutte le fattispecie di competenza della Corte. La possibilità di far rientrare il dominio cibernetico tra quelli contemplati dallo Statuto di Roma consentirebbe di poter perseguire tali condotte.

Questo cambio di visione, come dichiarato dall'Ufficio del Procuratore stesso[444], rappresenta a tutti gli effetti la posizione ufficiale della Corte nei tempi a venire mostrando dunque l'intenzione di occuparsi di tutte quelle casistiche considerate sufficientemente gravi sulla base di una valutazione caso per caso.

Nonostante non se ne faccia menzione direttamente, il conflitto russo-ucraino è sicuramente uno dei principali eventi ispiratori di queste dichiarazioni essendo non a caso considerato il primo conflitto comportante operazioni informatiche su larga scala[445]. Va oltretutto detto che negli ultimi tempi esponenti di vari governi nonché comunità di studenti di diritto hanno spinto affinché la Corte attuasse un'evoluzione interpretativa al fine di occuparsi degli innumerevoli attacchi informatici russi.

Tra questi un gruppo di avvocati specializzati nella tutela dei diritti umani dello Human Rights Center della UC Berkeley[446] che, ai sensi dell'articolo 15 dello Statuto di Roma, che consente a

---

[444] GREENBERG A., The International Criminal Court Will Now Prosecute Cyberwar Crimes, su wired.com, 2023, disponibile su https://www.wired.com/story/icc-cyberwar-crimes/?

[445] LEWIS J.A., Cyber War and Ukraine, in Center for strategic & international studies (CSIS), Washington, DC, 2022, disponibile su https://www.csis.org/analysis/cyber-war-and-ukraine

[446] https://humanrights.berkeley.edu/

qualsiasi individuo, gruppo o organizzazione di inviare informazioni su presunti crimini all'Ufficio del Procuratore della Corte penale internazionale[447], ha inviato due richieste formali in correlazione ai cyber attacchi perpetrati dal gruppo hacker "sandworm", facente parte dell'organico della componente intelligence militare russa nota come Glavnoe Razvedyvatel'noe Upravlenie (GRU)[448], che sin dal 2014 ha colpito ripetutamente infrastrutture critiche in Ucraina con ripercussioni in particolar modo sulla rete elettrica e sulle comunicazioni a danno di decine di migliaia di civili.

Va ben compreso che le operazioni cibernetiche non vengono effettuate unicamente in concomitanza dell'evento cinetico ma anche antecedentemente per preparare il campo.

Nonostante l'attuale scontro russo-ucraino abbia guadagnato gli onori della cronaca con l'invasione del mese di febbraio 2022, la Russia ha attuato nell'area, sin dagli eventi di Maidan del biennio 2013-2014[449], attacchi cibernetici e costanti campagne comunicative propagandistiche, soprattutto a mezzo social network, finalizzate da una parte a screditare il governo ucraino e dall'altra nell'infondere idee separatiste nella popolazione locale.

Al fine di meglio comprendere quanto un attacco cibernetico sferrato in un contesto bellico possa esondare dal campo di battaglia andando potenzialmente ad impattare sulle esigenze quotidiane delle popolazione civile e dunque a conforto dell'interpretazione estensiva dello Statuto di Roma in questo senso, va ricordato che nel febbraio 2022, appena un'ora prima dell'invasione dell'Ucraina, la Russia lanciò il malware "AcidRain" nei sistemi satellitari ucraini ottenendo il blocco delle

[447] https://www.coalitionfortheicc.org/how-file-communication-icc-prosecutor
[448] Direzione generale per le informazioni militari
[449] https://www.treccani.it/enciclopedia/euromaidan/

comunicazioni militari con ripercussioni a cascata. La Enercon, compagnia produttrice di energia tedesca, dichiarò in quella occasione di aver perso il controllo remoto di 5.800 pale eoliche dispiegate in Europa centrale.

Si stima inoltre che circa 27.000 utenti abbiano avuto problemi di connessione internet in vari paesi tra cui Repubblica Ceca, Francia, Germania, Polonia, Regno Unito e Marocco nonché decine di migliaia di cittadini ucraini, per più di due settimane, non hanno avuto accesso ad informazioni aggiornate sulla crisi in corso[450]. Lo stesso gruppo Sandworm ha causato un imponente blackout energetico nel 2016 attraverso un malware inoculato nei sistemi di controllo industriale delle reti elettriche ucraine, tentando una riedizione nel 2022 con il malware Industroyer2, questa volta senza esito ma con una ricaduta potenziale su milioni di utenze civili[451].

Si comprende quanto un attacco distribuito possa andare dunque ad impattare, in maniera istantanea ed indiscriminata, sulla vita di migliaia di persone ed è da questo presupposto, nonché sul timore di ulteriori escalation, che è stata richiesto a gran voce l'inclusione del contesto cibernetico nelle competenze della Corte penale internazionale.

Se da un lato appare definita la volontà di perseguire quegli attacchi comportanti danni fisici diretti ad oggetti o alla salute fisica di persone ritenuti violenti, come previsto dal primo comma dall'art. 49 del primo protocollo aggiuntivo alle Convenzioni di

[450] https://digitalfrontlines.io/2023/05/25/the-evolution-of-cyber-operations-in-armed-conflict/#attribution-challenges

[451] a conferma della tesi secondo la quale in ambito cyber tutto ciò che viene ripetuto perde inevitabilmente efficacia. Nel caso di specie i dispositivi difensivi ucraini hanno acquisito esperienza anche grazie al supporto degli Stati Uniti e al contributo di Microsoft.

Ginevra del 1977[452], le operazioni militari comportanti conseguenze non prettamente violente sembrerebbero a questo punto non rientrare nell'ambito di applicazione del Diritto internazionale umanitario. Anche i manuali di Tallin ritengono che un attacco informatico realmente dannoso presupponga una ragionevole aspettativa di lesioni, morte o di distruzione.

Un requisito come quello del danno effettivamente apportato potrebbe comportare l'esclusione di determinate operazioni informatiche meno eclatanti dall'applicazione delle Convenzioni di Ginevra come anche il disinteresse della Corte penale internazionale.

Il Procuratore, nelle dichiarazioni circa la nuova tendenza interpretativa, fa riferimento però al rapporto finale del Consiglio dei Consulenti sull'applicazione dello Statuto di Roma alla guerra informatica[453]. Tale rapporto suggerisce, ai sensi dell'art. 52, § 2 del già citato primo protocollo aggiuntivo, che un attacco possa essere considerato come avvenuto anche quando l'obiettivo risulti neutralizzato e non solo completamente distrutto. L'interruzione delle funzioni critiche di uno stato, come delle capacità militari dello stesso, può essere dunque qualificata come attacco ai sensi del Diritto umanitario.

Allo stesso modo nel rapporto si evidenzia che andare a colpire dati civili equivale al compiere un attacco facendo

---

[452] Art. 49, co. 1 del protocollo aggiuntivo alle convenzioni di Ginevra del 12 agosto 1949 relativo alla protezione delle vittime dei conflitti armati internazionali, adottato l'8 giugno 1977, in Suppl. ordinario alla Gazzetta Ufficiale n. 303 del 27 dicembre 1985 (a seguito di ratifica italiana con l. 11 dicembre 1985, n. 762): "Con l'espressione «attacchi» si intendono gli atti di violenza contro l'avversario, siano tali atti compiuti a scopo di offesa o di difesa."

[453] Permanent Mission of Liechtenstein to the United Nations, The council of advisers' Report on the application of the Rome statute of the International criminal court to cyberwarfare, 2021, disponibile su https://www.regierung.li/files/medienarchiv/The-Council-of-Advisers-Report-on-the-Application-of-the-Rome-Statute-of-the-International-Criminal-Court-to-Cyberwarfare.pdf

l’esempio dei dati sanitari dei pazienti conservati in ospedale, la cui cancellazione comporterebbe difficoltà di assistenza agli stessi.

In conclusione, a fronte di quanto esposto, sembrerebbe percepirsi la volontà di dotare la Comunità internazionale di mezzi giuridici tali da assicurare la persecuzione del crimine informatico.

Le parole del Procuratore capo della Corte penale internazionale andranno in ogni caso supportate dallo sviluppo di politiche e linee guida condivise su attribuzione, risposta, deterrenza e responsabilità internazionale al fine di far fronte alle future guerre ibride se non anche puramente cibernetiche.

Conclusioni

Con il presente lavoro ci si è posti in generale l'intento di analizzare la possibilità di convivenza tra il diritto internazionale tradizionalmente inteso e lo spazio cibernetico e nel particolare l'istituto della legittima difesa nella cyber warfare.

Per fare ciò si è proceduto per prima cosa a tratteggiare concetti cardine nei rapporti tra Stati, tra cui, su tutti, il divieto di uso della forza introducendo successivamente il concetto di cyberspazio, attraverso la definizione delle principali attività malevoli, le strategie di sicurezza nazionale in Italia e nel mondo, la descrizione delle attività delle principali organizzazioni internazionali coinvolte nella materia e l'analisi di alcuni casi studio ritenuti esemplificativi circa le difficoltà di applicazione delle previsioni giuridiche preesistenti.

Ci si è concentrati infine sul tema principale ovvero trovare risposta ad alcune problematiche legate all'esercizio della legittima difesa tradizionalmente intesa nel contesto cibernetico quali l'individuazione di un possibile punto di equiparazione delle operazioni informatiche all'uso della forza, la responsabilità internazionale, la legittima difesa collettiva ed ulteriori aspetti che ancora non risultano definitivamente condivisi come il riconoscimento del principio di sovranità nel cyberspazio e la responsabilità oggettiva degli Stati.

Da quanto analizzato è emersa una complessiva mancanza di normazione internazionalistica specifica dovuta soprattutto al mancato consolidamento di una qualsiasi forma di consuetudine o prassi ripetuta nel tempo. Si ritiene in questo senso che la continua evoluzione tecnica delle modalità di attacco non consenta tale processo trattandosi di un contesto, quello cibernetico, in cui

proprio la diuturnitas risulta portatrice di prevedibilità e dunque inefficacia. Da questo vuoto normativo discende inevitabilmente il tentativo di adattare quanto già previsto per i tradizionali attacchi di tipo cinetico nell'attesa di trovare punti di condivisione tra gli attori internazionali, cosa sicuramente non semplice.

Se da un lato sembra essere condivisa la qualificazione delle cyber operations come attacco armato nel momento in cui provochino danni materiali o perdite di vite umane, resiste ancora, ad esempio, una diffusa incertezza circa le azioni da intraprendere nel momento in cui queste operazioni non raggiungano tale soglia ma risultino comunque ingerenti negli affari interni.

Nonostante sembri scontato che gli Stati possano giovare di un adattamento del diritto esistente al cyberspazio è risultata invece, nell'osservazione di cui al presente studio, una certa reticenza da parte degli stessi, si ritiene nel timore di essere soggetti irreversibilmente a previsioni bloccanti che possano limitare la libertà di azione. A tal proposito un esempio riportato ha riguardato le posizioni mai completamente definite di paesi quali Inghilterra o Stati Uniti in tema di riconoscimento del principio di sovranità nel cyberspazio, principio che, se riconosciuto, comporterebbe importanti limitazioni in caso di operazioni particolarmente pervasive verso l'esterno.

Come detto l'assenza di una prassi consolidata come anche di giurisprudenza cui far riferimento in tema di attacco e difesa cibernetica, ha comportato nel tempo reazioni differenti da parte dei paesi vittima di attacco, sia nella valutazione della natura dell'attacco sia nel tipo di controffensiva.

La costante che però si evince dai casi studio riportati è stata la mancanza di coinvolgimento della Comunità internazionale a favore di risposte personali ritenute opportune in una valutazione caso per caso, dalla richiesta di sanzioni nel caso Sony, all'azione

penale nel caso estone, ad una cyber rappresaglia nel caso iraniano.

Nel complesso dunque una apparente sconfitta del diritto internazionale pur considerando, va detto, che i casi studio analizzati fossero situazioni al tempo realmente inedite.

Inevitabilmente va presa coscienza che ci troviamo, in una prospettiva temporale a lungo termine, agli albori della cyberwarfare, un contesto bellico in cui già un quinquennio viene considerato storia per libri. La visione attuale del dominio cyber è ancora quella dell'atto prodromico all'attacco cinetico o comunque inserito a supporto di operazioni tradizionali ma è plausibile pensare che nell'arco di pochi anni si parlerà di conflitti puramente cibernetici.

Questo momento di osservazione ed apprendimento comporta, come detto, l'assenza di un riferimento storico, facendoci trovare anzi in una fase in cui lo strumento di deterrenza principale non sono le norme che si potrebbero violare bensì il non sapere con certezza effetti e potenzialità delle nuove tecnologie. I vincoli sembrerebbero dunque risiedere non nell'aspetto giuridico ma in quello tecnico dei mezzi in gioco o strategico dei decisori. È quindi una situazione che richiede con urgenza che il Diritto internazionale prenda la posizione che gli compete, quella di grande ordinatore del sistema.

Una regolamentazione che, come visto, potrebbe avvenire o attraverso l'adattamento del diritto internazionale esistente o con un nuovo trattato vincolante. Per quanto visto dai rapporti prodotti dei gruppi di lavoro GGE e OEWG sembrerebbe essere auspicata la via del trattato anche se lo stato dei fatti attuale vede ancora visioni diverse e valutazioni discrezionali caso per caso, con contromisure autonome o in forma cooperativa in caso di scarsa capacità informatica delle vittime.

A detta degli studiosi[454] un processo di definizione comune a livello normativo necessita di una riduzione delle zone di ambiguità attraverso la formulazione di norme per quanto più possibile chiare ed articolate, trovando condivisioni in merito alle definizioni cardine quali quelle di attacco armato, di uso della forza o più in generale di responsabilità internazionale, con particolare riguardo a quella oggettiva, al fine di limitare la discrezionalità dei singoli Stati nelle risposte agli attacchi cibernetici.

Per assottigliare la differenza con l'ambito cinetico sarà inoltre necessario ridurre la marginalità e le tempistiche delle Nazioni Unite dotandole di strumenti di intervento adeguati alle esigenze del momento. In considerazione della continua evoluzione tecnica la proposta normativa non potrà prescindere dal contributo dell'industria e degli esperti di settore anche alla luce del coinvolgimento di attori non statuali nelle crisi internazionali a forte connotazione informatica.

La descrizione delle strutture operative nazionali ed internazionali dedicate al cyberspazio ha evidenziato l'effettivo sforzo globale verso un cambiamento strutturale che indubbiamente comporterà stratificazione burocratica, come già tradizionalmente nelle istituzioni internazionali particolarmente complesse, ma che, una volta trovata la corretta identificazione di figure e compiti, potrà contribuire al lenimento dell'incertezza portando il diritto condiviso in posizione preminente rispetto all'interesse del singolo Stato. È questo dunque un processo di implementazione necessario in particolar modo per supportare i paesi vittima come anche il personale impiegato nelle operazioni.

---

[454] MELE S., MORO F.N., Cyber security: un fronte sempre più caldo, in ISPI Commentary, 25 settembre 2015, disponibile su http://www.ispionline.it/sites/default/files/pubblicazioni/commentarymelemoro.pdf.

In considerazione dell'estrazione militare dello scrivente, risulta interessante riportare infine l'art. 37 del recente d.l. 9 agosto 2022, n. 115 recante "Disposizioni in materia di intelligence in ambito cibernetico"[455] il quale sembrerebbe mostrare una inedita sensibilità verso le esigenze di copertura giuridico-legale del personale militare utilizzato in operazioni che, per quanto difensive potrebbero, in determinate situazioni, risultare particolarmente pervasive verso sistemi altrui.

Si ritiene in tal senso auspicabile, sulla falsariga di quanto avviene per le coperture funzionali del personale impiegato in presso le agenzie facenti parte del nostro Sistema di informazione per la sicurezza della Repubblica[456], una modifica alla Codicistica militare[457] che consideri e renda possibili operazioni di reale difesa attiva andando a scriminare condotte, da autorizzare preventivamente caso per caso, normalmente oggetto di previsioni sanzionatorie, in particolar modo in riferimento all'accesso a sistemi informatici esterni, fattispecie normalmente configurabile come reato penale anche in condizione di crisi.

---

[455] d.l. 9 agosto 2022, n. 115, recante "Misure urgenti in materia di energia, emergenza idrica, politiche sociali e industriali", convertito con modificazioni dalla l. 21 settembre 2022, n. 142, in Gazzetta ufficiale n. 221 del 21 settembre 2022, disponibile su https://www.gazzettaufficiale.it/eli/id/2022/08/09/22G00128/sg

[456] AMATO G., Le garanzie funzionali per gli 'operatori' di Intelligence (1a parte), in Gnosis, Vol. 3, 2011, disponibile su http://gnosis.aisi.gov.it/gnosis/Rivista28.nsf/ServNavig/11

[457] d.l. 15 marzo 2010, n. 66, "Codice dell'ordinamento militare", in Gazzetta ufficiale n. 106 del 8 maggio 2010 e Decreto del Presidente della Repubblica 15 marzo 2010, n. 90, recante il "Testo unico delle disposizioni regolamentari in materia di ordinamento militare, a norma dell'articolo 14 della legge 28 novembre 2005, n. 246, in Gazzetta ufficiale n. 140 del 18 giugno 2010 – Supplemento ordinario n. 131.

Bibliografia

AA.VV., The Law of Cyber Attack, Berkeley university, in Berkeley Law, 2012, disponibile su https://doi.org/10.15779/Z38CR6N

AA.VV., W32. Stuxnet Dossier, versione 1.4, in National security archive, 2011, disponibile su https://nsarchive.gwu.edu/document/21440-document-44

AA.VV., Attribution of cyber attacks on industrial control systems, in EAI endorsed transactions on industrial Networks and Intelligent System, 2016, disponibile su https://publications.eai.eu/index.php/inis/article/view/458/352

AKANDE D. – TZANAKOPOULOS A., Use of Force in Self-Defence to Recover Occupied Territory: When Is It Permissible? in EJIL:Talk!, Blog of the European Journal of International Law, 2020, disponibile su https://www.ejiltalk.org/use-of-force-in-self-defence-torecover-occupied-territory-when-is-it-permissible

ALLEN Nick, Sony hack: Obama considers 'proportional response' against North Korea, su telegraph.co.uk, 2014, disponibile su https://www.telegraph.co.uk/news/worldnews/northamerica/usa/11302590/Sony-hack-Obama-considers-proportional-response-against-North-Korea.html

AMATO G., Le garanzie funzionali per gli 'operatori' di Intelligence (parte uno), in Gnosis, Vol. 3, 2011, disponibile su http://gnosis.aisi.gov.it/gnosis/Rivista28.nsf/ServNavig/11

ANDERSON N., How Georgia doxed a Russian hacker (and why it matters), in Ars Technica, 2012, disponibile su https://arstechnica.com/tech-policy/2012/11/how-georgia-doxed-a-russian-hacker-and-why-it-matters

ARANGIO RUIZ G., Difesa legittima, in Novissimo digesto italiano, Torino, 1960

BERINATO S., Active Defense and "Hacking Back": A Primer, in Harward business review, 2018, disponibile su https://hbr.org/2018/05/active-defense-and-hacking-back-a-primer

BLANK S., Web War I: Is Europe's First Information War a New Kind of War? In Comparative Strategy, Vol. 27, No. 3, 2008, disponibile su https://doi.org/10.1080/01495930802185312

BOBBIO N., Pace, in Enciclopedia del Novecento, Roma, 1989

BOEBERT W.E., A Survey of Challenges in Attribution, in National Research

Council, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, in National academies, Washington, DC, 2010 disponibile su https://doi.org/10.17226/12997

BONFIGLIO S., Il diritto del popolo ucraino alla legittima difesa, in Università Roma Tre, Democrazia e Sicurezza - Democracy and Security Review, Roma, 2022, disponibile su https://romatrepress.uniroma3.it/wp-content/uploads/2022/10/Editoriale-Bonfiglio.pdf

BOZHKOV N., China's Cyber Diplomacy: A Primer, in EU Cyber Direct, 2020, disponibile su https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/-GXl50Cl/bozhkov-digital-dialogue-final.pdf.

BRENNER J, America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare, New York, 2011

BRENNER S. W., At light speed: Attribution and response to cybercrime/terrorism/warfare, in Journal of Criminal Law and Criminology, 2007, disponibile su https://scholarlycommons.law.northwestern.edu/jclc/vol97/iss2/2/

BROWN G., Spying and fighting in cyberspace: what is which?, in Journal of National Security Law & Policy, Vol. 8, 2016, disponibile su https://jnslp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf

BROWNING K., Hundreds of companies, from Sweden to the United States, affected by cyberattacks, in The New York Times, 2021, disponibile su https://www.nytimes.com/2021/07/02/technology/cyberattack–businesses–ransom.html

CARR J, Inside Cyber Warfare: Mapping the Cyber Underworld, USA, 2012

CARTWRIGHT J. E., Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories: Joint Terminology for Cyberspace Operations, Washington (DC), 2010, disponibile su https://info.publicintelligence.net/DoD-JointCyberTerms.pdf

CENCETTI C., Cybersecurity: Unione europea e Italia Prospettive a confronto, Roma, 2014

CIEPLY M., BROOKS B., Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm, su nytimes.com, 2014, disponibile su https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html

CLARKE R., KNAKE R., Cyber War, The Next Threat to National Security and

What to Do About It, New York, 2012

CLAUSEWITZ K. V., Della guerra, Vom Kriege prima ed., 1832

CONFORTI B., FOCARELLI C., Le Nazioni Unite, 12. ed., Milano, 2020

CONFORTI B., IOVANE M., Diritto internazionale, Napoli, 2021

COT J. P., PELLET A., La Charte des Nationes Unites, Parigi-Bruxelles, 1995.

CRISTADORO N., La dottrina Gerasimov e la filosofia della guerra non convenzionale nella strategia russa contemporanea, 2022.

DELLA MORTE G., Big data e protezione internazionale dei diritti umani. Regole e conflitti, Napoli, 2018.

DEMACHAK C.C., DOMBROWSKI P., Rise of a Cybered Westphalian Age, in Strategic Studies Quarterly, 2011, disponibile su https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Demchak-Dombrowski.pdf.

DENNING D.E., STRAWSER B.J., Active Cyber Defense: Applying Air Defense to the Cyber Domain, in Carnegie Endowment for International Peace, 2016, disponibile su https://carnegieendowment.org/2017/10/16/active-cyber-defense-applying-air-defense-to-cyber-domain-pub-73416

DINSTEIN Y., War, Aggression and self defense, Cambridge, 1994.

EVEN S., SIMAN-TOV D., Cyber Warfare: Concepts and Strategic Trends, INSS - Memorandum 117, Tel Aviv, 2012.

FINLAY L, PAYNE C., The Attribution Problem and Cyber Armed Attack, in Ajil unboung, 2019, disponibile su https://doi.org/10.1017/aju.2019.35

GIACOMELLO G., BADIALETTI G, Manuale di Studi Strategici. Da Sun Tzu alle nuove guerre, Milano, 2016.

GILBLOM K., Old BlackBerrys Came to Sony's Rescue After Systems Hacked, su Bloomberg, 2014, disponibile su https://www.bloomberg.com/news/articles/2014-12-31/old-blackberrys-came-to-the-rescue-after-sonys-systems-hacked?utm_source=website&utm_medium=share&utm_campaign=copy

GILES K., Russia's Public Stance on Cyberspace Issues, Oxford UK, 2012, in CCDCOE disponibile su https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf

GILL T.D., Chapter 5. The Temporal Dimension of Self-Defense: Anticipation, Pre-emption, Prevention and Immediacy, in Brill, Leiden, 2007 disponibile su https://doi.org/10.1163/ej.9789004154285.i-590.37

GIUSTI S, La Proiezione Esterna della Federazione Russa, Pisa, 2012

GORI U., GERMANI L. S., Information Warfare. Le nuove minacce provenienti dal cyber spazio alla sicurezza nazionale italiana, Milano, 2011

GREENBERG A., The International Criminal Court Will Now Prosecute Cyberwar Crimes, in wired.com, 2023, disponibile su https://www.wired.com/story/icc-cyberwar-crimes/?

GREENWOOD C., Self-Defence, in Oxford public international law, Oxford Unversity Press, 2011

GRIFFIN A, Sony hack: who are the Guardians of Peace, and is North Korea really behind the attack?, in Independent.com, 2014, disponibile su https://www.independent.co.uk/tech/sony-hack-who-are-the-guardians-of-peace-and-is-north-korea-really-behind-the-attack-9931282.html

HESSELDAHL A., Details Emerge on Malware Used in Sony Hacking Attack, in vox.com, 2014, disponibile su https://www.vox.com/2014/12/2/11633426/details-emerge-on-malware-used-in-sony-hacking-attack.

KASTRENAKES J., Sony cancels The Interview release after theaters pull out, su theverge.com, 2014, disponibile su http://www.theverge.com/2014/12/17/7412393/sony-cancels-theinterview-release-after-theaters-pull-out

LA PISCOPIA S., SETTI S., Lo spionaggio cibernetico. Profili di diritto internazionale, Roma, 2021

LAMBERTI ZANARDI P., La legittima difesa nel diritto internazionale, Milano, 1972

LAMBERTI ZANARDI P., La Legittima difesa, cit., Milano, 1972

LANGNER R., What stuxnet is all about, su langner.com, 2011, disponibile su http://www.langner.com/en/2011/01/10/what-stuxnet-is-all-about/.

LEWIS J.A., Cyber War and Ukraine, in Center for strategic & international studies (CSIS), Washington, DC, 2022, disponibile su https://www.csis.org/analysis/cyber-war-and-ukraine

LIBICKI M. C., Information Technology Standards: Quest for the Common Byte, Berkeley, 1995

LIBICKI M. C., what is Information Warfare?, Washington, 2005

LINDSAY J. R., Stuxnet and the Limits of Cyber Warfare, in "Security Studies", Vol. 22, No. 3, 2013, disponibile su https://doi.org/10.1080/09636412.2013.816122

LUTTWAK E., Strategy: The Logic of War and Peace, Cambridge (MA), 2001

MAURER T., Cyber norm emergence at the United Nations. An Analysis of the UN's Activities Regarding Cyber-security. Discussion Paper, Cambridge

(MA), in Belfercenter.org, 2016, disponibile su https://www.belfercenter.org/publication/cyber-norm-emergence-united-nations-analysis-uns-activities-regarding-cyber-security

MCCOUBREY H., WHITE N.D., International law and armed conflict, Dartmouth, 1992.

MELE S., I principi strategici delle politiche di cybersecurity, su sicurezza nazionale.gov.it, 2013, disponibile su https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-dellepolitiche-di-cyber-security.html

MELE S., Sicurezza nazionale ICT, perché il decreto sul Perimetro farà la differenza, in Agenda digitale, 2019, disponibile su https://www.agendadigitale.eu/sicurezza/sicurezza-nazionale-ict-perche-il-decreto-sul-perimetro-fara-la-differenza/

MELE S., MORO F.N., Cyber security: un fronte sempre più caldo, in ispionline.it, 2015, disponibile su http://www.ispionline.it/sites/default/files/pubblicazioni/commentarymelemoro.pdf.

MIELI R., Israele reagisce a un attacco cyber di Hamas e ne abbatte il quartier generale informatico, su formiche.net, 2019, disponibile su https://formiche.net/2019/05/israele-abbattuto-quartier-generale-cyber-hamas/

MILANOVIC M., Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, in Harvard International Law Journal, Cambridge, 2015, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485#

NAKASHIMA E., Iran blamed for cyberattacks on U.S. banks and companies, su washingtonpost.com, 2012, disponibile su https://www.washingtonpost.com/world/national-security/iran-blamed-for-cyberattacks/2012/09/21/afbe2be4-0412-11e2-9b24-ff730c7f6312_story.html

NOCETTI J., cap. Cyber Power, Routledge Handbook of Russian Foreign Policy, 2018, disponibile su https://doi.org/10.4324/9781315536934

OSBORNE C., colonial pipeline ransomware attack: everything you need to know, in zdnet.com, 2021, disponibile su https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

PRETO P., Le parole dello spionaggio, in Per Aspera ad Veritatem, 1996, disponibile su https://gnosis.aisi.gov.it/sito/rivista6.nsf/servnavig/5

PUSTORINO P., Lezioni di tutela internazionale dei diritti umani, Bari, 2020

QUADRI R., Diritto Internazionale Pubblico, Napoli, 1968

REISMAN M., ARMSTRONG A., The Past and Future of the Claim of Pre-emptive Self-Defense, in American Journal of International Law, Loyola

university, New Orleans, 2006, disponibile su https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2169416

REVERON D. S., Cyberspace and National Security, Washington (DC), 2012

RID T., Cyber War Will Not Take Place, London, 2017

RONZITTI N., Diritto Internazionale, Torino, 2019

RONZITTI N., Diritto internazionale dei conflitti armati, Torino, 2022

RONZITTI N., La Corte Internazionale di Giustizia e la questione della liceità della minaccia o dell'uso delle armi nucleari, in Rivista di diritto internazionale, 4/1996

ROSCINI M., Cyber operations and the use of force in international law, Oxford, 2014,

SANGER D., FACKLER M., NSA breached north korean networks before sony attack, officials say, su newyorktimes.com, 2015, disponibile su https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

SARTOR G., La rivoluzione informatica e la globalizzazione, in Diritto, politica e realtà sociale nell'epoca della globalizzazione – Atti del XXII Congresso della Società Italiana di filosofia giuridica e politica, Macerata, 2002, disponibile su https://eum.unimc.it/it/index.php?controller=attachment&id_attachment=789

SCHMITT M.N., Computer network attack and the use of force in international law: thoughts on a normative framework, in The Columbia Journal of Transnational Law, Volume 37, 1999, disponibile su https://nsarchive.gwu.edu/sites/default/files/documents/3460881/Document-04-Michael-N-Schmitt-United-States-Air.pdf

SCHMITT M.N., Tallin Manual on the International Law Applicable to Cyber Warfare, Schmitt M.N., 2013

SCHMITT M. N., In Defense of Due Diligence in Cyberspace, in The Yale Law Journal Forum, 2015, disponibile su https://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace

SCHMITT M. N., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017

SCHMITT M. N., Three International Law Rules for Responding Effectively to Hostile Cyber Operations, in justsecurity.org, 2021, disponibile su https://www.justsecurity.org/77402/three-international-law-rules-for-respondng-effectively-to-hostile-cyber-operations/.

SCHMITT M., Top Expert Backgrounder: Russia's Solar Winds Operation and International Law, in Just Security, 2021, https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/.

SCOLART B., Il diritto all'autodifesa nel dominio cyber, in difesa.it, Roma, 2020, disponibile su https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/AO_SMD_01_Scolart.aspx

SHACKLEFORD S. J., From Nuclear War to Net War. Analogizing Cyber Attacks in International Law, in Berkeley Journal of International Law, Vol. 27, No. 1, 2009, p. 209,

SMITH B., The Third Industrial Revolution: Policymaking for the Internet, in Science and Technology Law Review, vol. 3, 2019, disponibile su https://doi.org/10.7916/stlr.v3i0.3621

TIKK E., KASKA K., VIHUL L., International Cyber Incidents, legal considerations, in NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010, disponibile su https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

TUNKIN G. I., Theory of International Law, Cambridge, 1974

VENTURINI G., Necessità e proporzionalità nell'uso della forza militare in diritto internazionale, Milano, 1988

VIGLIONE S., La nozione di minaccia e il riferimento ai rapporti tra Stati ex art. 2 par. 4 della Carta ONU, in iusinitinere.it, 2018, disponibile su https://www.iusinitinere.it/la-nozione-minaccia-riferimento-ai-rapporti-stati-ex-art-2-par-4-della-carta-onu-7758

WALL D. S., Cybercrime. The Transformation of Crime in the Information Age, Cambridge, 2007

WHEELER D. A., LARSEN G. N., Techniques for Cyber Attack Attribution, in Institute for defence analysis, 2003, disponibile su https://apps.dtic.mil/sti/pdfs/ADA468859.pdf

WILMSHURST E., The Chatham House Principles of International Law on the Use of Force in Self-Defence, in International & Comparative law quarterly, vol. 55, n. 4., Cambridge, 2008, disponibile su https://doi.org/10.1093/iclq/lei137

WISE A., The Republican National Committee Was Targeted by Hackers, su npr.org, 2021, disponibile su https://www.npr.org/2021/07/06/1013545363/russians-tried-to-hack-republican-national-committee.

YANNAKOGEORGOS P.A., LOWTHER A.B., Conflict and Cooperation in Cyberspace: The Challenge to National Security, Boca Raton, FL, 2013.

ZANARDI LAMERTI P., La legittima difesa nel diritto internazionale, Milano, 1972

ZIOLKOWSKY K., Computer network operations and the law of armed conflict, in The Military Law and the Law of War Review, Vol. 49, in ismllw.org, 2010, disponibile su http://www.ismllw.org/REVIEW/2010%20ART%20Ziolkowski.php

Sitografia

Agenda digitale: *www.agendadigitale.eu*

Agenzia per la cybersicurezza nazionale: *www.acn.gov.it*

Altalex: *www.altalex.com*

Analisi difesa: *www.analisidifesa.it*

Association of southeast asian nations: *www.asean.org/*

Centro Alti Studi per la Difesa (CASD): *www.difesa.it/smd_/casd*

Centro italiano di strategia e intelligence: *www.cisint.org/*

Centro studi internazionale (CESI): *www.cesi-italia.org/it*

Coalition for the ICC: *www.coalitionfortheicc.org*

Comando per le operazioni in rete: *www.difesa.it/smd_/cor*

Comitato internazionale della Croce Rossa: *www.icrc.org/it*

Commissione del diritto internazionale: *www.legal.un.org/ilc*

Commissione europea: *www.commission.europa.eu/index_it*

Computer Security Incident Response Team - Italia: *www.csirt.gov.it/*

Consiglio d'Europa (COE): *www.coe.int/en/web/portal*

CCDOE: *www.ccdcoe.org/*

Corte internazionale di giustizia: *www.icj-cij.org*

Corte penale internazionale: *www.icc-cpi.int*

Cyber defence magazine: *www.cyberdefensemagazine.com*

Cyberknow: *www.cyberknow.medium.com*

Cyberlab: *www.cyberlaw.ccdcoe.org*

Cyberlaws: *www.cyberlaws.it*

Cyberscoop: *www.cyberscoop.com/*

Cybersecurity & infrastructure security agency: *www.cisa.gov*

Cybersecurity360: *www.cybersecurity360.it*

Digital front lines: *www.digitalfrontlines.io*

Dipartimento federale degli affari esteri (DFAE): *www.eda.admin.ch*

Diritto.it: *www.diritto.it*

Economic Community of West African States (ECOWAS): *www.ecowas.int*

E-Estonia: *www.e-estonia.com*

European Journal of International Law (EJIL:Talk!): *www.ejiltalk.org*

Federal office for information security (GER): *www.bsi.bund.de/en*

Federation of american scientist, IRP: *www.irp.fas.org*

Global Centre for the Responsibility to Protect: *www.globalr2p.org*

Human Right Center, UC Berkley: *www.humanrights.berkeley.edu*

International advisory Council: *www.advisorycouncilinternationalaffairs.nl*

International Telecommunication Union (ITU): *www.itu.int*

Istituto di diritto internazionale: *www.idi-iil.org/en*

Iusinitinere: *www.iusinitinere.it*

Lieber institute: *www.lieber.westpoint.edu*

Ministero della Difesa: *www.difesa.it*

NATO Communications and information agency: *www.ncia.nato.int*

NATO: *www.nato.int*

Office of the Director of national intelligence: *www.odni.gov*

ONU: *www.un.org*

Opiniojuris: *www.opiniojuris.it*

Organization for Security and Co-operation in Europe: *www.osce.org*

Organization of American States: *www.oas.org*

Richard Clarcke: *www.richardaclarke.net*

Security Council Report: *www.securitycouncilreport.org*

Shangai Cooperation Organisation:*eng.sectsco.org*

Sidiblog: *www.sidiblog.org*

SISR: *www.sicurezzanazionale.gov.it*

Studio Previti: *www.previti.it*

Supreme headquarters allied powers Europe: *shape.nato.int*

The Strategy Bridge: *thestrategybridge.org*

UE Agenzia per la cibersicurezza (ENISA): *www.enisa.europa.eu/*

UN Conference on trade and development: *https://unctad.org*

Consiglio di sicurezza ONU: *www.un.org/securitycouncil/*

UN digital library: *https://digitallibrary.un.org*

UN institute for disarmament research: *https://unidir.org*

UN Office of information and communications technology: *https://unite.un.org/*

UN Office of legal affairs: *https://legal.un.org*

UN Office of the high commissioner for the human rights: *www.ohchr.org*

UN Office on drugs and crime: *www.unodc.org*

UN Official document system: *https://daccess-ods.un.org*

UN Regional information center for western Europe: *unric.org*

Università degli studi di Firenze, CSSI: *www.cssii.unifi.it*

Unione Africana: *https://au.int*

Università degli studi di Padova, diritti umani: *https://unipd-centrodirittiumani.it/*

U.S. Cyber command: *www.cybercom.mil*

Yarix labs: *www.labs.yarix.com*

Fino di pubblicare nel marzo 2024

TTS

Centro Studi Sviluppo
Relazioni per la Sicurezza