Istituto di Ricerche Internazionali
ARCHIVIO DISARMO

SIS n. 11/2014

Cyber war e cyber security

Diritto internazionale dei conflitti informatici, contesto strategico e strumenti di prevenzione e contrasto

di Emanuele Greco

Novembre 2014

SISTEMA INFOMATIVO A SCHEDE

Periodico Mensile
dell'IRIAD

Istituto di Ricerche Internazionali Archivio Disarmo (IRIAD)
SIS – 11/2014

In questo numero:

CYBER WAR E CYBER SECURITY
DIRITTO INTERNAZIONALE DEI CONFLITTI INFORMATICI, CONTESTO STRATEGICO E STRUMENTI DI PREVENZIONE
di Emanuele Greco

Pag. 3

Rubrica
FINESTRA SUL MONDO
- IS e il nuovo volto del Jihad
- L'educazione per tutti e la battaglia di Malala Yousafzai

di Barbara Gallo

Pag. 89

Sistema informativo a schede (SIS)
Mensile dell'Istituto di Ricerche Internazionali Archivio Disarmo (IRIAD)
Piazza Cavour 17, 00193 – Roma (RM)
Tel. 0636000343; Fax. 0636000345
www.archiviodisarmo.it

Direttore Responsabile: Sandro Medici
Direttore Scientifico: Maurizio Simoncelli
Registrazione Tribunale di Roma n. 545/96

Copyright © Istituto di Ricerche Internazionali Archivio Disarmo (IRIAD)

Emanuele Greco

CYBER WAR E CYBER SECURITY

DIRITTO INTERNAZIONALE DEI CONFLITTI INFORMATICI, CONTESTO STRATEGICO E STRUMENTI DI PREVENZIONE

ABSTRACT

Negli ultimi anni, l'attenzione nei confronti degli attacchi informatici è cresciuta tanto nei mass media e nell'opinione pubblica, quanto nelle istituzioni. Ovunque, però, traspare un'evidente incertezza nella definizione di queste operazioni, troppo spesso erroneamente ricondotte all'espressione *cyber war*. Tale semplificazione concettuale genera la concezione di spazio informatico come ambiente privo di regole in cui tutto può accadere e favorisce una retorica di tipo allarmistico che giustifica l'istituzione di numerose agenzie preposte a garantire la sicurezza informatica. Invece, è necessario stimolare una maggiore conoscenza del fenomeno in modo da poter definire le aree attraverso cui catalogare le diverse operazioni informatiche (*cyber war*, *cyber crime*, *info war*, ecc). In questa prospettiva, il diritto internazionale che disciplina l'utilizzo della forza nella comunità internazionale o *jus ad bellum* (contenuto nella Carta delle Nazioni Unite e nel diritto consuetudinario) aiuta a comprendere cosa è realmente una *cyber war*, chi sono i suoi attori, se è mai esistita e quali sarebbero le conseguenze e le peculiarità ad essa connesse. Sulla base di ciò diventa possibile valutare con obiettività e spirito critico le strategie e le azioni intraprese per assicurare la sicurezza informatica nell'area euro-atlantica e quali miglioramenti potrebbero essere effettuati.

In the last years, mass media, institutions and public opinion are increasing their attention on cyber attacks. However, an obvious uncertainty emerges in the definition of these operations, which are too often erroneously called *cyber war*. This conceptual simplification generates the belief that cyberspace is an unregulated environment in which everything can happen. Therefore, it produces concern in the society which justifies the foundation of several agencies of cyber security. On the contrary, it is necessary to increase the knowledge about the topic in order to distinguish cyber operations categories (*cyber war*, *cyber crime*, *info war*, etc.). In this perspective, the *jus ad bellum* (contained in the UN Charter and customary law) permits to understand what is really a *cyber war*, who are its actors, if it has ever existed and what could be its consequences and characteristics. In this way, it is possible to evaluate better strategies and actions that ensure cyber security in the euro-atlantic area.

"I computer sono incredibilmente accurati, veloci e stupidi.
Gli uomini sono incredibilmente lenti, inaccurati e intelligenti.
L'insieme dei due costituisce una forza incalcolabile"

Albert Einstein

Emanuele Greco ha conseguito la laurea in Giurisprudenza presso la *Pontificia Università Lateranense* e il master di I livello della SPICeS (Scuola di Politica Internazionale Cooperazione e Sviluppo). E' stato frequentatore della 65^ Sess. IASD (*Istituto Alti Studi della Difesa*) durante la quale ha ottenuto il master II livello in "Strategia Globale e Sicurezza" organizzato dal CASD (*Centro Alti Studi per la Difesa*) e l'Università di Roma "La Sapienza". Svolge attività di ricerca presso l'*Istituto di Ricerche Internazionali Archivio Disarmo* – IRIAD rivolgendo un'attenzione particolare ai profili normativi del disarmo, del controllo degli armamenti e delle relazioni internazionali.

INDICE

ELENCO DELLE ABBREVIAZIONI 6

PREFAZIONE 8

PARTE I
DIRITTO INTERNAZIONALE DEI CONFLITTI INFORMATICI
IL RICORSO ALLA MINACCIA E ALL'USO DELLA FORZA MEDIANTE LE OPERAZIONI INFORMATICHE

I. From cyber crime to cyber war 9
II. A colpi di bit come a colpi di bombe 12
III. Natura e soggetti della Cyber war 18
IV. Attacco informatico come uso della forza 23
V. La minaccia di un attacco informatico 32
VI. Operazioni informatiche e autotutela 33
VII. Autotutela anticipatoria e preventiva 42
VIII. Serie di eventi tenui 46
IX. Attori non-statali transnazionali 46
X. Il Consiglio di Sicurezza delle Nazioni Unite 51
XI. Case study: l'Estonia 53
XII. Considerazioni conclusive 55

PARTE II
STRATEGIE E MISURE DI PREVENZIONE E CONTRASTO ALLE OPERAZIONI INFORMATICHE NELL'AREA EURO-ATLANTICA

I. Il principio della deterrenza nell'ambito informatico 58
II. Cyber security concept 59
III. La strategia dell'Unione Europea 61
IV. La strategia statunitense 67
V. La strategia NATO 71
VI. Considerazioni conclusive 76

GLOSSARIO 77

BIBLIOGRAFIA 83

ELENCO DELLE ABBREVIAZIONI

AISE - Agenzia per l'Informazione e la Sicurezza Esterna (IT)
AISI - Agenzia per l'Informazione e la Sicurezza Interna (IT)
CCD CoE - Cooperative Cyber Defence Centre of Exellence (NATO)
CDMA - Cyber Defence Management Authority (NATO)
CDMB - Cyber Defence Management Board (NATO)
CEPOL - European Police College (UE)
CERT - Computer Emergency Response Teams (UE)
CIA - Central Intelligence Agency (US)
CNA - Computer Network Attack
CNA-OPE - Computer Network Attack Operational Preparation of the Environment
CND - Computer Network Defence
CNDA - Conference of National Armaments Directors (NATO)
CNE - Computer Network Exploitation
CNO - Computer Network Operation
CSDP - Common Security and Defence Policy (UE)
CYBERCOM - Cyber Comand (US)
DDoS - Distributed Denial of Service
DIA - Defense Intelligence Agency (US)
DIS - Dipartimento per l'Informazione e la Sicurezza (IT)
DIU - Diritto Internazionale Umanitario
DoD - Department of Defense (US)
DPPC(R) - Defence Policy and Planning Commitee in Reinforced format (NATO)
EC3 - European Cybercrime Centre (UE)
EDA - European Defence Agenzy (UE)
EESA - European External Action Service (UE)
ENISA - European Network and Information Security Agenzy (UE)
GIG - Global Information Grid
IANA - Internet Assigned Numbers Authority
IC - Intelligence Community (US)
ICANA - Internet Corporation for Assigned Names and Numbers
ICCC - The International Common Criteria Conference
ICJ - International Court of Justice
IHL - International Humanitarian Law
IT - Information Technology
ITU - International Telecommunication Union (UN)
NATO - North Atlantic Treaty Organization
NC3 - Nato Consultation Control and Command (NATO)
NCI - Nato Communications and Information Agenzy (NATO)
NCIRC - Nato Computer Incident Response Capability (NATO)

NCSA - Nato Communication and Information System Services Agenzy (NATO)
NDPP - Nato Defence Planning Process (NATO)
NGO – Non Governmental Organization
NIAG - Nato Industrial Advisory Group (NATO)
NIS - Network and Information Security (UE)
NMA - Nato Militay Authorities (NATO)
NSA - National Security Agenzy (US)
ONU - Organizzazione delle Nazioni Unite
UE – Unione Europea
UN – United Nations
US – United States

PREFAZIONE

Il presente elaborato si prefigge l'obiettivo di realizzare un po' di ordine concettuale sulla reale natura della *cyber war*.

Troppo spesso, infatti, questa espressione viene erroneamente ridotta ad unico contenitore concettuale all'interno del quale inserire ogni sorta di operazione cibernetica: spionaggio, furto di segreti industriali, *datagate* vari, disinformazione, attacchi a infrastrutture critiche, ecc.

Inoltre, parallelamente all'aumento esponenziale della dipendenza col cyberspazio in ogni aspetto della vita umana e della casistica delle operazioni informatiche aggressive, l'inesatto riferimento diventa sempre più frequente.

Da un lato, la complessità della materia, caratterizzata da numerose sfumature normative, genera confusione non solo tra gli operatori dell'informazione, ma tra gli stessi addetti ai lavori.

Dall'altro, però, la facilità di un siffatto utilizzo svela una certa convenienza mediatica, laddove contribuisce a creare clamore intorno alle notizie pubblicate.

Tuttavia, è necessario evitare un eccessivo ricorso a termini come *war* oppure *attack*. Una tale retorica si presta a fraintendimenti visto che le conseguenze che possono derivare dalle operazioni informatiche sono diverse, così come diverse sono le risposte che il diritto consente agli Stati di intraprendere.

In altre parole, in questo elaborato troveranno risposta domande quali: che cos'è veramente una *cyber war*, quando ha inizio, chi sono i suoi attori, quali conseguenze comporta e quali sono le regole che la disciplinano?

Il metodo utilizzato è rigorosamente scientifico e dottrinale, caratterizzato da ragionamenti resi accessibili dall'analisi delle caratteristiche empiriche del fenomeno e da numerosi esempi. La narrazione segue il criterio secondo cui la comprensione di un passaggio è indissolubilmente legata a quello che lo precede.

Durante la lettura ci si renderà conto di come il ricorso alle espressioni *cyber war* o *cyber attack*, nell'ottica di una corretta informazione, debba essere sicuramente meno gratuito e più ponderato.

Successivamente, consapevoli delle effettive minacce alla pace che si celano dietro ogni singola operazione informatica, verranno analizzate gli strumenti e le strategie che nell'area euro-atlantica sono state elaborate per contrastare e prevenire tutti i tipi di attacchi informatici, in una generica ottica di *cyber security*.

PARTE I

IL DIRITTO INTERNAZIONALE DEI CONFLITTI INFORMATICI

Il ricorso alla minaccia o all'uso della forza mediante le operazioni informatiche

Sommario: I. From cyber crime to cyber war – **II .** A colpi di bit come a colpi di bombe – **III.** Natura e soggetti della cyber war – **IV.** Attacco informatico come uso della forza – **V.** La minaccia di un attacco informatico – **VI**. Operazioni informatiche e autotutela – **VII.** Autotutela anticipata e preventiva – **VIII.** Serie di eventi tenui – **IX.** Attori non-statali transnazionali – **X.** Il consiglio di sicurezza delle nazioni unite – **XI.** Case study: l'Estonia – **XII.** Considerazioni conclusive.

I. From cyber crime to cyber war

L'avvento di Internet e della tecnologia informatica (IT) ha causato un mutamento epocale nelle dinamiche della società moderna sia civile sia militare[1]. Negli ultimi anni, in particolare, l'interesse sulle questioni legali riguardanti i problemi e le ostilità generate attraverso il cyberspazio è stato particolarmente elevato. La rete ha aperto un nuovo spazio conflittuale, un teatro artificiale di guerra supplementare ai teatri naturali di terra, d'aria, di mare e di spazio[2], che ha la capacità, inoltre, di essere interconnesso con tutti loro indipendentemente dalle frontiere.

Se queste caratteristiche sono di grande utilità in tempo di pace, in tempo di guerra 'interconnettività' significa che tutto ciò che ha un'interfaccia su internet può divenire oggetto di aggressione da qualsiasi parte del mondo. Significa che gli effetti di un attacco possono estendersi su altri sistemi. Le reti militari, ad esempio, in molti casi dipendono da infrastrutture commerciali civili.

Le operazioni informatiche possono essere descritte come l'invio di un flusso di dati verso e tramite un computer o un sistema di computer. Tali operazioni possono puntare a fare cose diverse, per esempio infiltrarsi in un sistema per raccogliere, esportare, distruggere, modificare o crittografare i dati o per attivare, modificare o manipolare i processi controllati dal sistema informatico che subisce l'infiltrazione. Conseguentemente, possono danneggiare o alterare una serie di obiettivi nel 'mondo reale', come le industrie o le infrastrutture delle

[1] Sulla trasformazione cui è andata incontro la nostra società con la "Rivoluzione" informatica si veda Heather Harrison Dannis, *Cyber Warefare and the Laws of War*, in *Cambridge studies in international and comparative law*, Cambridge University Press, Cambridge and New York, 2012, pagg. 26 - 27, la quale ha svolto un'analisi comparativa tra i *social trends* e i *military trends*.

[2] Melzer Nils in, *Cyberwarfare and International Law*, UNIDIR Resources, Ideas For Peace And Security, Ginevra, 2011, p. 3, parla di un *"quinto"* dominio della guerra.

telecomunicazioni o dei sistemi finanziari[3]. Gli effetti potenziali di tali operazioni generano, quindi, una seria preoccupazione per quanto riguarda la sicurezza degli Stati, nonché, nell'eventuale corso di un conflitto, preoccupazioni di carattere umanitario. Ciò trova un legittimo riscontro se si pensa che potrebbero essere manomessi sistemi informatici di supporto a servizi basilari (es. i sistemi ospedalieri), i sistemi di controllo del traffico aereo, le centrali elettriche, i sistemi di flusso degli oleodotti o, addirittura, gli impianti nucleari.

Il cambiamento strutturale che la nostra società sta affrontando dal punto di vista valoriale impone una rivisitazione delle necessità umane degne di protezione in tempo di pace e in tempo di guerra. Se da un lato, la società considera l'accesso ad internet come un diritto da garantire[4], dall'altro, non è possibile considerare il *cyber spazio* come un ambiente senza regole in cui tutto è lecito. Le norme giuridiche esistenti, infatti, dovrebbero essere interpretate in funzione della loro applicazione anche nel dominio informatico.

Date queste premesse, nella seguente ricerca, si è affrontato lo sforzo di analizzare le regole esistenti che disciplinano l'uso della forza nella comunità internazionale per vedere come esse trovino applicazione anche nel caso delle operazioni informatiche.

Inizialmente, è necessario specificare che il procedimento ermeneutico, seguito nel corso del trattato, ha avvalorato una concezione ampia di *cyber security*.

Infatti, le operazioni illecite condotte nell'arena informatica sono riconducibili a due realtà ben distinte a livello giuridico: si tratta del cosiddetto *cyber crime*[5] e della nuova dimensione di conflitto internazionale: la *cyber war*. In mezzo sono individuabili anche fenomeni empirici distinti: come quelli della *info war* o del *cyber terrorismo*[6], che, però, non trovano una specifica autonomia nel diritto, né una precisa collocazione, potendo rientrare, a seconda dei casi e dei soggetti, nell'una

[3] Agli albori, quando gli attacchi informatici venivano considerati come un semplice rischio possibile, molti erano scettici sull'attendibilità futura della minaccia e li consideravano poco più che 'fastidi' che non erano in grado di causare conseguenze nel mondo reale. Per es. v. PBS Frontline, *Interview with James Lewis for Frontline: Cyber War!*, in http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/lewis.html.

[4] Fino al 2013, già cinque Paesi hanno dichiarato l'accesso a internet essere un diritto fondamentale (Costa Rica, Estonia, Finlandia, Francia e Grecia).

[5] Esso include diversi reati, tra i quali la frode informatica, il furto, la divulgazione, pubblicazione, diffusione di materiale pedopornografico, la pornografia virtuale, le violazioni del copyright o della privacy, lo spionaggio industriale, ecc., previsti dagli ordinamenti statali e dalle convenzioni internazionali in materia, come la Convenzione del Consiglio d'Europa sul Cyber crime ratificata in Italia con Legge 18 marzo 2008, n. 48 .

[6] In questa tipologia potrebbe rientrare il collettivo hacker *Anonymous*, diventato famoso per aver organizzato proteste on-line, nonché veri e propri attacchi cibernetici nei confronti di strutture statali, in particolare contro lo Stato di Israele.

o nell'altra disciplina[7]. Questa ambiguità, conduce taluno ad asserire l'inesistenza di quadro giuridico nazionale o internazionale specifico in materia di 'terrorismo informatico' e a dibattere intorno alla sua effettiva esistenza[8].

Nelle loro definizioni più banali: 1) la guerra cibernetica è un conflitto tra soggetti di diritto internazionale condotto tramite operazioni informatiche; 2) il cyber terrorismo è un atto di terrorismo in genere, eseguito da un attore non-statale; 3) l'info war è l'atto di raccogliere informazioni tramite sistemi informatici da parte delle agenzie di sicurezza statali; 4) il crimine informatico è un qualsiasi reato commesso utilizzando un computer.

Una determinata attività informatica trova spazio nell'uno o nell'altro fenomeno, e nelle rispettive discipline giuridiche, a seconda che venga svolta da soggetti privati o da o per conto di soggetti di diritto internazionale, quali gli Stati, a seconda degli obiettivi dell'attacco, dagli effetti che produce o, anche, dalle motivazioni. La distinzione non è netta (prefigurandosi alcune volte responsabilità statali nel caso di attacchi 'privati'), né di facile intuizione, proprio per la difficoltà tecnica di individuare coloro che stanno dietro a un danno informatico[9]. A rendere la situazione più complessa è la proliferazione di attori non-statali a connotazione transnazionale coinvolti nei conflitti internazionali e la cui apparizione provoca non poche tensioni ed ambiguità nel capire se e quando il diritto internazionale sia ad essi applicabile[10]. Questo nodo gordiano costituisce una delle più grandi sfide contemporanee del diritto internazionale e le decisioni in merito avranno delle ripercussioni anche nel cyberspazio.

---

[7] Allo stesso modo gli atti per così dire tradizionali commessi dai gruppi terroristici possono essere disciplinati dal diritto interno o rientrare nel più ampio fenomeno delle cd. *guerre asimmetriche*, condotte contro soggetti non-statali (quali appunto i terroristi), e disciplinate dalle norme che regolano i conflitti armati internazionali e non-internazionali.

[8] Per approfondimenti si veda Vismara Luca Francesco, *Il cyber-terrorismo esiste o non esiste?*, Eurasia Rivista di Studi Geopolitici, 2012, in http://www.eurasia-rivista.org/il-cyber-terrorismo-esiste-o-non-esiste/15339/.

[9] La digitalizzazione su cui è costruito il cyberspazio consente l'anonimato e quindi complica l'attribuzione di condotta. Così, in molti casi, sembra che sia difficile, se non impossibile identificare l'autore di un attacco. Dal momento che il diritto che governa l'utilizzo della forza e il diritto internazionale umanitario si basano sull'attribuzione di responsabilità alle parti in conflitto e persino agli individui, ciò pone notevoli difficoltà. In particolare, se l'autore di una determinata operazione informatica non può essere identificato, è estremamente difficile determinare se il diritto internazionale umanitario possa essere applicabile a questa operazione.

[10] Si pensi al fenomeno della privatizzazione della guerra, che vede il proliferare di compagnie private (*PMF*: Private Military Firms secondo la definizione di P.W. Singer) che forniscono armamenti, sicurezza e servizi militari a chiunque abbia la disponibilità economica per commissionarli (principalmente gli Stati). Tali società non si esimono, ovviamente, dal fornire anche servizi di protezione informatica altamente specializzati. Sulle nuove forme di guerra in cui sono coinvolte le PMF ulteriori si veda Vignarca Francesco, *Mercenari S.P.A.*, BUR Futuropassato, Milano, 2004, da pag.199 a pag. 213. Per uno sguardo più italiano centrico al fenomeno delle PMF si veda Esther Marchetti, *Private Military and Security Companies: il caso italiano nel contesto internazionale*, Quaderni IAI, n. 7 Edizioni Nuova Cultura, Roma, 2013.

II. A colpi di bit come a colpi di bombe

Un primo passo per stabilire quali siano le regole attuali che disciplinano la *cyber war* è quello di esaminare la regolamentazione giuridica corrente dei conflitti armati e vedere se è possibile applicare la stessa a questa nuova forma di conflittualità. Per prima cosa, è necessario, quindi, analizzare i principi generali che sottendono alle leggi dei conflitti armati e cercare di valutare se i valori che esse cercano di proteggere sono gli stessi delle società moderne, sempre più dipendenti dall'informazione tecnologica e costantemente vittime di attacchi informatici[11].

L'applicazione delle leggi relative l'utilizzo della forza fra Stati (*jus ad bellum*) e la condotta dei conflitti armati (*jus in bello*) sono caratterizzate da un costante bilanciamento tra diritti e doveri degli Stati, nel primo caso, e tra il principio di umanità[12] e il principio di necessità militare[13], nel secondo caso. Stabilire come si inserisce in tutto ciò la *cyber war* non è compito facile, soprattutto in funzione dell'individuazione della responsabilità per gli eventuali danni procurati.

Bisogna, preliminarmente, sconfessare un luogo comune: per cui con l'espressione *cyber war* non si intende una particolare categoria di guerra con regole proprie e a sé stanti, ma piuttosto l'utilizzo di particolari strumenti tecnico-informatici, durante una guerra di stampo tradizionale[14].

Nonostante ci sia parte della dottrina[15] che continui ad affermare la necessità di una Convenzione Internazionale che affronti i problemi provocati dagli attacchi informatici, bisogna tenere conto del fatto che il cyberspazio non rappresenta un nuovo mondo concettuale in cui ci si combatte liberi da vincoli con il mondo reale: una specie di Matrix, parafrasando il titolo di un famoso film. Gli

[11] Per esempio, le leggi dei conflitti armati proteggono gli obiettivi civili, come conseguenza del principio di distinzione (*"i belligeranti debbono orientare l'azione militare distinguendo sempre tra la popolazione civile e i combattenti come pure tra obiettivi civili e militari"*). Perciò è necessario rivalutare le ragioni che stanno alla base del principio di distinzione, per stabilire se la sua protezione possa essere estesa anche agli obiettivi civili digitali, alla luce della diversa concezione di proprietà presente nella società moderna e della importanza della proprietà digitale nello scambio dei dati e delle informazioni, tenendo conto infine del fatto che il settore digitale ormai è diventato una vera e propria estensione della nostra personalità, non solo dal punto di vista sociale, ma anche quale strumento che garantisce i servizi essenziali (si pensi all'*home banking*).

[12] Clausola Martens, 1899.

[13] Dichiarazione di San Pietroburgo,1868.

[14] Con questa espressione si fa riferimento ai conflitti previsti dal I e dal II Protocollo Aggiuntivo alle Convenzioni di Ginevra e, quindi, a quelli internazionali e non-internazionali.

[15] Per approfondimenti si veda Brown Davis, *A Proposal for an International Convention to Regulate the Use of Information System in Armed Conflict*, 47 Harv. Int'l L.J., 179, 2006; ovvero Hollis, Duncan B., *Why States Need an International Law for Information Operations*, 11(4) Lewis & Clark L. Rev. 1023, 2007.

attori della cyber war agiscono nel mondo reale, così come gli hardware e i networks necessitano di strutture fisiche.

Infatti, se definiamo la guerra come *"una contesa tra due o più Stati attraverso le loro forze armate, con il fine di sopraffarsi vicendevolmente ed imporre le condizioni del vincitore"*[16], appare evidente che a prescindere dallo strumento utilizzato, sono gli effetti, *alias* i danni, che devono essere presi in considerazione per stabilire quando da una determinata azione scaturisce una guerra e quando conseguentemente è applicabile la normativa di riferimento.

A sostegno di questa interpretazione vi è il fatto che, anche, un'eventuale *nuclear war* sarebbe soggetta alle norme che disciplinano la condotta degli Stati nei conflitti armati, sebbene non vi sia alcuna regolamentazione che vieti o tantomeno limiti l'utilizzo delle armi nucleari, il cui disimpiego si regge unicamente sul principio della deterrenza[17]. Mere definizioni di modi diversi di condurre la guerra non corrispondono all'applicazione di regole diverse. Per il diritto dei conflitti armati, senza voler minimizzare le particolarità della sua applicazione al contesto cibernetico, la guerra è guerra. Nonostante l'avvento delle nuove tecnologie, insomma, la natura dei conflitti armati, dal punto di vista giuridico, rimane la stessa.

Una certa perplessità su questo assunto, tuttavia, potrebbe nascere dal confronto tra una pronuncia della *Corte Internazionale di Giustizia*, secondo la quale il diritto dei conflitti armati si applica to *"any use of force, regardless of the weapons employed"* (trad. qualsiasi uso della forza, indipendentemente dalle armi impiegate)[18], e la stretta applicazione che gli Stati fanno di un famoso principio contenuto in un pronunciamento della *Corte permanente di giustizia internazionale*[19], secondo il quale gli atti non proibiti nel diritto internazionale sono generalmente permessi.

Se non vi è dubbio che vi sia un conflitto armato e che il diritto internazionale umanitario trovi applicazione quando le armi tradizionali sono

---

[16] Lauterpacht Hersch, *Oppenheim's Intnational Law*, Longmans, Green & Co, 7ma edizione, Londra, 1952, p. 270

[17] Sull'argomento si veda Emanuele Greco, *Gli arsenali nucleari mondiali. Profili di diritto internazionale*, 2013, disponibile su www.archiviodisarmo.it > Nuclearnews o al seguente link:http://www.archiviodisarmo.it/siti/sito_archiviodisarmo/upload/documenti/31872_GRECO_-_Gli_arsenali_nucleari_mondiali_nel_2013.pdf.

[18] *Legality of the threat or use of nuclear weapons*, Advisory opinion, I.J.C. Reports 1996, 226 (July 8), para. 39, in http://www.icj-cij.org/docket/files/95/7495.pdf.

[19] Essa ha affermato *"The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these Co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed"*. Lotus Case, *S.S. 'Lotus' (Fr. v. Turk.)*, 1927 P.C.I.J. (ser. A) No. 10, (Sept. 7), p. 18; in http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

utilizzate in combinazione con le operazioni informatiche, ciò non è scontato nel caso di atti ostili condotti unicamente per mezzo di operazioni informatiche. In altre parole, queste ultime da sole possono essere elementi costitutivi di un conflitto armato ai sensi delle regole che governano l'uso o la minaccia della forza fra gli Stati e secondo le Convenzioni di Ginevra? La risposta, probabilmente, può essere determinata, in modo definitivo e autorevole, solo attraverso la pratica futura.

Però, alla luce del più recente pronunciamento della *Corte Internazionale di Giustizia*, nonché dell'analisi del comportamento degli Stati sempre più preoccupati degli effetti che possono scatenare le guerre cibernetiche, generalmente si ritiene che la mancanza di regole pattizie per le operazioni cibernetiche non costituisce motivo per la mancata applicazione del diritto internazionale *ad* o *in bello*. Anche il *Comitato Internazionale della Croce Rossa* si è pronunciato a favore di questa prospettiva[20], affermando che *"non vi può essere alcun dubbio che il DIU (Diritto Internazionale Umanitario) si applichi ai nuovi armamenti e all'impiego in guerra dei nuovi sviluppi tecnologici, come riconosciuto, tra l'altro, dall'articolo 36 del I Protocollo addizionale"*[21].

Il *Comitato*, con un ragionamento di più ampio respiro, analizzando più dettagliatamente la *cyber warfare*[22], nei passaggi più significativi, ha stabilito che, anche qualora una particolare attività militare non sia espressamente regolata dal diritto internazionale, non significa che essa possa essere utilizzata senza limitazioni. Mezzi e metodi di guerra che ricorrono alla tecnologia informatica dovrebbero essere soggetti al diritto internazionale umanitario così come ogni arma usata finora in un conflitto armato da o per conto di una parte del conflitto stesso. Se operazioni informatiche fossero usate contro un nemico in un conflitto armato, al fine di causare dei danni, per esempio mediante la manipolazione di un sistema di controllo del traffico aereo civile, causandone la caduta, difficilmente potrebbe essere obiettato che un tale attacco non sia in realtà un atto di guerra e che non sia, perciò, soggetto ai divieti del diritto internazionale umanitario.

Nonostante la novità, quindi, vincoli giuridici si applicano anche ai mezzi e ai metodi di guerra che fanno ricorso alla tecnologia informatica. In altre parole, mentre non vi è alcuna disposizione del diritto internazionale che esplicitamente

[20] *International Humanitarian Law and Challenges of Contemporary Armed Conflicts*, ICRC Doc. 31IC/11/5.1.2, pp. 36-38 (Oct. 2011); in http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf.
[21] (1977) I Protocollo Addizionale alle Convenzioni di Ginevra del 12 agosto 1949. Art. 36 – 'Nuove armi': *"Nello studio, messa a punto, acquisizione o adozione di una nuova arma, di nuovi mezzi o metodi di guerra, un'Alta Parte contraente ha l'obbligo di stabilire se il suo impiego non sia vietato, in talune circostanze o in qualunque circostanza, dalle disposizioni del presente Protocollo o da qualsiasi altra regola del diritto internazionale applicabile a detta Alta Parte contraente"*.
[22] *International Humanitarian Law and Challenges of Contemporary Armed Conflicts*, cit., lett. a.

vieta le operazioni informatiche, è chiaro che le operazioni informatiche nei conflitti armati possono essere intraprese solo in modo che rispettino il diritto vigente.

Il fatto che le norme vigenti siano capaci di adattarsi alle nuove tecnologie e ai nuovi metodi di condurre le guerre è reso palese, anche, dalla formulazione della *clausola Martens*[23], vero e proprio pilastro del diritto internazionale umanitario (contenente *in nuce* il *principio di umanità*), la quale, anzi, *"è stata redatta esattamente con questa intenzione"*[24]. Dello stesso parere la *Corte Internazionale di Giustizia*, secondo la quale la Clausola *"ha dimostrato di essere un mezzo efficace per affrontare la rapida evoluzione della tecnologia militare"*[25].

A fianco del principio di umanità, ritroviamo, come già detto, il *principio di necessità militare*, che *"riguarda il modo di condurre la guerra ed impone una valutazione continuativa dei combattenti sulla necessità, liceità e proporzionalità dell'uso della forza armata, così da stabilire un equilibrio tra la necessità militare e le esigenze umanitarie"*[26]. Esso trae origine dalla Dichiarazione di San Pietroburgo del 1868 e apre le porte all'applicazione del diritto dei conflitti armati nel contesto cibernetico nella parte in cui afferma *"che i progressi della civiltà devono produrre l'effetto di attenuare, nei limiti del possibile, le calamità della guerra"* e *"che il solo scopo legittimo che gli Stati devono prefiggersi durante la guerra è l'indebolire le forze militari del nemico"*. L'utilizzo della tecnologia cibernetica, infatti, per quanto potenzialmente dannoso, sta mutando completamente la natura dei conflitti, essendo ancora privo di quell'impatto distruttivo immediato tipico delle armi

[23] La Clausola Martens, che ha visto la sua prima comparsa nel preambolo della *II Convenzione dell'Aia concernente le leggi e gli usi della guerra terrestre* del 1899, costituisce il fondamento concettuale che sta alla base dell'art. 3 comune alle quattro Convenzioni di Ginevra, che tutela le persone che non partecipano direttamente alle ostilità nei conflitti armati non-internazionali. Essa è stata, anche, inserita nell'Art. 1, comma 2, del I Protocollo Addizionale del 1977 alle suddette Convenzioni, che recita: *"Nei casi non previsti nel presente Protocollo o in altri accordi internazionali, le persone civili e i combattenti restano sotto la protezione e l'imperio dei principi del diritto delle genti, quali risultano dagli usi stabiliti, dai principi di umanità e dai precetti della pubblica coscienza"*, nel preambolo del II Protocollo Addizionale: *"Ricordando che, nei casi non previsti dal diritto in vigore, la persona umana resta sotto la salvaguardia dei principi di umanità e delle esigenze della pubblica coscienza"*. La Clausola Martens rappresenta un principio di diritto internazionale consuetudinario. Sull'argomento cfr. Emanuele Greco, Emanuela Malatesta, *La violazione dei diritti umani nei conflitti armati internazionali. Il caso dei bambini soldato e della violenza di genere*, Gruppo CEDUR, 2013, pp. 12-16, oppure in www.archiviodisarmo.it>Ricerche>papers, al seguente link: http://www.archiviodisarmo.it/siti/sito_archiviodisarmo/upload/documenti/27179_Malatesta_-_Greco__Violazione_dei_diritti_umani_nei_conflitti_armati_internazionali.pdf.

[24] Heather Harrison Dinnis, *Cyber Warefare and the Laws of War*, in Cambridge studies in international and comparative law, Cambridge University Press, Cambridge and New York, 2012, pag. 28.

[25] *Legality of the threat or use of nuclear weapons*, Advisory opinion, I.J.C. Reports 1996, 226 (July 8), para. 78, in http://www.icj-cij.org/docket/files/95/7495.pdf.

[26] Vincenzo Buonomo, *Il Diritto della Comunità Internazionale*, Lateran University Press, Città del Vaticano, 2010, p. 147

convenzionali ed in quanto coinvolge solo indirettamente la popolazione civile. Almeno per ora, siamo di fronte a un fenomeno totalmente in controtendenza rispetto alle modalità di conduzione delle guerre moderne e contemporanee, dove, rispetto al passato, il coinvolgimento della popolazione civile nella lotta armata, e conseguentemente la percentuale delle vittime civili, è salita esponenzialmente[27]. Di converso, gli attori della guerra cibernetica sono essenzialmente statali, così come le strutture oggetto di attacco. Una convergenza sempre maggiore delle risorse umane e finanziarie su questo tipo di conflitto, allora, è auspicabile qualora contribuisse ad inseguire il fine ultimo delle leggi sui conflitti armati: la cd. *umanizzazione dei conflitti*, non solo in termini di vite umane risparmiate, ma anche in termini di conflitti rispettosi dei diritti umani.

Finora l'umanità è stata in grado di sfruttare il progresso tecnologico per produrre armamenti sempre più numerosi e sofisticati, in grado di coinvolgere un numero sempre più ampio di persone[28]. La guerra cibernetica, invece, sempre che mantenga nella maggior parte dei casi la sua qualità di *non-lethal weapon*[29], forse, appartiene a quei *"progressi della civiltà"* in cui la *Dichiarazione di San Pietroburgo* aveva riposto la propria fiducia.

Per cogliere questa opportunità e tenere sotto controllo il potenziale distruttivo delle operazioni informatiche, è essenziale, però, non svincolare il contesto in esame dalle norme esistenti dei conflitti armati internazionali; ipotesi che comunque appare teoricamente irrinunciabile, nonostante la troppo spesso dichiarata anarchia in cui si muoverebbero gli attacchi informatici.

Per la *Corte Internazionale di Giustizia*, pronunciatasi nella Sentenza sul *Caso delle attività militari e paramilitari in Nicaragua e contro il Nicaragua* del 27 giugno 1986, i principi generali del diritto umanitario, in quanto principi generali del diritto internazionale, oltre a fondare la protezione della persona in quanto vittima della guerra hanno un carattere vincolante indipendentemente dalla loro codificazione nei contesti specifici. Pertanto nella posizione espressa dalla Corte non è riscontrabile alcuna deroga alla loro obbligatorietà e inderogabilità. Non bisogna dimenticare, però, che ogni tentativo di applicare le norme dei conflitti armati alle *operazioni informatiche* non può prescindere da una valutazione degli

[27] Sull'argomento si veda Maurizio Simoncelli (a cura di), *La pace possibile. Successi e fallimenti degli accordi internazionali sul disarmo e sul controllo degli armamenti*, Ediesse, Roma, 2012. Del medesimo autore, *Dove i diritti umani non esistono più. La violazione dei diritti umani nelle guerre contemporanee*, Ediesse, Roma, 2010 e *Guerre senza confini*, Ediesse, Roma, 2003.

[28] Per approfondimenti si veda Stockholm International Peace Research Insitute, *Sipri Yearbook, Armaments, Disarmament and International Security*, Oxford University Press, Stockholm, 2012.

[29] Questa espressione associate alle operazioni informatiche la troviamo in Even Shmuel, Siman David-Tov, *Cyber Warfare: Concepts and Strategic Trends*, INSS - Memorandum 117, Tel Aviv, 2012, p. 14.

effetti prodotti dalle stesse, che quanto meno devono essere equiparabili alla violenza di un attacco armato convenzionale.

E la prassi degli Stati? Nessun discorso che prenda in considerazione un tema di diritto internazionale può dirsi completo se non tiene in considerazione l'elemento fondante del diritto internazionale stesso, ossia la consuetudine[30]. Di certo può dirsi che non esiste, ad oggi, una prassi consolidata, da parte degli Stati, sull'applicazione delle norme dei conflitti armati al dominio cybernetico, anzi la pratica informatica (*diuturnitas*) e le *opinio juris* disponibili sono piuttosto scarsi. Un'attenzione particolare, tuttavia, deve essere rivolta al lavoro del *North Atlantic Treaty Organization* (NATO) *Cooperative Cyber Defence Centre of Exellence* (CCDCoE), che ha riunito un Gruppo Internazionale di Esperti e ha redatto il c.d. *Tallinn Manual*[31]. Esso contiene una serie di regole, che seppur non rappresentino l'opinione ufficiale della Nato o dei suoi Stati membri, costituisce un contributo significativo per chiarire il legame tra il diritto internazionale e la *cyber war*.

Tra le dottrine maggiormente condivise vi è quella della Casa Bianca, secondo la quale: *"Lo sviluppo delle norme per la condotta degli Stati nel cyberspazio non richiede che venga reinventato il diritto internazionale tradizionale, né che vengano applicate norme internazionali obsolete. Le norme internazionali che guidano il comportamento degli Stati – in tempo di pace e in tempo di guerra – si applicano anche nel cyberspazio"*[32].

In conclusione, però, bisogna esprimere una certa cautela. Anche se le limitazioni del diritto internazionale dei conflitti armati possono essere applicate alla *cyber war*, moltissime difficoltà nascono in relazione all'interpretazione e all'applicazione di alcune specifiche norme alla fattispecie *de qua*, lasciando aperte moltissime prospettive di *lege ferenda*. Lo stesso *Tallinn Manual* riconosce la necessità, data dalle caratteristiche uniche della tecnologia, di un lavoro normativo aggiuntivo.

---

[30] Elementi della consuetudine sono: la *Diurnitas* (la prassi) e l'*opinio juris sive necessitatis* (la convinzione della obbligatorietà e della necessità del comportamento). Lo *jus cogens* è accolto sia dalla Convenzione di Vienna sul diritto dei trattati del 1969 che dalla Convenzione di Vienna sul diritto dei trattati tra Stati e organizzazioni internazionali o tra organizzazioni internazionali del 1986. Lo jus cogens è percepito dai membri della c.d. comunità internazionale (gli Stati in particolare) come diritto assolutamente inderogabile. Secondo l'articolo 53 della convenzione del 1969, *"È nullo qualsiasi trattato che, al momento della sua conclusione, sia in contrasto con una norma imperativa di diritto internazionale generale..."*.

[31] Si veda Schmitt Michael N. (a cura di), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Tallinn, 2013.

[32] *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World* o c.d. *White House Cyber Strategy,* May, 2011, p. 9, in http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

III. Natura e soggetti della Cyber war

All'espressione *cyber war* sono attribuiti molteplici significati. La maggior parte delle definizioni in circolazione, però, appare incompleta e inesatta. Ad es., Richard Clarke la definisce come le *"Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"*[33]. Questa definizione, però, appare riduttiva perché prende in considerazione unicamente l'azione degli Stati. Una definizione esaustiva dal punto di vista giuridico, perciò, potrebbe essere:

la *cyber war* è l'insieme delle condotte poste in essere nel cyberspazio per manipolare, sabotare, danneggiare o distruggere sistemi informatici e/o obiettivi civili e militari ad essi connessi, al fine specifico di causare effetti corrispondenti alla minaccia o all'uso della forza armata, prima e/o durante un conflitto che vede la partecipazione di uno o più soggetti di diritto internazionale.

La ratio di una definizione così lunga e articolata, specialmente riguardo al significato della minaccia o uso della forza, troverà giustificazione nel corso della trattazione.

Si cominci dicendo che le azioni cui ci si riferisce sono riconducibili alla nozione di *cyber operation* (o *Computer network operation* - CNO) e cioè *"all'impiego delle capacità cibernetiche con il proposito primario di raggiungere obiettivi all'interno o mediante l'uso del cyberspazio"*[34].

Secondo il Dipartimento di Difesa degli Stati Uniti le *cyber operation* possono essere distinte in tre categorie differenti: a) *computer network attack* - CNA ; b) *computer network exploitation*– CNE ; c) *computer network defence*- CND[35].

Le CNA comprendono tutte quelle operazioni *"finalizzate a disturbare, negare, degradare, distruggere le informazioni contenute all'interno di computer o reti di computer, o i computer e le reti stesse"*. Le CNE sono quelle operazioni di intelligence *"atte a permettere la raccolta di dati da una rete o un sistema informativo automatizzato di un obiettivo o di un avversario"*. Le CND, infine, si riferiscono alle *"azioni intraprese per proteggere, monitorare, analizzare, rilevare e*

[33] Richard Clarke, *Cyber war*, Harper-Collins, New York, 2010, p. 6.
[34] Per approfondimenti si veda *Tallinn Manual*, cit., *Glossary*, *Cyber operation*.
[35] US Department of Defense, *The National Military Strategy for Cyberspace operations*, 2006, GL-1, http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf; La scelta di utilizzare il presente documento per la classificazione delle operazioni informatiche è dovuta dal fatto che la maggior parte della letteratura mondiale sull'argomento *de qua* ha adottato i termini e le definizioni in esso contenute.

rispondere alle attività non autorizzate nei sistemi informativi [del Ministero della Difesa] *e nelle reti informatiche"*.

E' bene tenere a mente che, a rigore, solo le CNA, e tra queste solo quelle che costituiscono una minaccia o un uso della forza, potrebbero dare vita a una *cyber war* vera e propria.

C'è chi parla di *soft cyber war*[36] per le altre CNA che non raggiungono tale livello di bellicosità e che sono finalizzate al mero disturbo dei sistemi informatici. Una tale espressione, tuttavia, non appare condivisibile. Avallare l'esistenza di una natura ambivalente della *cyber war*, dal punto di vista giuridico, rischierebbe di creare un pasticcio concettuale.

Per le operazioni diverse (CNA che non costituiscono un uso della forza, CNE e CND), quindi, sarebbe più corretto parlare di *info war*.

Tabella n. 1: collocazione delle CNO

Computer Network Operations	
Cyber war	***Info war***
CNA che raggiungono il livello della minaccia o dell'uso della forza: sabotaggio, manomissione, danneggiamento o distruzione diretta e grave di sistemi informatici (computers, networks, database, ecc.) nonché di strutture o dispositivi fisici sensibili ad essi connessi (es. centrali nucleari, reti elettriche, centri finanziari, mezzi di trasporto, strutture militari, aerei, droni).	**CNA che non raggiungono il livello della minaccia o dell'uso della forza:** danneggiamento o distruzione lieve o parziale di sistemi informatici; interferenza o disturbo nella funzionalità dei sistemi; interruzione degli stessi; manipolazione dei dati e delle informazioni; divulgazione di dati e informazioni segrete e imbarazzanti; information operations (IO oppure INFO OPS)[37]; operazioni di preparazione alle CNA (CNA-OPE).[c.d. *soft cyber war*]
	CNE: infiltrazioni in computer o sistemi di computer; estrazione, raccolta o duplicazione di dati sensibili o riservati; furto di segreti tecnologici, militari o industriali.
	CND: spionaggio; controspionaggio; sorveglianza; isolamento e separazione dei sistemi; difesa 'dinamica'[38]; implementazione delle potenzialità informatiche e delle strutture di sicurezza; attività di formazione; valutazioni sulle capacità e sulle intenzioni del nemico; formulazione di strategie.

Nota: è, qui, presa in considerazione unicamente l'ipotesi in cui CNO siano condotte isolatamente e non in sinergia ad attacchi di altro tipo o in altri contesti (es. attacchi cinetici, elettronic warefare, ecc.).

[36] Si veda Even Shmuel, Siman David-Tov, *Cyber Warfare*, cit., pp. 22 - 24.

[37] Le *information operations* sono funzioni militari preposte al coordinamento di attività militari collegate con le informazioni ed i sistemi preposti alla loro trasmissione al fine di creare effetti desiderati sulla volontà, comprensione e capacità dell'avversario o di potenziali avversari al fine di conseguire gli obiettivi della missione.

[38] Questo concetto si basa sulla capacità di identificare le attività sul web, su sistemi di difesa automatici per identificare gli attacchi e generare una risposta automatica senza l'intervento umano e sventare le attività nemiche.

Le modalità tecniche con le operazioni informatiche possono essere condotte sono varie, versatili e adattabili ad delle categorie di cui sopra: DDoS, malware, spyware, virus, worm, pharming, phishing, backup, ecc. Le minacce, inoltre, riguardano non solo i software, ma anche gli hardware dei sistemi informatici che possono essere manomessi con l'istallazione manuale di componenti controllabili dall'aggressore. Ognuna di queste operazioni, poi, può essere effettuata sia dall'esterno di un sistema informatico, cui si accede attraverso le reti globali, sia dall'interno, attraverso personale introdotto segretamente nelle strutture organizzative, nonché attraverso azioni combinate.

Il *cyberspazio*, invece, può essere descritto come l'insieme di strutture che offrono servizi di informazione e comunicazione globalmente interconnesse attraverso una rete internet, una rete di telecomunicazioni o un sistema di computer. Oppure come *"l'ambiente formato da componenti fisici, caratterizzati dall'uso del computer e di uno spettro elettromagnetico per memorizzare, modificare e scambiare dati tramite reti di computer"*[39].

Secondo l'International Telecomunications Union (ITU)[40], invece, il cyberspazio è: *"the physical and non-physical terrain created by and/or composed of some or all of the following: computers, computer systems, network and their computer programs, computer data, content data, traffic data, and users"*.

Queste e tutte le altre definizioni del cyberspazio, proprie delle strategie dei singoli Stati, sono molto simili tra loro, tanto da implicare, in ogni caso, secondo la catalogazione presentata da Even S., la presenza di tre componenti costanti ed interdipendenti[41]:

- **The human layer** [le risorse umane dedite all'utilizzo dei sistemi di informatizzazione e comunicazione];
- **The logical layer** [i programmi/software - sistemi operativi ed applicazioni - e i bit che viaggiano nell'etere];
- **The physical layer** [le infrastrutture e le apparecchiature fisiche- nonché i loro componenti (hardware) -, mobili o fisse, che rendono possibile la trasmissione dei dati].

Già da queste definizioni, è deducibile che l'infezione di una rete di computer da parte di un nemico con un virus maligno potrebbe costituire un atto di "guerra cibernetica", al contrario di un bombardamento aereo di strutture

[39] *Tallinn Manual*, cit., Glossary, Cyberspace.
[40] L'ITU è l'agenzia specializzata delle Nazioni Unite in materia di informazione e comunicazioni tecnologiche (ICT). Il sito ufficiale è: www.itu.int.
[41] Per approfondimenti si veda Even Shmuel, Siman David-Tov, *Cyber Warfare*, cit., Table 1, pp. 10 -11.

informatiche militari. Il fatto che la *cyber war* sia condotta nel cyberspazio non vuol dire che non possa produrre effetti non elettronici, svincolati dal dominio informatico. Obiettivi della *cyber war* possono essere persone la cui vita, o oggetti la cui funzionalità, dipendono da un sistema di computer, come certamente sono i mezzi di trasporto o le persone connesse a sistemi di supporto medico, militare o professionale.

Le caratteristiche del cyberspazio sono uniche rispetto a quelle dei domini fisici (terra, mare, aria, spazio). Una valutazione strategico/comparativa tra i vantaggi e/o gli svantaggi derivanti dall'interazione di queste caratteristiche unitamente alla facoltà di condurre operazioni informatiche offensive, lo rende un luogo privilegiato per la conduzione della guerra, soprattutto per coloro i quali hanno difficoltà a ingaggiare battaglie convenzionali:

Tabella n. 2: Vantaggi e svantaggi di un'attività offensiva nel dominio informatico

Pro:	Contro:
La sua creazione e gestione è affidata contemporaneamente sia a strutture militari sia a compagnie private. Ciò aumenta considerevolmente il numero degli obiettivi sensibili.	La vastità del suo "spazio" e del suo impiego comporta una certa difficoltà nell'individuazione degli obiettivi strategici.
I continui sviluppi tecnologici, nonché la connettività e l'interdipendenza tra il cyberspazio e le apparecchiature che operano negli altri domini, se da un lato migliorano le attività umane, dall'altro ne aumentano la vulnerabilità .	I continui sviluppi tecnologici costringono a frequenti cambiamenti della strumentazione. L'aggiornamento regolare e lo sviluppo delle capacità di operare nel cyberspazio, obbligano gli utenti a migliorare e sostituire i propri strumenti di attacco e di difesa una volta diventati obsoleti.
Il cyber spazio non è soggetto a confini politici o naturali: le informazioni o i contenuti caricati sono distribuiti quasi istantaneamente da un punto di origine a qualsiasi altra destinazione nel globo connessa attraverso uno spettro elettromagnetico, ciò permette di operare attacchi fulminei anche a lunga distanza, senza la necessità di uno scontro fisico diretto.	La difficoltà tecnica che presenta la sua gestione e conseguentemente quella di garantire una continuità dell'attacco, nella maggior parte dei casi, rendono incerto il risultato dell'operazione.
I programmi/software necessari per operare nel cyberspazio riducono il margine di errore umano.	La maggioranza dei danni inflitti nel cyberspazio, escluse le eventuali ripercussioni fisiche degli stessi, sono temporanei e facilmente risanabili attraverso efficaci sistemi di backup o di rebuild.
Non è soggetto a variabili provenienti dagli altri domini (come gli agenti atmosferici), pertanto comporta una elevata capacità di controllo umano.	E' soggetto a numerosi eventi imprevisti dai gestori del dominio a causa dell'interazione massiccia di computer e dell'intensificarsi delle azioni malevole.
Permette un considerevole risparmio di tempo, mezzi e risorse umane. Inoltre, la	Operare al suo interno richiede un elevato grado di formazione e specializzazione.

produzione di massa di 'armi' nel cyberspazio è considerevolmente più veloce ed economica.	
Consente di operare attacchi generalmente meno letali sia per le truppe combattenti, sia in termini di coinvolgimento della popolazione civile, rispetto alle armi cinetiche, ma economicamente più devastanti.	Il basso margine di rischio per la vita dei combattenti e dei civili può comportare una maggiore audacia e spregiudicatezza nella promozione di operazioni offensive.
Consente di operare in pieno anonimato e di nascondersi dietro le attività di altri soggetti (hackers, organizzazioni criminali o terroristiche, agenzie estere, nazioni), ciò naturalmente favorisce una esposizione minima al rischio di accuse e di contrattacchi.	L'anonimato può causare un'escalation di risposte incontrollate e indiscriminate da parte di chi ha subito l'attacco.
Consente ai virus di replicarsi esponenzialmente e tale circostanza fornisce il vantaggio, a chi attacca, di poter creare effetti addizionali, capaci di diffondersi in maniera virale, anche mediante sforzi limitati.	Tale circostanza può causare effetti incontrollati e non voluti, comportando una riduzione in termini di selettività dei propri obiettivi e delle proprie finalità.

Nota: il punto di vista qui considerato è quello di chi attacca o di chi contrattacca.

Il cyberspazio è accessibile ai governi, alle organizzazioni internazionali, alle ONG, alle imprese private e perfino ai singoli individui, e con tutti questi soggetti sulla 'piazza', l'utilizzo di un *IP Spoofing* o di *botnet*[42], per esempio, può rendere particolarmente difficile distinguere l'origine dell'operazione.

Nonostante l'accessibilità eterogenea, però, una *cyber war* può essere scatenata unicamente a seguito di attacchi informatici condotti da soggetti di diritto internazionale[43], o da soggetti non internazionali le cui azioni sono tuttavia attribuibili ai primi, ovvero ricadono sotto la propria sovranità, e che mirano a violare la sovranità di uno Stato, influire negativamente contro di esso o che più genericamente violano un obbligo di diritto internazionale[44].

Inoltre, la fattispecie degli attacchi informatici condotti reciprocamente da forze armate regolari di uno Stato contrapposte a forze armate dissidenti o da gruppi armati organizzati che, sotto la condotta di un comando responsabile, esercitano, su una parte del territorio, un controllo tale da permettere loro di condurre operazioni militari prolungate e concertate[45], può essere qualificata come una *cyber war*.

Pertanto, come qualsiasi altra guerra, quella cibernetica può avere la duplice natura di conflitto armato internazionale e conflitto armato non-internazionale.

[42] Si veda il Glossario dell'elaborato.
[43] Per una carrellata dei soggetti di diritto internazionale o presunti tali v. Benedetto Conforti, *Diritto Internazionale*, Editoriale Scientifica, Napoli, 2006, pp.10-28.
[44] Si veda *Rule n. 1* a *Rule n. 6* del *Tallinn Manual*.
[45] Si veda Art. 1 del II Protocollo Aggiuntivo sui conflitti non internazionali, 1977.

Una riserva va fatta per il nuovo fenomeno delle guerre c.d. asimmetriche che vedono la partecipazione di attori non-statali che agiscono senza la direzione o la complicità di uno Stato, nel territorio di un altro Stato, come potrebbero essere i *cyber terroristi* (per *cyber terrorismo*, deve intendersi l'utilizzo di operazioni informatiche da parte di un gruppo terroristico così come individuabile secondo la nozione di terrorismo nel diritto internazionale[46]).

In definitiva, è corretto affermare che una *cyber war* esiste quando si creano le condizioni per l'applicazione delle norme che disciplinano l'utilizzo della forza nel diritto internazionale, nonché quelle sui conflitti armati (Diritto Internazionale Umanitario). Se così non fosse, si finirebbe per accettare passivamente la prospettiva troppo spesso ventilata dai mass media, secondo i quali una *cyber war* è oggi in corso.

A onore del vero va precisato che, nonostante la possibilità teorica che vari soggetti possano dar vita a una *cyber war*, andrebbero presi in considerazione, per una trattazione che abbia un effettivo riscontro nella realtà, solo gli Stati (tra questi principalmente Stati Uniti, Cina, Russia ed Israele) e le Organizzazioni Internazionali, i quali sono gli unici a possedere le risorse tecnico-economiche e il *know-how* necessario per attuarne una. Pertanto, è difficilmente immaginabile una *cyber war* non-internazionale (che coinvolga soggetti privi di personalità giuridica internazionale, quali quelli elencati nell'art. 1 del II Protocollo Aggiuntivo alle Convenzioni di Ginevra[47]) o di tipo asimmetrico.

Per questo motivo, d'ora in avanti la trattazione sarà dedicata principalmente al caso dei conflitti internazionali, con l'unica eccezione di una breve esposizione dedicata alle cyber war asimmetriche (v. par. IX).

IV. Attacco informatico come uso della forza

L'avvento dell'era della gestione digitale dell'informazione e delle infrastrutture impone una rivisitazione del significato del termine 'forza'.

Rispetto al passato, oggi le norme che regolano il ricorso all'uso della forza da parte degli Stati (*jus ad bellum*) sono contenute principalmente nella *Carta delle Nazioni Unite*, che prevede la proibizione dell'uso della forza[48].

[46] Per approfondimenti si veda Nigro Raffaella, *La nozione di terrorismo nel diritto internazionale*, Università degli suti di Napoli Federico II, Facoltà di Giurisprudenza, Tesi di dottorato in diritto internazionale, XVII ciclo, 2006.

[47] A conferma di ciò può dirsi che nel *Tallinn Manual* non è stata prevista alcuna Regola che disciplini questa eventualità.

[48] Il modello delle relazioni internazionali vigente fino al 1945 era fondato su un sistema prodotto quasi interamente dagli assetti della Pace di Westfalia che il 24 ottobre 1648 aveva legittimato l'uso della forza, la sua minaccia e, in particolare, della forza armata.

"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".

Art.2, comma 4 Carta delle Nazioni Unite

Tuttavia, tale proibizione non è ristretta agli Stati membri dell'Onu: la *Corte Internazionale di Giustizia* ha notato che essa rappresenta non solo un principio di diritto internazionale consuetudinario, ma un *"principio fondamentale o meglio cardine di tale diritto"*[49]. Questa previsione pertanto è da considerarsi assurta al rango di *jus cogens*, soprattutto se letta alla luce del combinato disposto dagli artt. 1 e 2 della *Carta*, che ha inteso codificare la volontà degli Stati a seguito delle disastrose esperienze della I e della II guerra mondiale, sancendo, così, il *principio dell'illiceità della guerra*, sul piano internazionale[50]. Quest'ultima precisazione è essenziale visto che tale costrutto normativo non comprende gli scontri interni o le azioni condotte da attori non-statali.

Quanto appena esposto è stato oggetto di un ampio dibattito, in quanto i redattori della Carta non hanno definito specificatamente il significato del termine 'forza'. Sin dalla Conferenza di San Francisco, i Paesi in via di sviluppo e quelli appartenenti al blocco orientale avevano richiesto l'inclusione all'interno della proibizione dell'art. 2, comma 4, delle azioni coercitive di tipo politico o economico[51]. Nonostante una certa ambiguità letterale sia rimasta all'interno della Carta (come si evince dai lavori preparatori), il pensiero prevalentemente accettato è stato quello che vede il termine suddetto riferirsi unicamente alla forza armata o di tipo militare. Ciò, a dire il vero, risulta anche da un'analisi testuale della Carta nel suo complesso.

Il termine forza, senza alcun aggettivo, appare nella Carta solamente due volte, nell'art. 2, comma 4 e nell'art. 44[52]. In quest'ultimo però il suo utilizzo è

[49] Caso delle *Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).* Merits, Judgment. I.C.J. Reports 1986, p. 14, para. 190 e 209, in http://www.icj-cij.org/docket/files/70/6503.pdf. Inoltre, la medesima posizione è stata esposta dalla Corte nella sentenza sul caso delle *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda),* Judgment, I.C.J. Reports 2005, p. 168, para. 148 e 165.

[50] Sul principio della illiceità della guerra quale garanzia di pace e sicurezza si veda Vincenzo Buonomo, *Il diritto della Comunità internazionale*, cit., pp. 123-143.

[51] Il Brasile, ad esempio, aveva proposto di estendere la proibizione dell'uso della forza *"alla minaccia o all'uso delle misure economiche che fossero i qualche modo contrari con i fini delle Nazioni Unite"*.

[52] Art. 44, Carta delle Nazioni Unite: *"Quando il consiglio abbia deciso di impiegare la forza, esso, prima di richiedere ad un Membro non rappresentato nel Consiglio di fornire forze armate in esecuzione degli obblighi assunti a norma dell'art. 43, inviterà tale Membro, ove questo lo desideri,*

contestualizzato nel Cap. VII della Carta (Azioni rispetto alle minacce della pace, alla violazione della pace ed agli atti di aggressione), per cui necessariamente si riferisce alla ristretta definizione di forza prevista dagli artt. 41 e 42[53], dove è qualificata come *"armata"*. Così se il significato del termine forza contenuto nell'art. 44 è quello appena descritto, di conseguenza, anche quello contenuto nell'art. 2, co. 4, dovrebbe essere lo stesso, a causa di una presunta e coerente relazione tra tutte le norme del Testo. Un ragionamento siffatto trova supporto anche nel Preambolo della Carta, nella parte in cui si afferma che *"la forza delle armi non sarà usata, salvo che nell'interesse comune"*. Per cui il termine forza dell'art. 2, comma 4 non può essere inteso oltre la forza armata, posto che gli articoli della Carta sono stati scritti per dare effettività e concretezza alle aspirazioni del Preambolo.

Mentre la definizione di forza è limitata alla forza armata, la definizione di forza armata *per se* deve essere interpretata in maniera ampia, ricomprendendo non solo gli atti di utilizzo diretto della forza armata, ma anche le attività indirette. La *Corte Internazionale di Giustizia*, nel caso *Nicaragua*, ha stabilito che gli atti che violano il *principio di non ingerenza*[54], se prevedano l'uso diretto o *indiretto* della forza armata, costituiscono anche una violazione del divieto di utilizzo della forza nelle relazioni internazionali[55].

L'ingerenza, di per sé, è un'interferenza esercitata da uno Stato negli affari interni ed esterni di un altro Stato con il proposito di condizionare l'esercizio della sovranità di quest'ultimo. In ogni modo l'interferenza deve essere caratterizzata dall'elemento della *costrizione* e dell'imposizione della volontà.

---

a partecipare alle decisioni del Consiglio di Sicurezza concernenti l'impiego di contingenti di forze armate del Membro stesso".

[53] Prevedono le misure non implicanti o implicanti l'impiego della forza armata che il *Consiglio di Sicurezza* può adottare in caso di accertata esistenza di una minaccia alla pace, di una violazione della pace o di un atto di aggressione. Per approfondire cfr. Benedetto Conforti,, Focarelli Carlo, *Le Nazioni Unite*, VIII ed., Cedam, Verona, 2011.

[54] Sebbene il principio di non ingerenza nel rapporto tra Stati non sia previsto espressamente dalla Carta delle Nazioni Unite, esso è implicito nel principio di sovrana uguaglianza tra gli Stati (art.2.1); esso è comunque considerato un principio di diritto internazionale consuetudinario. Tutt'al più nella Carta, all'art. 2.7 è previsto un limite ratione materiae all'azione delle Nazioni Unite, il c.d. limite della competenza interna o dominio riservato (*domestic jurisdiction*): *"Nessuna disposizione del presente Statuto autorizza le NU ad intervenire in questioni che appartengono essenzialmente alla competenza interna di uno Stato…"*.

[55] *Caso Nicaragua*, cit., para. 209. In questo caso la Corte ha stabilito che la fornitura di assistenza ai ribelli nelle forme di assistenza di armi o di supporto logistico o di altro tipo può costituire una minaccia o uso della forza. Tuttavia, ha anche stabilito che non tutte le forme di azione o di assistenza indiretta devono essere considerate tali. In particolare, ha creduto che la mera fornitura di fondi, se senza dubbio costituisce un atto di intervento negli affari interni (del Nicaragua nel caso specifico), non può essere considerata una violazione della proibizione della forza così come stabilita dall'art. 2(4) della Carta delle NU e dal suo corrispondente principio di diritto consuetudinario.

"The element of coercion, which defines, and indeed forms the very essence of prohibited intervention, is particularly obvious in the case of an intervention which use force, either in the direct form of military action, or in the indirect form of support for subversive or terrorist armed activities within another State. A noted above, General Assembly resolution 2625 (XXV) equates assistance of this kind with the use of force by the assisting State when the acts committed in another State involve a threat or use of force".

ICJ, *Caso Nicaragua*, para. 205.

In dottrina si suole affermare che si ha ingerenza quando lo Stato esterno domanda all'altro Stato di compiere un atto che, non costretto, non avrebbe compiuto o di astenersi dal compiere un atto che, non costretto, avrebbe compiuto[56].

Quindi le misure utilizzate possono anche non implicare la minaccia o l'uso della forza armata e consistere, semplicemente, in coercizioni di natura politica ed economica al fine di condizionare l'esercizio della sovranità dello Stato, secondo quanto desunto dalla *Dichiarazione relativa ai principi di diritto internazionale riguardanti le relazioni amichevoli e la cooperazione tra gli Stati conformemente alla Carta delle Nazioni Unite*[57].

La Corte, invece, riprendendo le disposizioni di quest'ultimo documento, ha enfatizzato le regole che, se violate, costituiscono non solo violazione del principio di non ingerenza, ma, anche, dell'art. 2, comma 4 e del suo *alter ego* consuetudinario:

- *Ogni Stato ha il dovere di astenersi dalla minaccia o dall'uso della forza per violare i confini internazionali esistenti di un altro Stato o per risolvere le dispute internazionali, incluse quelle territoriali;*
- *Ogni Stato ha il dovere di astenersi da qualsiasi azione diretta a privare i popoli nella formulazione del principio di uguaglianza e del loro diritto all'autodeterminazione, della loro libertà e della loro indipendenza;*
- *Ogni Stato ha il dovere di astenersi dall'organizzare o dall'incoraggiare l'organizzazione di forze irregolari o di bande armate, in particolare bande di mercenari, per compiere incursioni nel territorio di un altro Stato;*
- *Ogni Stato ha il dovere di astenersi dall'organizzare, incoraggiare, appoggiare o partecipare ad atti di guerra civile o di terrorismo nel territorio di un altro Stato, o dal tollerare sul proprio territorio attività*

[56] David, *Portée et limite du principe de non-intervention,* in Revue Belge de Droit International, 1990, p. 350.
[57] Adottata con Ris. 2625 (XXV) 24 ottobre 1970.

organizzate al fine di perpetrare tali atti, quando gli atti menzionati nel presente paragrafo comportino la minaccia o l'uso della forza;

- *Gli Stati hanno il dovere di astenersi da atti di rappresaglia che coinvolgono l'uso della forza.*

A scanso di equivoci, è importante ripetere come tale precisazione operata dalla Corte alle attività indirette rimanga ristretta alle attività militari o paramilitari. Si è già precisato che la mera fornitura di fondi ai ribelli (a differenza della fornitura delle armi) costituisce un atto di ingerenza negli affari interni (del Nicaragua nel caso specifico), ma non una violazione della proibizione dell'uso della forza. Allo stesso modo il mero finanziamento di un gruppo di attivisti che conducono operazioni cibernetiche come parte di un'insurrezione non costituirebbe un uso della forza. Mentre rifornire un gruppo organizzato con *malware* o con l'addestramento necessario per utilizzarlo al fine di effettuare attacchi informatici contro un altro Stato si qualificherebbe come uso della forza.

Alla luce di quanto detto finora, il *Tallinn Manual*, dopo aver stabilito che un'operazione informatica è illecita quando costituisce una minaccia o un uso della forza contro l'integrità territoriale o l'indipendenza politica di qualsiasi Stato o quando è in qualsiasi altro modo contrario con i propositi delle Nazioni Unite[58], ha previsto che:

> *"A cyber operation constitutes a use of force when its scale and effects are comparable to non cyber operations rising to the level of a use of force".*
> (Un'operazione informatica costituisce uso della forza quando la sua portata e i suoi effetti sono comparabili con operazioni non informatiche che accrescono il livello dell'uso della forza).
>
> Rule 11, Tallinn Manual

Il Gruppo Internazionale di Esperti che ha redatto il Manuale ha trovato nella formula *portata e effetti* uno strumento utile per distinguere gli atti che si qualificano come uso della forza da quelli che invece non si qualificano come tali. In altre parole, prende in considerazione i fattori qualitativi e quantitativi da analizzare nel determinare se un'operazione informatica si qualifica come uso della forza. Secondo il Gruppo, la necessità di utilizzare un simile approccio deriva dal fatto che, nonostante le direttive fornite dalla *Corte Internazionale di Giustizia*, la soglia oltre la quale un'ingerenza costituisce un utilizzo della forza rimane poco chiara e definita. Sostanzialmente, tale approccio è diretto a identificare le

[58] Rule 10: *"A cyber operation that constitutes a threat or use of force against the territorial integrity or poltical indipendence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful"*.

operazioni informatiche che sono analoghe a quelle cinetiche o non cinetiche[59] che la comunità internazionale considera come uso della forza. Nella misura in cui alcune operazioni verrebbero considerate uso della forza, allo stesso modo lo sarebbero le operazioni informatiche con la stessa portata e gli stessi effetti. I fattori presi in considerazione sono[60]:

- ***Severity*** (Gravità del danno): le operazioni che provocano danni fisici a individui o a proprietà sono, secondo il Manuale, qualificate come atti di uso della forza. Quelle che generano meri inconvenienti o irritazioni, invece, non sono considerati tali. Tra i due estremi, più le conseguenze interferiscono con gli interessi critici nazionali, più contribuiscono a valutare le operazioni informatiche come uso della forza. A riguardo, lo scopo, la durata e l'intensità delle conseguenze hanno una grande importanza per la suddetta valutazione. Un'operazione informatica, come qualsiasi altra operazione, che provoca danno, distruzione, lesioni o morte è altamente probabile che venga considerata uso della forza, così come una operazione che danneggia il sistema informatico di una struttura sensibile come un impianto nucleare. La gravità in se è il fattore più significativo per l'analisi.
- ***Immediacy*** (Immediatezza): quando gli effetti si verificano nello spazio temporale di secondi o minuti (come quando esplode una bomba), l'operazione è probabilmente militare e quindi qualificabile come uso della forza; al contrario, se i suoi effetti si manifestano entro settimane o addirittura mesi, è più probabile che rientrino in attività diplomatiche o economiche.
- ***Directness*** (Connessione): se l'azione intrapresa è l'unica causa del risultato è più probabile che venga vista come un uso della forza. Quando il legame tra la cause e l'effetto si attenua, allo stesso modo si attenua la natura militare dell'operazione. Mentre il fattore *immediatezza* si focalizza sull'aspetto temporale delle conseguenze in questione, il fattore della *connessione* analizza il legame tra causa ed effetto. Per esempio, nel caso di una coercizione economica, la connessione causale tra l'atto iniziale e i suoi effetti tende ad essere indiretta. Nelle azioni armate, al contrario, la causa e gli effetti sono strettamente correlati. Un'esplosione, per esempio, danneggia direttamente le persone o gli oggetti. Le operazioni cibernetiche nelle quali la causa e

[59] Che prevedono, cioè, l'utilizzo di armi cinetiche o non cinetiche.
[60] Si deve specificare che questi sono meri fattori derivanti dall'interpretazione che gli Stati fanno nel valutare l'uso della forza e non formali criteri giuridici.

l'effetto sono chiaramente connessi è più probabile che vengano caratterizzati come uso della forza.

- ***Invasiveness*** (Invasività): dell'operazione nello Stato obiettivo. La violazione di un confine rimane ancora uno degli indicatori essenziali delle azioni militari. Generalmente le operazioni che vengono attivate al di fuori del territorio di uno Stato sono considerate probabilmente più diplomatiche o economiche, che altro. Tuttavia, nel caso specifico, tale regola soffre delle limitazioni: l'invasività si riferisce al grado con il quale le operazioni informatiche si introducono nello Stato di destinazione o nei suoi sistemi contrariamente agli interessi di detto Stato. Di norma, più sicuro è il sistema informatico di destinazione, maggiore è la percezione del grado di invasività. Per esempio, l'intrusione in un sistema militare che è stato accreditato di Livello 7 (EAL7) dei *Common Criteria*[61] è considerato più invasivo di una operazione che semplicemente sfrutta le vulnerabilità di un sistema non-accreditato e apertamente accessibile, come quello di una università pubblica o di piccole aziende. In più, quando gli effetti previsti da una operazione informatica sono limitati a uno Stato in particolare la percezione del grado di invasività di queste operazioni aumenta. Il nome del *dominio* è un indicatore che svolge una grande importanza nel valutare l'estensione dell'invasività di una operazione. Le operazioni informatiche che sono rivolte contro un dominio il cui nome è direttamente riconducibile a uno Stato (es. 'difesa.it') o di un particolare organo di uno Stato possono essere considerati più invasivi rispetto a operazioni dirette verso estensioni di dominio di Stati non specifici con nome *'.com'*.
- ***Measurability of effects*** (Misurabilità degli effetti): tradizionalmente, gli effetti delle operazioni delle forze armate che si qualificano come uso della forza sono generalmente misurabili (come nel caso delle valutazioni dei danni di una battaglia). Nel regno informatico, le conseguenze possono essere più o meno apparenti. Perciò, più una serie di conseguenze è qualificabile e identificabile, più sarà facile per uno Stato valutare la situazione nel determinare se l'operazione informatica in questione ha superato la soglia dell'uso della forza. Di conseguenza, se una operazione informatica può essere valutata in termini specifici (per es. quantità di dati danneggiati, percentuale di

[61] *Common Criteria for Information Technology Security Evaluation,* International Standard ISO/IEC *15408,* ver. 3.1, Revision 3 Final, July 2009, in http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3%20-%20marked%20changes.pdf.

server disabilitati, numero di dati rubati) è più probabile che venga caratterizzata come uso della forza.

- ***Military Character*** (Carattere militare): il nesso tra un operazione informatica e le operazioni militari aumenta la probabilità di caratterizzarla come uso della forza.
- ***State involvement*** (Coinvolgimento statale): più chiaro e vicino è il nesso tra lo Stato e le operazioni informatiche, più è probabile che gli altri Stati le caratterizzeranno come uso della forza da parte di detto Stato.
- ***Presumptive legality*** (Presunzione di legalità): il diritto internazionale è per natura proibitivo[62]. Gli atti che non sono vietati sono generalmente permessi; perciò, in assenza di un trattato o di una norma di diritto internazionale, un atto è presumibilmente legale. Per esempio, il diritto internazionale non vieta lo spionaggio o la semplice pressione economica. Perciò, le operazioni informatiche che ricadono dentro queste o altre categorie sono presumibilmente lecite.

Questi fattori non sono del tutto esaustivi. A seconda delle circostanze, infatti, gli Stati possono considerarne altri, come l'ambiente politico, se l'operazione protende verso un impiego futuro della forza militare, l'identità di chi attacca, la natura del bersaglio (strutture critiche), ecc. Inoltre, si sottolinea come i fattori operino in concerto tra di loro, anche se non devono necessariamente sussistere contemporaneamente.

Da rilevare è lo sforzo che il Gruppo di Tallinn ha compiuto nell'adattare e specificare i suddetti criteri alle caratteristiche delle operazioni informatiche (soprattutto nel caso dell'invasività), recependo l'indirizzo fornito dalla *Corte Internazionale di Giustizia* nel parere consultivo sulle armi nucleari[63], secondo il quale nell'applicazione delle norme della *Carta* Onu, nonché del diritto applicabile durante i conflitti armati, è essenziale prendere in considerazione le caratteristiche uniche delle armi nucleari. Così, il medesimo approccio è stato utilizzato riguardo alle operazioni informatiche.

Lo sforzo è considerevole, visto che le caratteristiche delle operazioni informatiche sono quasi sempre del tutto antitetiche ai fattori sopra esposti, rendendone quanto mai raro l'accostamento; quelle più complesse che rendono improbabile la qualificazione di un operazione informatica come uso o minaccia della forza sono[64]:

[62] V. *Lotus Case*, cit.
[63] *Nuclear weapons*, Advisory opinion, cit. para. 36.
[64] Heather Harrison Dinnis, cit., pp.65-74.

- **Indirectness** (ambiguità): ossia la quasi impossibilità sostanziale di stabilire con certezza chi sia il vero autore o mandante di un'operazione informatica. Nell'attacco contro l'Estonia nel 2007, sebbene sia stato perfino chiarito come fossero stati usati computer presenti all'interno del Cremlino, una successiva analisi ha stabilito che gli stessi, in realtà, erano stati compromessi da un gruppo di attivisti esterni. Pertanto, è particolarmente complicata l'attribuzione di responsabilità e il rischio di contromisure verso innocenti è elevato;
- **Intangibility** (intangibilità): il problema dell'intangibilità esiste su tre livelli:
  a) l'obiettivo dell'attacco non è tangibile; esso si sostanzia nella distruzione totale o parziale di informazioni o di sistemi di informazione, che collateralmente può causare danni nel mondo fisico;
  b) i mezzi utilizzati sono intangibili (come ad es. un codice binario) e perciò non associabili alla percezione classica di arma, il cui impiego, come visto, è essenziale nella definizione di un'azione come uso o minaccia della forza. Ma qualora dovessero direttamente causare danni fisici e lesioni umane dovrebbero essere considerati tali. Invero, tutte le perplessità nascono sulle capacità concrete di tali strumenti di causare danni fisici diretti a persone o cose, ma, visti i risultati raggiunti fino ad oggi e il continuo aumento della casistica, sicuramente sono potenzialmente riconducibili alla categoria delle armi.
  c) persino il tipo di danno causato può essere intangibile, anche se un attacco informatico che non agisce nella sfera fisica, può comunque causare danni collaterali sostanziali. Si pensi al crollo di un sistema economico che scateni il panico tra la popolazione.
- **Locus** (luogo): o per meglio dire il 'non luogo' di provenienza di un attacco informatico. E' particolarmente difficoltoso stabilire con un grado soddisfacente di certezza da dove si generi una determinata azione informatica. Nel caso dell'attacco *Solar Sunrise* del 1998, nel quale furono compromesse le reti di informazione del Dipartimento della Difesa degli Stati Uniti, esso sembrò provenire da diversi server sparsi in tutto il mondo. Anche se questo è un esempio di crimine informatico, fa ugualmente capire come la stessa cosa possa accadere nel caso di un attacco di uno Stato e la impossibilità di provare il suo coinvolgimento. Ciò anche alla luce del fatto che i sistemi militari, spesso, sono usati e integrati all'interno delle reti informatiche civili.
- **Result** (risultato): la cui natura è indeterminata, inaspettata e imprevedibile. Le armi tradizionali sono inconfutabilmente distruttive, contrariamente la capacità delle operazioni informatiche di causare meri

inconvenienti è sicuramente maggiore dell'incerta possibilità di causare veri e propri danni fisici, mettendo in tal modo in discussione il legame tra il loro utilizzo e una particolare tipologia di guerra: la *cyber war*, per l'appunto.

Nonostante l'intangibilità dell''arma' in questione, appare chiaro, dall'interpretazione degli strumenti legali, che ogni operazione informatica che direttamente o indirettamente dovesse causare conseguenze fisiche come la distruzione di proprietà o lesioni o perdita di vite sarebbe una violazione del divieto di utilizzare la forza contenuto nell'art. 2.4 della *Carta delle Nazioni Unite* e nel diritto internazionale consuetudinario. Quando, invece, gli effetti non si manifestano nella sfera fisica (ma colpiscono solo la sfera dell'informazione), oppure quando gli effetti fisici sono minimi o non legati all'operazione digitale da un nesso di causalità certo, la violazione non dovrebbe verificarsi.

Il fatto che un'operazione informatica, tuttavia, non assurga a violazione del divieto di uso della forza, non vuol dire che sia lecita. E' probabile che essa, infatti, possa costituire un'ingerenza negli affari interni ed esterni dello Stato.

V. La minaccia di un attacco informatico

L'art. 2.4 vieta, anche, la minaccia dell'uso della forza armata, per quanto sia talvolta difficile determinare quando ricorra tale situazione. Sul punto il *Tallinn Manual* recita:

> *"A cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force".*
> (Un'operazione informatica, o la minaccia di un'operazione informatica, costituisce una minaccia all'uso illecito della forza quando l'azione minacciata, se effettivamente messa in atto, costituirebbe un impiego illecito della forza).
>
> Rule 12, Tallinn Manual

La prima è un'operazione informatica che è usata per comunicare una minaccia di un impiego della forza. La seconda è una minaccia veicolata con qualsiasi mezzo (ad es. un annuncio pubblico) per mettere in atto operazioni informatiche che si qualificano come uso della forza[65]. In entrambi i casi è richiesto

[65] Infatti non si viola questa regola se le minacce degli Stati riguardano azioni lecite.

che la minaccia abbia natura comunicativa. Anche la *Corte Internazionale di Giustizia*, sempre nel caso Nicaragua, ha stabilito che vi è sicuramente minaccia nel caso di un ultimatum, mentre ha escluso che ricorra la minaccia di uso della forza nel caso in cui uno Stato metta a punto un notevole livello di armamenti, dato che nel diritto internazionale consuetudinario non esistono delle regole che impongono agli Stati sovrani dei limiti di armamento.

Allo stesso modo se uno Stato, in tensione con un altro, cominciasse aggressivamente a sviluppare la capacità di condurre operazioni informatiche dannose di massa, la semplice acquisizione di queste capacità, che potrebbero essere utilizzate in maniera forzosa, non costituirebbe una minaccia. Tuttavia, se il leader dello Stato in questione annunciasse che queste capacità saranno utilizzate per fini bellicosi e contro lo Stato antagonista, esso violerebbe di certo la regola in esame.

VI. Operazioni informatiche e autotutela

Deve essere chiaro che l'uso della forza, così come finora considerato, e l'attacco armato sono due cose distinte collegate a conseguenze normative diverse. L'uso della forza è impiegato per determinare se uno Stato ha violato l'articolo 2, comma 4 della *Carta delle Nazioni Unite* e la relativa proibizione del diritto internazionale consuetudinario. Al contrario, la nozione di 'attacco armato' consente allo Stato bersaglio di stabilire se può rispondere con l'uso della forza senza che esso stesso violi il divieto dell'art. 2.

La *Carta delle Nazioni Unite* ammette solo due eccezioni al divieto dell'uso della forza: le misure collettive autorizzate dal *Consiglio di Sicurezza* secondo il Capitolo VII e il diritto all'autotutela individuale e collettiva previsto dall'art. 51, cioè, alla legittima difesa intesa come risposta ad un attacco armato già sferrato.

La distinzione è critica poiché il semplice fatto che si sia verificato l'uso della forza da solo non giustifica l'uso della forza in risposta, poiché non ogni uso della forza è considerato un attacco armato. Di certo non lo sono gli atti che indirettamente violano l'art. 2, comma 4. Gli Stati che subiscono un uso della forza diverso da un attacco armato dovranno ricorrere ad altre misure se desiderano rispondere in maniera lecita, come ad. es. le contromisure[66].

[66] La contromisura, nel diritto internazionale, è la forma più importante di autotutela. E' prevista dall'art. 22 e dagli artt. dal 49 al 53 degli *Articoli sulla responsabilità dello Stato della Commissione di diritto internazionale*. Consiste in un comportamento dello Stato leso, che in sé sarebbe illecito, ma che diviene lecito in quanto costituisce una reazione ad un illecito altrui. In altri termini, lo Stato leso può, per reagire contro lo Stato offensore, violare a sua volta, ovviamente nei confronti di quest'ultimo, gli obblighi che derivano da norme consuetudinarie, da norme convenzionali e da norme contenuti in decisioni di organi internazionali, per reintegrare l'ordine giuridico violato. Essa

"A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State".
(Uno Stato leso da un atto internazionale illecito può ricorrere a contromisure proporzionate, incluse le contromisure informatiche, contro lo Stato responsabile).

Rule 9, Tallinn Manual

La singolare natura delle operazioni informatiche e la loro capacità di garantire l'anonimato, rendono fortemente appetibile il loro utilizzo come contromisure contro un precedente atto illecito internazionale, anche di altro genere. Inoltre, il loro utilizzo risulta particolarmente adeguato anche in caso di risposta contro un attacco informatico riconducibile ad attori non statali.

Secondo gli Esperti di Tallinn, alcune misure protettive informatiche possono essere giustificate, anche, sulla base dello *stato di necessità*[67]. Esso, a differenza delle contromisure, non dipende dal precedente comportamento illecito di un altro Stato. Per esempio, se uno Stato si trova di fronte a un attacco informatico che potrebbe danneggiare i suoi interessi essenziali e non ci fosse altro modo per contrastare la situazione, esso potrebbe temporaneamente

---

dovrebbe consistere in una azione che, nella misura del possibile, ha effetti temporanei e reversibili. La contromisura incontra vari limiti, tra cui la proporzionalità della violazione subita e la violazione commessa per rappresaglia (art. 51). Non si tratta di una perfetta corrispondenza tra le due violazioni, come è dimostrato dal fatto che normalmente contro l'inosservanza di un obbligo si può reagire con la violazione di un obbligo del tutto diverso. Si dice pertanto che più che la proporzionalità il diritto internazionale richiede che non vi sia una eccessiva sproporzione tra le due violazioni. E' chiaro che, se sproporzione c'è, la contromisura diviene illecita per la parte eccedente; è chiaro pure che, se si vuole esser certi che la reazione non sia sproporzionata, la strada più praticabile è quella di farla consistere nella violazione del medesimo obbligo violato. Un altro limite è quello dell'impossibilità di ricorrere a violazioni del diritto internazionale cogente, anche nel caso in cui si tratta di reagire a violazioni dello stesso tipo (art. 50, n.1, lett. a-d). Altri limiti sono il rispetto dei principi umanitari e il limite del previo esaurimento dei mezzi di soluzione delle controversie (art. 52, n.1). Infine non possono essere prese contromisure e, se già prese, devono essere sospese senza indebito ritardo, se: a) l'atto internazionalmente illecito è cessato; e se b) la controversia pende innanzi ad una corte o ad un tribunale che abbia il potete di adottare decisioni vincolanti per le parti (art. 52, n.3). Per approfondire v. Conforti Benedetto, *Diritto Internazionale*, pp. 347-350.

[67] Articolo 25 degli Articoli sulla responsabilità dello Stato: "*Stato di necessità"*
1. Lo Stato non può invocare lo stato di necessità come causa di esclusione dell'illiceità di un atto non conforme ad uno dei suoi obblighi internazionali se non quando tale atto: a) costituisca per lo Stato l'unico mezzo per proteggere un interesse essenziale contro un pericolo grave ed imminente; e b) non leda gravemente un interesse essenziale dello Stato o degli Stati nei confronti dei quali l'obbligo sussiste, oppure della comunità internazionale nel suo complesso.
2. In ogni caso, lo stato di necessità non può essere invocato da uno Stato come motivo di esclusione dell'illiceità se: a) l'obbligo internazionale in questione esclude la possibilità di invocare lo stato di necessità; o b) lo Stato ha contribuito al verificarsi della situazione di necessità.

inabilitare certe infrastrutture informatiche, anche se nel fare ciò danneggiasse sistemi informatici di Stati terzi. Allo stesso modo, se affrontasse operazioni informatiche potenzialmente dannose rivolte contro una struttura critica dello Stato, lo stato di necessità potrebbe giustificare il ricorso a operazioni cibernetiche di contrasto (*counter-hacking*). Tuttavia, come ha espresso la Commissione di diritto internazionale, il ricorso a un'azione selezionata deve essere l'*"unico modo"* disponibile per salvaguardare l'interesse in questione e ad ogni modo non deve seriamente pregiudicare gli interessi essenziali degli altri Stati o della comunità internazionale nel suo complesso[68].

Un utilizzo oculato e responsabile dei criteri elencati nei paragrafi precedenti da parte degli Stati, pertanto, è fondamentale per stabilire la portata, gli effetti e le conseguenze derivanti da una qualsiasi operazione informatica, la cui diversa natura è individuabile all'interno della seguente tripartizione:

- operazione informatica non implicante l'uso o la minaccia della forza ⟶ contromisure + stato di necessità;
- operazione informatica implicante l'uso o la minaccia della forza ex. art. 2.4 ⟶ contromisure + Capitolo VII *Carta delle Nazioni Unite*;
- operazione informatica che equivale ad un attacco armato ⟶ art. 51 + Capitolo VII *Carta delle Nazioni Unite*.

L'ultima categoria è sicuramente la più problematica. Secondo il *Tallinn Manual*:

> *"A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self defence. Whether a cyber operation constitutes an armed attcack depends on its scale and effects".*
> (Uno Stato che è vittima di una operazione informatica che si qualifica fino al livello di un attacco armato può esercitare il suo diritto naturale di autotutela. Se l'operazione cibernetica costituisce un attacco armato dipende dalla sua portata e dai suoi effetti).
>
> Rule 13, Tallinn Manual

Questa regola richiama ovviamente la *Carta delle Nazioni Unite*:

[68] Per una visione critica dello Stato di Necessità, quale circostanza che esclude l'illiceità dell'uso della forza, cfr. Conforti Benedetto, *Diritto Internazionale*, pp. 330-331.

"Nessuna disposizione del presente Statuto pregiudica il diritto naturale di autotutela individuale o collettiva, nel caso che abbia luogo un attacco armato contro un Membro delle Nazioni Unite, fintantoché il Consiglio di Sicurezza non abbia preso le misure necessarie per mantenere la pace e la sicurezza internazionale…".

Art. 51, Carta delle Nazioni Unite

Il principio che vieta il ricorso alla forza trova pertanto un limite generale nella legittima difesa contro un attacco armato. La *Corte Internazionale di Giustizia* nel caso *Nicaragua*[69] e nel caso *Piattaforme petrolifere*[70], dopo aver stabilito che l'autotutela non può consistere nella minaccia o nell'uso della forza, ha fatto propria l'eccezione dell'art. 51, specificando come essa sia corrispondente al diritto internazionale consuetudinario.

L'applicazione dell'art. 51, così come contestualizzato dalla Rule 13 del Tallinn Manual al regno informatico, incontra, però, una enorme difficoltà nello stabilire quando il livello dell'uso della forza condotto attraverso delle operazioni informatiche sia tale da far valere il diritto all'autodifesa individuale o collettiva di cui all'art. 51. Ove ciò dovesse accadere ci troveremmo di fronte ad un attacco armato.

Ma cos'è un attacco armato? La *Carta delle Nazioni Unite* non fornisce una definizione precisa.

Certamente è un atto illecito internazionale[71] dal carattere *transfrontaliero*, ossia rivolto da uno Stato contro un altro Stato, oppure da attori non-statali verso uno Stato, che si trovino fuori dal suo territorio[72].

Una panoramica giurisprudenziale della *Corte Internazionale di Giustizia* fornisce qualche dato in più: esso implica necessariamente l'utilizzo di un'arma, indipendentemente da quale essa sia[73]. La nozione di arma deve essere intesa in maniera estensiva, ricomprendendo non solo quelle tradizionali cinetiche, biologiche, chimiche o nucleari, ma anche qualsiasi altro dispositivo capace di causare distruzioni, lesioni o morte.

Inoltre, la Corte ha specificato che l'attacco o aggressione si ha non solo quando ad attaccare sono forze regolari ma, anche, quando, con effetti equivalenti, lo Stato agisce per mano di bande irregolari o di mercenari da esso

[69] *Nicaragua Case*, cit. para.187 ss.
[70] *Oil Platforms (Islamic Republic of Iran v. United States of America),* Judgment, I. C. J. Reports 2003, p. 161, para. 43 e ss. e 65 e ss.
[71] Sulla nozione di illecito internazionale v. Conforti Benedetto, *Diritto Internazionale*, da pp. 321-335.
[72] *Tallinn Manual*, cit., p. 54.
[73] *Legality of the threat or use of nuclear weapons*, cit., para. 39.

assoldati[74]. Ha affermato che non costituisce aggressione armata la sola assistenza data a forze ribelli che agiscono sul territorio di uno Stato, sotto forma di fornitura di armi, di assistenza logistica e simili; siffatta assistenza costituirebbe soltanto un'ipotesi di violazione del divieto di ingerirsi negli affari interni e al contempo un'ipotesi di violazione meno grave del divieto della minaccia o dell'uso della forza, come tali non giustificanti una risposta armata[75]. Infine ha stabilito che la definizione di *attacco armato* dipende dalla portata e dagli effetti (*scale and effects*) dell'uso della forza, distinguendo tra "forme meno gravi" e "forme più gravi" di uso della forza e che queste ultime devono essere di una gravità tale da elevarsi oltre la definizione di meri incidenti di frontiera (*mere frontier incidents*)[76].

La Corte, in tal modo, ha reso effettivi alcuni parametri presenti negli artt. 2 e 3 della Dichiarazione dell'Assemblea Generale delle Nazioni Unite sulla Definizione di Aggressione[77]:

[74] Così se un gruppo di individui privati sotto la direzione di uno Stato effettua operazioni informatiche dirette contro un altro Stato, e la conseguenza di queste azioni raggiunge la proporzione e gli effetti sufficienti, il primo commette un attacco armato. La stessa conclusione si applica alle operazioni informatiche condotte da un singolo individuo sotto la direzione di uno Stato.

[75] *Legality of the threat or use of nuclear weapons*, cit., para. 195 – 231.

[76] Ibid., para. 195.

[77] Ricordiamo che le Dichiarazioni secondo la Carta delle Nazioni Unite hanno valore di mera raccomandazione e pertanto non sono vincolanti.

"Any of the following acts, regardless of a declaration of war, shall, subject to and in accordance with the provision of article 2, qualify as an act of aggression: a) the invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof; b) Bombardment by the armed forces of a State against the territory of another State or the use of any weapon by a State against the territory of another State; c) The blockade of ports or coasts of a State by the armed forces of another State; d) An attack by armed forces of a State on the land, sea or air forces, or marine and air fleets of another State; e)The use of armed forces of one State which are within the territory of another State with the agreement of the receiving State, in contravention of the condition provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement; f) The action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State; g) The sending by no behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to the acts listed above, or in substantial involvement therein".

Art. 3, Dichiarazione dell'Assemblea Generale delle Nazioni Unite n. 3314 – XXIX del 14/12/1974

La *gravità sufficiente* delle conseguenze dell'uso della forza è, anche, il criterio attraverso il quale il Consiglio di Sicurezza, coerentemente con il compito assegnatogli dal Capitolo VII della Carta, determina quando le azioni ricadono o meno negli esempi dell'art. 3:

"The first use of armed force by a State in contravention of the Charter shall constitute prima facie evidence of an act of aggression although the Security Council may, in conformity with the Charter, conclude that a determination that an act of aggression has been committed would not be justified in the light of other relevant circumstances, including the fact that the acts concerned or their consequences are not sufficient gravity".

Art. 3, Dichiarazione dell'Assemblea Generale delle Nazioni Unite n. 3314 – XXIX del 14/12/1974

Parte della dottrina, però, per distinguere, tra forme meno gravi di uso della forza e attacco armato nel regime cibernetico richiede da parte dell'autore, anche, l'intento specifico di violare la sovranità territoriale di un altro Stato[78]. C'è chi suggerisce di prendere in considerazione l'obiettivo dell'attacco, e cioè le c.d.*"critical infrastructures"*[79], la protezione delle quali è sempre stata una delle preoccupazioni maggiori della cyber security nazionali[80]. Secondo l'*Assemblea Generale dell'Onu* tale nozione include: *"those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health – and the critical information infrastructures that increasingly interconnect and affect their operations"*[81]. Tali autori affermano che una operazione informatica che colpisce questi obiettivi all'interno della sfera di sovranità di un altro Stato, è da considerarsi un attacco armato anche se non causa morte, lesioni o distruzione.

Il Gruppo del Tallinn Manual, invece, ha preferito concentrarsi esclusivamente sulla proporzione e sugli effetti dell'attacco: l'unico intento da considerare sarebbe quello di causare danni fisici ad oggetti o ad essere umani, pertanto l'autotutela sarebbe limitata solo contro operazioni che sono *de facto* attacchi armati contro una qualsiasi struttura di uno Stato.

In definitiva, sebbene la *Corte Internazionale di Giustizia* abbia affermato che ad oggi esiste un'opinione condivisa sulla natura degli atti che sono considerati un attacco armato[82], cosa sia in realtà quest'ultimo non è ancora chiaro.

Nel caso *Piattaforme petrolifere*, ha stabilito che è compito dello Stato che utilizza la forza per legittima difesa provare che è stato vittima di un attacco armato[83], legittimando una certa discrezionalità decisionale conseguente all'incertezza internazionale.

La valutazione non è semplice di per sé e, in questa sede, una serie motivi la rendono ancora più ardua. Il primo è che anche i più catastrofici attacchi finora

[78] Cfr. Melzer Nils, *Cyberwarfare and International Law*, cit., p. 16; Si veda anche Sharp Walter G., *Cyberspace and the Use of Force*, Aegis Research Corp., Falls Church, Virginia, 1999, p. 129, in http://www.thomas-hastings.org/CyberSpace%20and%20the%20Use%20of%20Force%20%20Sharp1999.pdf ;

[79] Per approfondimenti si veda Roscini Marco, *World Wide Warefare – Jus ad bellum and the Use of Cyber Force*, in Armin Bogdany and Rudiger Wolfrum (eds), Max Planck Yearbook of United Nations Law, vol. 14, 2010, p. 96; Melzer Nils, *Cyberwarfare and International Law*, cit., p. 14.

[80] Si veda per esempio, la Risoluione dell'Assemblea Generale dell'Onu n. 58/199 del 30 gennaio 2004, intitolata *"Creation of a global culture of a cybersecurity and the protection of critical information infrastructure"*, in http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/58/199&Lang=E.

[81] Ibid., p. 1; per altre definizioni di *critical infrastructures* si veda Melzer Nils, cit., p. 15.

[82] *Nicaragua Case,* cit. para. 195.

[83] *Oil Platform Case*, para. 57.

condotti attraverso le operazioni informatiche non sono stati in grado di causare da soli quei danni necessari affinché si verifichi la violazione del divieto di utilizzare la forza (distruzione, lesione, perdita di vite, ecc.). E' dunque legittimo chiedersi se hanno addirittura la capacità di costituire un attacco armato (sempre che tali attacchi non vengano usati in concomitanza ad attacchi convenzionali). Un secondo motivo si concretizza nella difficoltà di attribuire l'attacco all'autore originario, per non parlare poi del tempo necessario per effettuare un attacco armato con strumenti informatici. Quest'ultimo aspetto, in particolare, rende difficile soddisfare il requisito dell'attualità o dell'imminenza[84] dell'attacco armato, indispensabile affinché sorga il diritto all'autodifesa. Tale requisito è ricavabile in via interpretativa dall'art. 51 della Carta delle Nazioni Unite dove afferma *"nel caso in cui abbia luogo un attacco armato"*.

Siamo realmente nel campo della pura speculazione ipotetica: ad esempio un attacco informatico che mette fuori uso o manometta un impianto di depurazione dell'acqua, causando morti estese per avvelenamento, oppure che colpisce infrastrutture critiche come le dighe e gli oleodotti, causando danni devastanti. Tuttavia, a prescindere dagli esempi che possono essere immaginati, la regola dovrebbe essere la seguente: quando uno Stato è vittima di un attacco informatico *transfrontaliero* che causa un danno alla proprietà o alle persone e la cui proporzione ed effetti siano tali da essere paragonati ad un attacco armato convenzionale, può sicuramente agire in autotutela attraverso l'uso della forza.

Non è richiesto che la forza in difesa debba essere della stessa natura di quella che ha costituito l'attacco armato. Perciò, un uso informatico della forza può essere utilizzato in risposta ad attacchi armati convenzionali e viceversa, purché sia necessario, proporzionato ed immediato[85].

- La **Necessità** richiede che l'uso della forza, compreso il caso delle operazioni informatiche, sia l'unica risposta possibile per respingere efficacemente un attacco in corso. Ciò non significa che la forza debba essere necessariamente l'unica risposta a un attacco armato. Essa richiede solo che le misure non forzose siano insufficienti per affrontare la situazione. Certamente, le azioni che implicano l'uso della forza possono essere combinate con misure che non la prevedono, come le misure diplomatiche o le sanzioni economiche. La chiave per l'analisi della necessità nel contesto informatico è, perciò, l'esistenza o la mancanza di azioni alternative a quelle che raggiungono il livello di uso della forza. Così se le difese informatiche passive come i firewall

[84] *Rules 15* del *Tallinn Manual*.
[85] *Rules 14* e *15* del *Tallinn Manual*.

(distinte da quelle attive) dovessero essere adeguate per contrastare in modo affidabile e completo un attacco armato informatico, le altre misure, sia informatiche sia convenzionali, a livello dell'uso della forza non sarebbero permesse. Ugualmente, se operazioni informatiche attive che non raggiungono il livello dell'uso della forza sono adeguate per scoraggiare o respingere attacchi armati (imminenti o in atto), attività informatiche forzose o alternative convenzionali sarebbero escluse dal criterio della necessità. Tuttavia, quando le misure che non implicano l'uso della forza non possono da sole ragionevolmente presumere di sconfiggere un attacco armato e di prevenire quelli successivi, operazioni informatiche o convenzionali al livello dell'uso della forza sono permesse secondo il diritto dell'autotutela. La Necessità è giudicata secondo la prospettiva dello Stato vittima, la cui determinazione deve essere ragionevole a seconda delle circostanze.

- La **proporzionalità** affronta il problema di quanta forza, inclusa l'uso della forza informatica, è permessa una volta che l'uso della forza è ritenuto necessario. Il criterio della proporzionalità limita la quantità, le modalità e i mezzi, il fine, la durata e l'intensità della risposta rispetto a quella richiesta e necessaria per porre fine alla situazione che ha dato origine al diritto di agire in autotutela. La limitazione della quantità della forza usata non viene effettuata rispetto a quella utilizzata nell'attacco armato in quanto il livello della forza necessaria per eseguire con successo una difesa dipende dal contesto; più forza può essere necessaria, o meno forza può essere sufficiente, per respingere un attacco o sconfiggerne uno imminente. Secondo tale principio non può essere negato in assoluto l'utilizzo di armi convenzionali in risposta ad un attacco informatico.
- L'**immediatezza** si riferisce al periodo seguente l'esecuzione o l'inizio dell'attacco armato entro cui lo Stato vittima può ragionevolmente rispondere in autotutela. Essa considera fattori come la prossimità temporale tra l'attacco e la risposta, il periodo necessario per identificare l'attacco e il tempo richiesto per preparare la risposta. Particolarmente complesso è il caso di un attacco armato eseguito con una serie di operazioni informatiche. La situazione di autotutela in questo non si conclude necessariamente con l'interruzione delle operazioni informatiche. Infatti, se fosse ragionevole pensare che esse sono propense a riprendere o continuare, lo Stato vittima potrebbe trattare queste operazioni come parte di un attacco più esteso e continuare ad agire in autotutela. Tuttavia, se questa conclusione non fosse ragionevole, qualsiasi uso ulteriore della forza, sia convenzionale sia

informatico, rischierebbe di risultare illecito. Ciò detto, il requisito dell'immediatezza si riduce a una valutazione di ragionevolezza alla luce delle circostanze che prevalgono sul momento. Un altro problema consiste nel fatto che un attacco informatico che si è già verificato o si sta verificando può non essere evidente per un periodo di tempo. Ciò può accadere quando il danno o la lesione e/o le loro cause non sono stati identificati. Ugualmente, può accadere che l'autore dell'attacco non venga identificato se non dopo la fine dell'attacco. Il classico esempio di entrambe le situazioni è lo sviluppo di un *worm* come Stuxnet. In questi casi, il criterio dell'immediatezza non dovrebbe essere soddisfatto e pertanto non si dovrebbe generare il diritto all'autotutela.

I requisiti di necessità e proporzionalità sono stati riconosciuti dalla *Corte Internazionale di Giustizia* nel caso *Nicaragua* e nel caso delle *Piattaforme petrolifere*[86], mentre il requisito dell'immediatezza è insito nella definizione di autotutela come *risposta* o *reazione necessaria* ad un attacco armato.

Quanto detto in questo paragrafo vale *mutatis mutandis* per l'autotutela collettiva[87], che può essere esercitata su richiesta dello Stato vittima o in base a un trattato o un accordo *ad hoc*, nonché per l'autotutela intrapresa contro attori non-statali (v. IX. Attori non-statali transnazionali).

VII. Autotutela anticipatoria e preventiva

Mentre è altamente improbabile che ad oggi operazioni informatiche siano in grado da sole di realizzare un attacco armato, è invece molto più realistica l'ipotesi che esse vengano usate prima o in concomitanza di attacchi armati convenzionali. Per esempio, nel 2007, prima dell'attacco israeliano sulla Siria, sospettata di ospitare siti nucleari, il sistema difensivo aereo dei radar è stato messo fuori uso; oppure nel 2008, un attacco massiccio di DDoS (*distributed denial of service*) aveva anticipato l'invasione fisica della Russia in Georgia.

Questa ipotesi giustificherebbe la legittimità dell'uso della forza, secondo la dottrina dell'autotutela anticipatoria.

L'art. 51 della *Carta delle Nazioni Unite* non prevede espressamente la possibilità di agire in legittima difesa in via anticipatoria nel caso di un attacco

[86] Rispettivamente in para. 176, 194 e in para. 43, 73-74, 76.
[87] *Rule n. 16* del *Tallinn Manual*.

imminente, ma soltanto *"nel caso in cui abbia luogo un attacco armato"*, richiedendo pertanto l'attualità dello stesso.

In realtà questa interpretazione restrittiva e letterale non coincide con il diritto naturale di autotutela così come previsto dal diritto internazionale consuetudinario. La *Corte Internazionale di Giustizia*, infatti, ha riconosciuto che la previsione dell'art. 51 non contiene tutte le regole pertinenti all'autotutela, tra cui la definizione di attacco armato o i requisiti di necessità e proporzionalità[88] (tuttavia non si è espressamente pronunciata sulla legittimità dell'autotutela anticipatoria in caso di attacco armato imminente non essendo richiesto dalle circostanze del caso).

L'autotutela anticipatoria è riconosciuta a tutti gli effetti nella prassi degli Stati, come sottolinea il Tallinn Manual: *"non è necessario che uno Stato attenda pigramente che il nemico inizi ad attaccare. Al contrario, esso può difendersi una volta che l'attacco sia imminente"*[89]. Questa posizione si basa sullo standard di imminenza articolato nel diciannovesimo secolo dal Segretario di Stato degli Stati Uniti Daniel Webster a seguito dell'incidente *Caroline*. Egli ha rilevato che il diritto in questione nasce solo quando *"la necessità dell'autodifesa è immediata, travolgente, che non lascia scelta di mezzi, e nessun momento per la riflessione"*[90]. Anche se l'incidente in realtà non aveva nulla a che fare con le azioni prese in anticipazione dell'attacco (gli attacchi di questo episodio, infatti, erano in corso), la formulazione di Webster è sopravvissuta come la classica espressione della soglia temporale delle azioni difensive anticipatorie.

Nel valutare i casi di autotutela anticipatoria, il Gruppo sottolinea la necessità di distinguere tra azioni preparatorie e quelle che costituiscono una fase iniziale dell'attacco: *"…se l'attore, infatti, sta semplicemente acquisendo la capacità di avviare un attacco armato in futuro, il criterio dell'imminenza non è soddisfatto. Tuttavia, se vi sono informazioni tali da presumere ragionevolmente che l'attore abbia attualmente deciso di condurre un attacco armato usando ad es. un malware, l'attacco è considerato imminente al punto tale che lo Stato vittima deve agire per non perdere l'opportunità di difendersi. Certamente, è difficile effettuare una distinzione nella pratica. In ogni caso, la legittimità di qualsiasi risposta difensiva sarà determinata dalla ragionevole valutazione della situazione da parte dello Stato vittima"*.

[88] *Nicaragua Case*, cit., para. 176.
[89] *Tallinn Manual*, cit., *Rule 15*, para. 2, p. 60.
[90] Formula Webster: *"a necessity of self-defence instant, overwhelming, leaving no choice on means and no moment for deliberation"*.

Secondo Heather Harrison Dinnis[91], nel caso di attacchi informatici possono essere individuate due situazioni nelle quali vale il diritto all'autotutela anticipatoria:

- quando un'operazione informatica prelude la minaccia di un attacco armato di tipo convenzionale;
- quando attività informatiche indicano che un attacco informatico più grave (pari ad un attacco armato) è imminente.

L'autrice spiega che per stabilire se sorge il diritto all'autotutela anticipatoria nel primo caso è l'obiettivo dell'attacco che deve essere preso in considerazione: se prende di mira sistemi di allarme, postazioni radar o satellitari, comunicazioni militari o sistemi di emergenza è altamente probabile che uno Stato giudichi imminente un attacco convenzionale (caso siriano). Al contrario la distruzione o la manomissione di sistemi finanziari o mediatici non è di per sé un'indicazione sufficiente per presumere un successivo e imminente attacco convenzionale (caso estone). Tuttavia quando attacchi di questo genere sono valutati insieme ad altri indicatori contestuali, gli Stati possono ragionevolmente concludere che un attacco convenzionale è imminente (ciò sarebbe potuto accadere nel conflitto tra la Russia e la Georgia del 2008, caratterizzato da un'atmosfera di crescente tensione fra gli Stati. Tuttavia, in questo caso, non è stato possibile individuare nessuna connessione evidente tra il governo russo e gli attacchi informatici che hanno colpito la Georgia).

Nel secondo caso, invece, nonostante le potenzialità devastanti degli attacchi informatici e visto che ad oggi non è stato lanciato nessun attacco paragonabile a quelli delle armi cinetiche, nucleari, biologiche o chimiche, il diritto all'autotutela anticipatoria non dovrebbe sussistere.

Un'altra estensione della legittima difesa ad ipotesi non espressamente previste dall'art. 51 della *Carta delle Nazioni Unite* è stata effettuata per legittimare l'uso della forza in via *preventiva* o per giustificare le reazioni contro Stati che alimentano il terrorismo (v. ad es. i bombardamenti della Libia e dell'Iraq ad opera degli Stati Uniti rispettivamente nel 1986 e nel 1993, la guerra della coalizione di Stati facente capo agli Stati Uniti contro l'Afghanistan, diretta a distruggere le basi dell'organizzazione terroristica Al Qaeda o la guerra contro l'Iraq giustificata dagli Usa e dal Regno Unito con la necessità di distruggere armi di distruzione di massa poi rivelatesi inesistenti). La dottrina della legittima difesa preventiva è contenuta nel documento intitolato *"La strategia per la sicurezza nazionale degli Stati Uniti"*

[91] In *Cyber Warefare and the Laws of War*, cit., p. 88.

(c.d. dottrina Bush), presentata dal Presidente degli Stati Uniti al Congresso per la prima volta nel settembre 2002 e riconfermata nel 2006[92]. Secondo tale documento, la legittima difesa preventiva verrà esercitata dagli Stati Uniti ogni qualvolta ciò si rendesse necessario per prevenire un'imminente minaccia o un imminente attacco con armi di distruzione di massa o atti di terrorismo.

Nonostante questa dottrina non abbia nessun fondamento giuridico, né nel diritto consuetudinario, né a livello pattizio, neanche *La Strategia per la sicurezza nazionale degli Stati Uniti* dell'amministrazione Obama l'ha respinta completamente, affermando semplicemente che gli Stati devono rispettare gli standard che governano l'uso della forza, senza però specificare quali siano tali standard[93].

Anche questa dottrina è presa in considerazione dal *Tallinn Manual* nella parte in cui afferma che: *"il fatto che uno Stato apertamente ostile è capace di lanciare attacchi informatici, anche quelli devastanti, non autorizza da solo un potenziale Stato vittima di agire in difesa con la forza. Il potenziale Stato Vittima deve prima ragionevolmente concludere che l'ostilità sta maturando in una decisione attuale di attaccare. Finché esso non sia arrivato a questa conclusione, la risposta dello Stato vittima dovrebbe essere limitata a misure non forzose e al rinvio della questione al Consiglio di Sicurezza. Certamente, anche se uno Stato ha l'intento e l'opportunità di condurre un attacco armato contro un altro Stato, il diritto del presunto Stato vittima di prendere misure difensive pari al livello dell'uso della forza non matura finché il momento di agire priverebbe la vittima della possibilità di difendersi effettivamente una volta cominciato l'attacco"*[94].

Un esempio di autotutela preventiva nel campo della sicurezza informatica potrebbe essere quello di uno Stato A che agisce in autotutela contro uno Stato B, dotatosi di infrastrutture informatiche superiori alle proprie, per il timore di non essere capace di difendersi da un eventuale attacco informatico.

Tale impostazione non dovrebbe essere condivisa non solo perché, come detto, la guerra preventiva non ha alcun fondamento giuridico né a livello pattizio né a livello consuetudinario, ma soprattutto perché la prevenzione, tramite l'uso della forza, di operazioni informatiche che costituirebbero, secondo la valutazione di uno Stato, il preludio ad un'imminente minaccia o ad un imminente uso della forza al livello di un attacco armato convenzionale o informatico, costituirebbe sicuramente una forzatura delle relazioni internazionali.

[92] *The National Security Strategy of the United States of America*, White House, 2002, 15 e *The National Security Strategy of the United States of America*, White House, 2006, p. 23.
[93] *The National Security Strategy of the United States of America*, White House, 2010.
[94] Si veda *Tallinn Manual*, cit., *Rule 15*, para. 7, p. 62.

VIII. Serie di eventi tenui

La realtà delle operazioni informatiche ha anche evidenziato come sia prevedibile effettuare una serie multipla di attacchi meno gravi, piuttosto che singole operazioni pari a un attacco armato.

Un'analogia si può ritrovare con le incursioni oltre confine. In questo caso, gli Stati hanno rivendicato il diritto di agire in autotutela contro una serie di attacchi meno gravi che collettivamente raggiungono il livello di un singolo attacco armato. Si tratta della c.d. *pinprick* (lett. puntura di spillo) o *accumulation of events theory*. La *Corte Internazionale di Giustizia*, nel caso *Nicaragua*, commentando le incursioni del Nicaragua nel territorio dell'Honduras e del Costa Rica, ha affermato che in questo caso c'erano poche informazioni per stabilire se tali incursioni potessero essere considerato un attacco armato[95], lasciando così intendere che una circostanza del genere possa avvenire. Questa posizione è stata reiterata anche in casi successivi, quali quello delle *Piattaforme petrolifere* e delle *Attività armate*. In questi casi la Corte, abbracciando il concetto degli attacchi cumulativi come attacco armato, ha però stabilito che non vi fossero elementi sufficienti per giungere a tale conclusione.

Così allo stesso modo, dei loro equivalenti convenzionali, le operazioni informatiche cumulative potrebbero raggiungere il livello di un attacco armato e legittimare pertanto la legittima difesa, ma ciò è altamente improbabile che si verifichi.

Inoltre, va distinto il caso degli attacchi cumulativi dal caso di un attacco effettuato da una molteplicità di computer. Così, un attacco tipo DDoS, nonostante sia perpetuato con l'ausilio di un ampio numero di computer dislocati in diversi luoghi, deve essere considerato come un singolo attacco armato, poiché comunque viene generato e controllato da una singola entità (*botmaster*) che dirige i *botnet*. Tale caso è l'equivalente di un attacco terrestre che utilizzi più di un soldato o di un attacco aereo che veda l'impiego di una serie di bombe.

IX. Attori non-statali transnazionali

Ormai è certo dalla prassi che operazioni informatiche transnazionali che non raggiungono il livello di un attacco armato, riconducibili ad attori non-statali che agiscono senza la direzione di uno Stato (per es. organizzazioni terroristiche, gruppi organizzati di attivisti), possano essere contrastate con proporzionate contromisure. Meno chiaro è se le operazioni dei medesimi soggetti che

[95] *Nicaragua Case*, cit., para.231.

raggiungono il livello di forza sufficiente da costituire un attacco armato, possano far valere il diritto al ricorso dell'uso della forza in legittima difesa contro di essi.

Tradizionalmente, l'articolo 51 della *Carta delle Nazioni Unite* e il diritto internazionale consuetudinario sono stati caratterizzati dalla loro applicazione unicamente nel caso di attacchi armati intrapresi da uno Stato contro un altro Stato.

Anche la dottrina più eminente, fino ai tempi più recenti, è stata generalmente orientata nel considerare solo gli Stati quali possibili fonti di un attacco armato[96].

Tuttavia, la comunità internazionale ha caratterizzato gli attacchi di Al Qaeda dell'11/09/2001 contro gli Stati Uniti come un attacco armato vero e proprio innescando il diritto naturale di legittima difesa:

> *"Il Consiglio di Sicurezza…determinato a combattere con tutti i mezzi le minacce alla pace e alla sicurezza internazionale causate dagli atti terroristici, riconoscendo il diritto intrinseco all'autodifesa individuale o collettiva in accordo con la Carta, condanna inequivocabilmente nei termini più forti possibili i raccapriccianti attacchi terroristici che hanno avuto luogo l'11 settembre 2001 a New York, Washington, D.C. e in Pennsylvania e considera tali atti, come qualsiasi atto di terrorismo internazionale, una minaccia alla pace e alla sicurezza internazionali".*
>
> Risoluzione del Consiglio di Sicurezza n. 1368, 12 settembre 2001.

Tale evento sembra segnalare la volontà degli Stati di applicare il diritto di legittima difesa agli attacchi condotti da attori non-statali. Inoltre, mentre l'articolo 2.4 si applica alle azioni degli *"Stati membri"*, l'articolo 51 non menziona da chi l'attacco armato debba provenire (anche se il testo sottolinea chiaramente che solo gli Stati godono del diritto di legittima difesa).

Questo è uno dei tanti casi in cui la pratica degli Stati nel diritto internazionale è andata oltre le previsioni dello stesso, confermando la sua natura principalmente consuetudinaria. Infatti, non è previsto esplicitamente il diritto di uno Stato di rispondere con la forza contro un attacco armato condotto da attori non-statali che agiscono senza la direzione o la complicità di un altro Stato.

Inoltre, la *Corte Internazionale di Giustizia* non ha mai chiarito la questione della liceità e delle modalità con le quali tale autotutela debba avvenire, né se un livello minimo di coinvolgimento di uno Stato debba o meno sussistere, né quale debba essere il livello di organizzazione del gruppo.

[96] Uno su tutti, Antonio Cassese, *The International Community's 'Legal' Response to Terrorism*¸ 38 INT'L & COMP. L. Q., 1989, pp. 589 – 597.

In ogni caso, data per buona questa possibilità, il Gruppo di Tallinn ha evidenziato che quando operazioni informatiche pari ad un attacco armato sono generate da attori non-statali all'interno del territorio di uno Stato a cui l'attacco non può essere attribuito, è indispensabile salvaguardare il principio di sovranità. E' indiscutibile che azioni di legittima difesa possono essere intraprese in territorio estero qualora vi sia il consenso di quello Stato, senza violare, così, la sua sovranità. Pertanto, la questione chiave per quanto riguarda l'azione difensiva sul territorio di un altro Stato è come caratterizzare le azioni non consensuali: il gruppo internazionale di esperti si è diviso. La maggior parte ha concluso che l'autodifesa contro un cyber attacco armato è ammessa quando lo Stato territoriale non è in grado (perché manca la competenza o la tecnologia) o non voglia intraprendere azioni efficaci per reprimere gli elementi rilevanti dell'attacco. A riguardo, hanno sottolineato che gli Stati hanno il dovere di garantire che il loro territorio non venga utilizzato per atti contrari al diritto internazionale.

"A State shall not knowingly allow the cyber infrastructure located in its tettirory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States".
(Uno Stato non deve consentire consapevolmente che una infrastruttura locata sul proprio territorio o sotto il suo esclusivo controllo governativo possa essere usata per atti che influiscono negativamente e illegalmente contro un altro Stato).

Rule n. 5, Tallin Manual

Al contrario, una minoranza del Gruppo ha preso la posizione secondo cui l'uso della forza per legittima difesa sul territorio di uno Stato a cui l'attacco armato non è imputabile è inammissibile, anche se altre risposte, come un'azione basata sullo stato di necessità, potrebbero essere appropriate. Questo, naturalmente, presuppone l'assenza sia del consenso di questo Stato sia dell'autorizzazione da parte del Consiglio di Sicurezza delle Nazioni Unite.

Gli Esperti, che hanno accettato la liceità delle azioni difensive oltre confine, hanno enfatizzato il fatto che lo Stato vittima deve prima chiedere allo Stato territoriale di porre fine alle attività che pongono in essere l'attacco armato. Lo Stato vittima deve anche dare l'opportunità e il tempo necessario allo Stato territoriale di affrontare la situazione. Questi requisiti derivano da un obbligo di diritto internazionale di rispettare (nella maniera più estesa possibile) la sovranità dello Stato sul quale le azioni difensive sono prese. Tuttavia, ci potrebbero essere situazioni eccezionali in cui non c'è il tempo di trasmettere la richiesta o di risolvere la situazione. Se è necessaria un'azione immediata per respingere un

attacco armato informatico o per ridurne le conseguenze, lo Stato vittima può agire immediatamente in autodifesa[97].

Comunque sia, va nuovamente sottolineata la difficoltà nell'attività di attribuzione delle operazioni informatiche, siano esse condotte da attori statali o non-statali, a causa della difficoltà tecnica di individuarne l'origine. Mentre la provenienza di alcuni attacchi è particolarmente evidente, sia perché gli autori si identificano[98], sia perché a seconda delle circostanze è più facile attribuirne la fonte[99], la maggior parte di essi, invece, grazie all'utilizzo congiunto di *botnet* e di *IP Spoofing*, sono svolti nell'anonimato. Per cui atti che ricadrebbero sotto la responsabilità degli Stati, spesso, vengono attribuiti ad attori non statali e viceversa.

La *Corte Internazionale di Giustizia* ha stabilito che l'attribuzione dell'azione e quindi la responsabilità debba essere provata dallo Stato vittima con una certa evidenza, affinché soggetti innocenti non vengano coinvolti nelle ostilità. Ciò, in generale, rende molto improbabile che sorga il diritto di autotutela individuale o collettiva.

Le azioni intraprese prima che tale responsabilità venga confermata, infatti, sono classificate come rappresaglia armata, piuttosto che come azioni di autotutela[100].

Sono considerate rappresaglie anche le azioni di autotutela intraprese contro attori non-statali, che non rispettano i requisiti di necessità, proporzionalità e immediatezza[101].

Un altro punto merita una precisazione. Generalmente è accettato l'uso della forza in autodifesa contro attacchi armati effettuati da attori non-statali che agiscono su scala transnazionale (come le organizzazioni terroristiche), organizzati con un nome, una leadership, una gerarchia, una struttura e un metodo. Ciò, ovviamente, varrebbe anche nel caso in cui essi avvenissero nel cyberspazio[102].

---

[97] Si veda *Tallinn Manual*, cit., *Rule 13*, para. 22, pag. 58.

[98] Per approfondimenti si veda il caso di *Anonymous*. Va sottolineato, tuttavia, che ad oggi né nazioni, né organizzazioni terroristiche si sono assunte alcun tipo di responsabilità per il loro attacchi.

[99] Come nel caso dell'attacco di Israele contro la Siria.

[100] Le rappresaglie o contromisure che comportano l'uso della forza sono proibite nel diritto internazionale. Uno dei limiti che si è soliti assegnare loro è costituito, infatti, dall'impossibilità di ricorrere a violazioni del diritto internazionale cogente, tra cui, ovviamente, la norma che sancisce il divieto di ricorrere alla minaccia o all'uso della forza.

[101] Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, Emory Public Law Research Paper No. 12-234, Emory University School of Law, Atlanta, 2012, p. 14.

[102] Sul punto Jhon Gray parla di *"…rischio crescente di terrorismo* [informatico]. *Il diffondersi di avanzate abilità informatiche tra i soldati di armate senza Stato crea la potenzialità per un tipo di guerra informatica diretta sia contro bersagli civili, come aeroporti e centrali energetiche, sia contro*

Non è altrettanto chiaro, invece, se il diritto di legittima difesa valga qualora attacchi cibernetici vengano effettuati da singoli individui o gruppi ristretti di individui non appartenenti a nessuna organizzazione e che agiscono autonomamente e separatamente (come ad es. un singolo hacker) dal territorio di altri Stati. Quest'ultima circostanza è la vera peculiarità dei conflitti informatici.

Laurie R. Blanck afferma che non esiste nessun impedimento al fatto che gli Stati Uniti o un qualsiasi altro Stato possa ricorrere in futuro all'uso della forza per scoraggiare, respingere o rispondere ad attacchi armati provenienti da un singolo individuo che agisce nel cyberspazio dal territorio di un altro Stato, o da individui che agiscono separatamente dai territori di Stati diversi[103].

Anche se ciò è altamente improbabile che avvenga, sarà la prassi a confermarlo ma, a pensarci bene, cosa è stato il conflitto in Afghanistan se non una gigantesca 'caccia all'uomo' culminata con la cattura di Osama Bin Laden, il 2 maggio 2011, nel rifugio segreto ad Abbottabad, in Pakistan[104]?

La possibilità di una *cyber war* asimmetrica, cioè contro soggetti non-statali, specialmente le organizzazioni terroristiche, tuttavia, è di difficile concretizzazione per una serie di altri motivi. Prima di tutto, non sono in possesso delle capacità sufficienti per causare danni di una certa importanza; inoltre tali organizzazioni preferiscono ricorrere ad atti sanguinosi reali, che dal loro punto di vista, sono molto più efficaci; infine, esse sarebbero più propense ad evitare il cyberspazio per scopi terroristici per il timore che possano cambiare le regole che ne disciplinano l'utilizzo: la libertà del cyberspazio, infatti, garantisce loro innumerevoli benefici, come la gestione delle organizzazioni, il mantenimento delle comunicazioni tra gli attivisti, la possibilità di fare appelli o proselitismo, la possibilità di utilizzare la rete come mezzo di addestramento o reclutamento di potenziali autori di attentati[105].

Per questi e altri motivi, si può affermare che ad oggi il *cyber terrorismo* non sia mai esistito, ma rimane certamente un'ipotesi futuribile.

La totalità delle attività informatiche finora condotte da attori non-statali, quindi, ricade nella categoria del *cyber crime*.

---

strutture di comando militare…Ci sono voci secondo cui Al Qaeda avrebbe fatto tentativi simili." in Jhon Gray, *Al Qaeda e il significato della modernità*, Fazi Editore, Roma, 2004, pag. 83.

[103] ibidem pp.10-11.

[104] Per approfondimenti sulla vicenda si veda Guido Olimpio, *La testa del serpente. Tutti i segreti di Osama Bin Laden*, Instant book Corriere della Sera n.32 del 25/01/2010.

[105] Even Shmuel, Siman David-Tov, *Cyber Warfare*, cit., pp. 43-44.

X. Il Consiglio di Sicurezza delle Nazioni Unite

La Carta delle Nazioni Unite e il Tallinn Manual prevedono l'obbligo di segnalare le misure informatiche prese in autotutela al Consiglio di Sicurezza delle Nazioni Unite.

> *"…Le misure prese dai 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 ed il compito spettanti secondo il presente Statuto, al Consiglio di Sicurezza, di intraprendere in qualsiasi momento quella azione che esso ritenga necessaria per mantenere o ristabilire la pace e la sicurezza internazionale".*
>
> Art. 51, Carta delle Nazioni Unite

> *"Measures involving cyber operations undertaken by States in the exercise of the right of self defence pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council"*.
> (Le misure che coinvolgono operazioni informatiche prese dagli Stati nell'esercizio del diritto di autotutela secondo l'Articolo 51 della Carta delle Nazioni Unite devono essere immediatamente segnalate al Consiglio di Sicurezza delle Nazioni Unite).
>
> Rule 17, Tallinn Manual

La mancata segnalazione da parte di un Membro delle Nazioni Unite delle operazioni informatiche intraprese in questo contesto costituisce pertanto una violazione della Carta. Tuttavia, l'obbligo di segnalazione non corrisponde a una norma di diritto internazionale consuetudinario e una sua violazione non priva lo Stato in questione del diritto di agire in autotutela.

Secondo l'art. 51, il diritto di agire in autotutela continua fino a che il Consiglio di Sicurezza non *"ha preso le misure necessarie per mantenere la pace e la sicurezza internazionale"*. Il Consiglio può espressamente privare lo Stato del diritto di autotutela secondo l'art. 51. Solo esso gode di questa autorità, sebbene non l'abbia mai esercitata. Viceversa il Consiglio non può mai essere privato della sua autorità in relazione al mantenimento della pace e della sicurezza internazionale ex. Capitolo VII della Carta, dal fatto che uno Stato stia lecitamente esercitando il suo diritto di autotutela.

La seconda eccezione del divieto di uso della forza secondo la *Carta* Onu sono le misure di sicurezza collettiva autorizzate dal Consiglio di Sicurezza:

"Should the United Nations Security Council determine that an act constitutes a threat to the peace, breach of the peace, or act of aggression, it may authorize non-forceful measures, including cyber operations. If the Security Council considers such measures to be inadequate, it may decide upon forceful measures, including cyber measures".
(Il Consiglio di Sicurezza delle Nazioni Unite accerta l'esistenza di una minaccia alla pace, di una violazione della pace o di un atto di aggressione, può autorizzare le misure non implicanti l'uso della forza, incluse le operazioni informatiche. Se il Consiglio di Sicurezza ritiene queste misure inadeguate, può intraprendere misure implicanti l'uso della forza, incluse le misure informatiche).

Rule 18, Tallinn Manual

Questa regola è basata sul Capitolo VII della *Carta delle Nazioni Unite* e precisamente sugli artt. 39, 40, 41 e 42. Fino ad oggi, il Consiglio di Sicurezza non ha mai determinato che una operazione informatica costituisce una minaccia alla pace, una violazione della pace o un atto di aggressione. Tuttavia, a Tallinn pensano che: *"il Consiglio di Sicurezza abbia tutta l'autorità per farlo. Sebbene esso abbia etichettato solo due fenomeni come minaccia alla pace (il terrorismo internazionale e la proliferazione delle armi di distruzione di massa) esso potrebbe ugualmente decidere che un particolare tipo di operazione informatica può essere una minaccia alla pace, una violazione alla pace o un atto di aggressione, anche in abstracto, ovvero, senza riferimento ad atti particolari che hanno avuto luogo o stanno avendo luogo"*[106]. Per esempio, sarebbe nell'autorità del Consiglio di Sicurezza determinare se operazioni informatiche dirette contro sistemi bancari nazionali o infrastrutture critiche nazionali si qualificano come tali.

L'art. 41 della *Carta* prevede che il Consiglio *"può decidere quali misure non implicanti l'impiego della forza debbano essere adottate per dare effetto alle sue decisioni, e può invitare i Membri delle Nazioni Unite ad applicare tali misure. Queste possono comprendere una totale o parziale interruzione delle relazioni economiche e o delle comunicazioni ferroviarie, marittime, aeree, postali, telegrafiche, radio ed altre, e la rottura delle relazioni diplomatiche"*. La lista di tali misure è solo esemplificativa e non tassativa, potendo il Consiglio prendere qualsiasi altra misura che abbia scopo sanzionatorio e che non comporti l'impiego delle forze armate[107], inclusa la completa o parziale interruzione delle comunicazioni informatiche con attori statali o entità non statali.

[106] *Tallinn Manual*, cit., *Rule 18*, para 2, p. 65; di questa opinione è anche Heather Harrison Dinnis, cit., p. 110.
[107] Anche se il Consiglio può prendere misure di carattere militare, riconducibili all'art. 42 della Carta, per assicurare il rispetto delle misure pacifiche di cui all'art. 41.

L'ultima frase della *Rule 18* è tratta dall'art. 42 della Carta: una volta che il Consiglio di Sicurezza ha determinato l'esistenza di una minaccia alla pace, una violazione alla pace o un atto di aggressione e che le misure non implicanti l'uso della forza sono inadeguate o si sono dimostrate tali, per mantenere o restaurare la pace o la sicurezza internazionale, può autorizzare l'uso della forza con *"ogni azione necessaria per mantenere o ristabilire la pace e la sicurezza internazionale"*. Ciò implica l'autorità di intraprendere operazioni informatiche contro uno Stato o entità non statali oggetto della risoluzione, ma anche di intraprendere azioni cinetiche contro le loro capacità o infrastrutture informatiche, anche se va ricordato che quest'ultime non sono il mezzo ideale per contrastare gli attacchi informatici vista la loro natura 'geograficamente distribuita' a causa dei *botnet*. Un esempio perfetto del primo caso sarebbe potuto essere il *worm Stuxnet* lanciato nella centrale nucleare iraniana di Natanz, allo scopo di sabotare la centrifuga della centrale, una volta espresso, da parte del Consiglio, il timore di un rischio proliferazione nel programma nucleare iraniano.

XI. Case study: l'Estonia

Il 27 aprile 2007 l'Estonia è stata vittima di una prolungata serie di attacchi informatici senza precedenti (di tipo DDoS) che ha causato il collasso del sistema bancario, di numerosi servizi governativi, di alcune società e perfino del sistema mediatico. Gli attacchi hanno causato un danno economico di circa dieci milioni di euro a causa dell'elevata dipendenza tecnologica dell'Estonia. Tuttavia, nessuna infrastruttura strategica è stata compromessa. La piccola repubblica baltica, che fa parte dell'Unione Europea dal 2003 e della Nato dall'anno successivo, è forse il paese a più alta penetrazione tecnologica del mondo. E' la patria di Skype e dell'*e-Government*. A Tallinn e dintorni i cittadini possono fare tutto via internet. Votare alle elezioni politiche e amministrative, pagare le tasse, consultare il catasto, prenotare una visita medica specialistica con lo smartphone, ecc.

Gli attacchi provenivano da tutto il mondo, ma funzionari estoni ed esperti di sicurezza informatica hanno affermato che, soprattutto nella fase iniziale, molti aggressori, identificati dai loro indirizzi internet, erano russi e alcuni dei quali appartenevano a istituzioni statali russe.

Nonostante le immediate ed esplicite accuse da parte del governo estone rivolte alla Federazione Russa, considerata il mandante dell'offensiva informatica, l'Estonia ha successivamente fatto marcia indietro[108]. Questo è stato il primo caso in cui uno Stato ha accusato direttamente un altro Stato di aver lanciato attacchi

[108] http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

informatici contro di esso. Il governo estone, a seguito di ciò, ha sollevato l'emergenza informatica di fronte alla Comunità Europea e all'Alleanza Atlantica, sottolineando specificatamente la vulnerabilità della materia anche dal punto di vista giuridico.

"At present, Nato does not define cyber-attacks as a clear military action. This means that the provisions of Article V of the North Atlantic Treaty, or, in other words collective self-defence, will not automatically be extended to the attacked country"

ha detto il ministro della difesa estone, Jaak Aaviksoo.

"…Not a single Nato defence minister would define a cyber-attack as a clear military action at present. However, this matter needs to be resolved in the near future".

Questa dichiarazione riflette perfettamente quello che era il punto di vista degli Stati a seguito degli eventi estoni, che in maniera coerente al diritto internazionale e alle indicazioni della *Corte Internazionale di Giustizia*, fin qui esposte, non hanno ritenuto opportuno far rientrare il caso Estone nell'art. V del *Trattato Nord Atlantico* o *Patto Atlantico*:

> *"Le parti convengono che un attacco armato contro una o più di esse in Europa o nell'America settentrionale sarà considerato come un attacco diretto contro tutte le parti, e di conseguenza convengono che se un tale attacco si producesse, ciascuna di esse, nell'esercizio del diritto di legittima difesa, individuale o collettiva, riconosciuto dall' art. 51 dello Statuto delle Nazioni Unite, assisterà la parte o le parti così attaccate intraprendendo immediatamente, individualmente e di concerto con le altre parti, l'azione che giudicherà necessaria, ivi compreso l'uso della forza armata, per ristabilire e mantenere la sicurezza nella regione dell'Atlantico settentrionale. Ogni attacco armato di questo genere e tutte le misure prese in conseguenza di esso saranno immediatamente portate a conoscenza del Consiglio di Sicurezza. Queste misure termineranno allorché il Consiglio di Sicurezza avrà preso le misure necessarie per ristabilire e mantenere la pace e la sicurezza internazionali".*
>
> Art. V , Trattato Nord Atlantico

Ciò non vuol dire che in futuro un'operazione informatica non possa essere considerata un attacco armato ai sensi dell'art. V del Patto Atlantico, ma ciò potrà essere deciso solo volta per volta.

Il caso estone ha spinto la NATO ad approfondire le proprie difese informatiche. Dopo gli attacchi informatici contro l'Estonia nel 2007, le minacce informatiche si sono rapidamente evolute in frequenza e raffinatezza. Nell'estate del 2008, la guerra in Georgia ha dimostrato che gli attacchi informatici hanno il potenziale per diventare una componente importante della guerra convenzionale. Lo sviluppo e l'utilizzo di strumenti informatici distruttivi che possono minacciare la sicurezza e la stabilità nazionale ed euro-atlantica rappresentano un cambiamento strategico che ha aumentato l'urgenza di una nuova politica di difesa informatica della NATO, al fine di rafforzare le difese informatiche non solo del proprio Quartier Generale e delle relative strutture, ma di tutta l'Alleanza nel suo complesso.

Con questa convinzione, il nuovo Concetto strategico adottato al vertice di Lisbona per il 2010 ha evidenziato la necessità di intensificare gli sforzi in difesa informatica[109] e ha incaricato il Consiglio Nord Atlantico di sviluppare una nuova politica sulla difesa informatica che è stata adottata dai ministri della Difesa NATO l'8 Giugno 2011 e un piano d'azione che è in corso di attuazione[110]. Il successivo vertice di Chicago nel 2012 ha riaffermato questa politica.

XII. Considerazioni conclusive

Sopra quanto detto, si può raggiungere la conclusione che la *cyber war*, in realtà, non è niente di così astratto o trascendentale. E' necessario ridimensionare il fenomeno e trascinarlo all'interno della normale concezione dei conflitti armati convenzionali affinché non si dia vita a uno spazio di azione indisciplinato e senza nessun limite. Tale lavoro ermeneutico deve basarsi sulla fondamentale distinzione fra la *cyber war*, come qui descritta, e altri fenomeni, come la *info war* o il *cyber crime*.

La classificazione dei vari livelli dell'uso della forza, pertanto, evidenzia come le uniche operazioni informatiche che rientrano nel fenomeno della *cyber war* sono quelle che: 1) causano danni fisici alla proprietà o alle persone di una gravità tale da costituire un attacco armato (secondo la nozione più ristretta che prende in considerazione solo la proporzione e gli effetti del danno) e che provocano una risposta in autotutela individuale o collettiva; 2) che, al di sotto dell'uso della forza come attacco armato, possono essere contrastate con

[109] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon*, Lisbona, 19 Novembre 2010, para. 19.

[110] Per approfondimenti si veda *Principal cyber defence activities*, in http://www.nato.int/cps/en/SID-252D781D-1D0C211D/natolive/topics_78170.htm?.

proporzionate contromisure o facendo affidamento al Consiglio di Sicurezza delle Nazioni Unite.

Quanto detto finora non ha ancora trovato, ad oggi, nessuna espressione pratica né è stato formalizzato in un accordo internazionale. Quasi nessuno Stato, infatti, ha adottato questa linea di pensiero, trovando nello *status quo*, fornito dall'ambiguità della normativa applicabile alle operazioni informatiche, mutui benefici e un maggiore libertà d'azione. Ma dato l'utilizzo sempre più frequente delle operazioni informatiche e la loro già appurata potenzialità distruttiva, è molto probabile un cambio di atteggiamento e che, pertanto, o:

- venga spontaneamente applicato il diritto esistente dei conflitti armati, oppure
- venga formalizzato in un trattato che delinei chiaramente le pratiche della moderna guerra cibernetica.

Per questo motivo è importante, fin da ora, affermare la conseguente applicabilità del diritto internazionale umanitario (*jus in bello*[111]) alle *cyber war* internazionali e non-internazionali[112].

Anche questa conclusione, però, non è esente da criticità interpretative. Per quanto riguarda le potenziali *cyber war* asimmetriche (essenzialmente quelle contro il *cyber terrorismo* internazionale), se la certezza che si possa rispondere in legittima difesa contro un attacco armato di un attore non-statale e che, conseguentemente, si possa generare un conflitto armato, appare confermata, meno chiara è la natura che tale conflitto debba avere e pertanto quale delle seguenti discipline si debba applicare:

- diritto umanitario dei conflitti armati internazionali;
- diritto umanitario dei conflitti armati non-internazionali (Art. 3 comune alle Convenzioni di Ginevra 1949 e II Protocollo Aggiuntivo 1977);
- o il solo diritto internazionale dei diritti umani[113].

[111] Esso è composto in larga parte dalle previsioni delle Convenzioni di Ginevra e dal diritto consuetudinario.

[112] Su come i principi fondamentali del diritto internazionale umanitario (lealtà, , necessità militare, distinzione, precauzione, proporzionalità) possono trovare adattamento alla *cyber war* cfr. Blank Laurie R., *International Law and Cyber Threats from Non-State Actors*, cit., pp.21-29 e Heather Harrison Dinnis, *Cyber Warefare and the Laws of War*, cit., pp. 117-278; SchmittMichael N. (a cura di), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, cit., pp. 83-148.

[113] Per un approfondimento su questo problema si veda Renata Tallarico, *La definizione di conflitto armato nel diritto internazionale umanitario*, CORSO DI DOTTORATO DI RICERCA IN DIRITTO INTERNAZIONALE E DELL'UNIONE EUROPEA CICLO XXIII, Università degli Studi di Macerata, 2011, pp. 78-125, disponibile su http://ecum.unicam.it/598/1/Tesi_di_dottorato_in_diritto_Internazionale_e_dell'Unione_Europea_Ta

Lo stesso dicasi per una eventuale *cyber war* tra uno Stato vittima e singoli individui *non organizzati* tra loro che provocano attacchi armati oltre i confini territoriali degli Stati in cui si trovano fisicamente e in cui agiscono in maniera autonoma e separata.

llarico_2012.pdf.

PARTE II

STRATEGIE E MISURE DI PREVENZIONE E CONTRASTO ALLE OPERAZIONI INFORMATICHE NELL'AREA EURO-ATLANTICA

Sommario: **I.** Il principio della deterrenza nell'ambito informatico – **II.** Cyber security concept – **III.** La strategia europea – **IV.** La strategia statunitense – **V.** La strategia nato – **VI.** Considerazioni conclusive.

I. Il principio della deterrenza nell'ambito informatico

Le operazioni informatiche sono caratterizzate dalle seguenti peculiarità:

- la maggior parte delle volte non è possibile conoscere l'autore di un attacco informatico, il quale può anche utilizzare strutture informatiche di soggetti terzi (come nel caso Estone);
- nessuno Stato ha finora rivendicato alcun tipo di attacco informatico;
- la capacità di effettuare danni non è sempre legata alle quantità delle strutture informatiche a propria disposizione;
- le modalità tecniche utilizzate in un attacco non sempre sono identificabili;
- le operazioni informatiche finalizzate a procurare un danno non è detto che raggiungano il proprio obbiettivo con assoluta certezza;
- gli strumenti informatici finora non possono essere considerate armi di distruzione di massa.

Questi sono alcuni motivi per cui non è possibile adattare il tradizionale principio della deterrenza, esistente tra gli Stati nell'ambito delle armi convenzionali e nucleari, alle loro capacità informatiche.

La ricerca della deterrenza costringerebbe gli stati a rivelare pubblicamente ed anticipatamente le proprie capacità informatiche, la cui efficienza, al contrario, si basa sulla segretezza e sulla sorpresa. Ogni attacco va progettato di per sé e adattato ai sistemi di protezione della struttura cui viene indirizzato. Non è possibile, pertanto, predisporre preventivamente delle 'armi informatiche' generiche capaci di colpire chiunque, in qualsiasi momento.

Così, mentre le capacità difensive vengono rivelate dagli Stati, le capacità offensive vengono tenute nascoste.

Tuttavia, l'impossibilità di adattare analogicamente suddetto principio al cyberspazio non preclude che equilibri dissuasivi tra gli Stati possano sussistere:

avvertimenti, penetrazioni nei sistemi, attacchi limitati sono attività diffuse per dimostrare parzialmente le proprie capacità.

La differenza sostanziale sta nel fatto che, mentre il principio classico della deterrenza si basa sullo sviluppo di capacità offensive e distruttive atte a scoraggiare ogni aggressione (per cui il nemico in vista delle conseguenze certe di un proprio attacco sia dissuaso dal metterlo in opera), al contrario il bilanciamento dei poteri nel cyberspazio si basa principalmente sulle capacità difensive, ossia sulle capacità di evitare, limitare e contenere i danni eventuali derivanti da un attacco informatico, così da dissuadere o vanificare ogni tipo di tentativo, e solo secondariamente sulle capacità offensive.

Il primo si regge sull'equilibrio del terrore, il secondo tutt'al più sulla sfida all'inviolabilità dei propri domini e sulla capacità di resilienza.

In conclusione può affermarsi, nonostante parte della dottrina adduca il contrario[114] e contrariamente agli ambiti governati dal principio della deterrenza, che le capacità difensive nel cyberspazio sono importanti tanto quanto quelle offensive.

Come vedremo, questo perfetto bilanciamento ha causato negli ultimi anni una colossale proliferazione di strutture specificatamente impiegate in attività di difesa informatica.

II. Cyber security concept

Comunemente e ufficiosamente col termine *cyber security* ci si riferisce alle garanzie e alle azioni intraprese per proteggere il dominio informatico, sia nel campo civile sia in quello militare, dalle minacce che possono danneggiare l'interdipendenza delle reti e le infrastrutture informatiche.

Tuttavia, è necessario rilevare l'assenza di definizioni condivise. In tutti i documenti strategici relativi alla politica in materia, né in quelli più generici relativi alla sicurezza statale, è presente una definizione comune dell'espressione *cyber security*.

Così, quella della *cyber security* risulta essere un problema dalla natura non ben definita, che deriverebbe da un'infelice combinazione di intuizione e incertezza uniti alla necessità di dare una risposta alle problematiche ritenute più urgenti in un determinato momento storico.

[114] Si veda Lin Herbert, *Cyber conflict and international humanitarian law*, "International Review of the Red Cross, June 2012 – Vol. 94, No 886 – New technologies and warfare", pp. 515 – 531, Cambridge University Press online, 01/05/2013, pp. 522 e 523, dove afferma: *"The inherent superiority of offensive cyber operations over defensive operations…"*.

Ad esempio, in un particolare periodo si è assistito principalmente all'accostamento tra la *cyber security* e la necessità di proteggere la privacy dei cittadini.

Una cosa è certa: una percezione aleatoria di *cyber security*, che periodicamente si interessa talora di un ambito, talora di un altro, è profondamente irrazionale perché contribuisce a far sì che le analisi delle minacce si concentrino su eventi di grande effetto per l'opinione pubblica, distogliendo le risorse dalla gestione di problemi altrettanto urgenti.

Da un'analisi comparata dei principali documenti strategici in ambito nazionale, europeo, extraeuropeo e delle organizzazioni internazionali traspare inoltre un'evidente incoerenza sulle aree di competenza rispetto alle quali deve considerarsi necessario approntare dei piani di sicurezza informatica.

In particolare, delle differenze sostanziali risultano dai documenti strategici dell'UE e dei suoi paesi membri, degli USA e della NATO.

Riguardo i primi[115], l'Osservatorio di politica internazionale del Senato della Repubblica e della Camera dei Deputati, ha evidenziato una certa varietà semantica e la completa mancanza di definizioni formali di *cyber security*. Tuttavia è stato possibile ricostruire, facendo riferimento anche alle politiche concrete adottate dall'UE, l'insieme degli ambiti in cui è considerata necessaria la sicurezza informatica e le minacce dalle quali doversi proteggere:

Figura n. 5 – Ambiti di cyber security

[115] 1) *Un'Europa sicura in un mondo migliore – Strategia europea in materia di sicurezza* (2003); 2) *Relazione sull'attuazione della Strategia europea in materia di sicurezza – Garantire sicurezza in un mondo in piena evoluzione* (2008); 3) Dichiarazione del Consiglio dell'8 dicembre 2008 sul rafforzamento della sicurezza internazionale (2008); 4) *Strategia di sicurezza interna per l'Unione Europea: "Verso un modello di sicurezza europeo"* (2010); 5) *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura* (2010).

Pur nella diversità di contesti (dimensioni interna ed esterna della sicurezza), di paternità istituzionale e di valore politico e legale, i documenti analizzati dall'Osservatorio: *"tentano comunque di fissare delle priorità in termini di risposta alla minaccia"*.

Specialmente l'interesse per il contrasto al *cyber crime* risulta particolarmente elevato con riferimento a categorie come frodi bancarie, furto di identità e di informazioni (es. spionaggio industriale) ecc., che arrecano ingenti danni patrimoniali. Inoltre, questo tipo di attacchi statisticamente rappresenta la maggior parte ed è perciò percepito come più urgente dai cittadini e dal settore privato (certamente più di questioni considerate remote dall'opinione pubblica, come la cyber war).

L'aspetto più rilevante che è necessario considerare in questa sede è che il concetto europeo di *cyber security* (tralasciando qualche vago riferimento *"agli attacchi contro sistemi informatici privati o governativi…"* come *"…nuova arma potenziale di tipo economico, politico e militare"*[116]), non ricomprende esplicitamente la guerra cibernetica o *cyber war*, come realtà distinta.

Nell'approccio europeo, le iniziative di protezione delle reti e delle infrastrutture in senso lato e la lotta al *cyber crime* sono strettamente correlate tra loro, per non dire che sono la stessa cosa.

Al contrario, la dimensione della guerra cibernetica è da qualche anno parte integrante della dottrina di difesa statunitense.

La conclusione è che in Europa la *cyber war* è per il momento considerata di esclusiva competenza della NATO, oltre che ovviamente dei singoli Stati. Infatti, nell'Alleanza atlantica si è assistito ad un dibattito sull'opportunità di considerare attacchi cibernetici su larga scala, come quelli perpetrati ai danni dell'Estonia (membro NATO) nel 2007 e della Georgia (aspirante membro NATO) nel 2008, come fattispecie rientranti negli artt. 4 e 5 del Trattato di Washington, tali dunque da attivare la clausola di difesa collettiva tra gli Alleati e sull'opportunità di rafforzare le capacità di difesa cibernetica degli stessi.

III. La strategia dell'Unione Europea

Il 7 febbraio 2013, la Commissione Europea, di concerto con l'*Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza* Catherine Ashton, ha pubblicato il primo documento strategico globale che l'UE abbia mai

[116] *Relazione sull'attuazione della Strategia europea in materia di sicurezza – Garantire sicurezza in un mondo in piena evoluzione* (sintesi), Consiglio dell'Unione Europea, Bruxelles, 11 dicembre, 2008, p. 5.

prodotto in materia di *cyber security*. Esso si intitola *"An Open, Safe and Secure Cyberspace"*[117] ed espone la visione complessiva dell'Unione Europea sul modo migliore per prevenire e contrastare le perturbazioni, gli incidenti e gli attacchi informatici. L'intento è promuovere i valori europei di libertà e democrazia e garantire che l'economia digitale possa svilupparsi in modo sicuro.

L'obiettivo è alquanto ambizioso: rendere lo spazio informatico europeo il più sicuro del mondo (*"the safest in the world"*).

Secondo la strategia, il principio fondamentale che dovrebbe guidare la politica di sicurezza dell'Unione nel cyberspazio è quello secondo il quale **i valori e le norme che si applicano nelle altre aree della nostra vita quotidiana debbono applicarsi anche nel dominio informatico** (libertà, democrazia, rispetto della dignità umana, uguaglianza). Da questo assunto, ovviamente, derivano una serie di corollari come la protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della privacy, così come la necessità di consentire un acceso senza limitazioni a tutti i cittadini e ancora l'importanza di una governance condivisa tra attori pubblici e privati nella gestione della rete.

Viene evidenziata la necessità di rispettare lo stato di diritto e il diritto esistente anche nel cyberspazio, non essendo chiamata l'UE alla creazione di nuove norme in materia.

La strategia stabilisce una serie di priorità chiare per rafforzare la politica internazionale dell'UE in materia di sicurezza informatica. Esse sono:

- conseguire la resilienza informatica;
- ridurre drasticamente la criminalità informatica;
- **sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune (CSDP);**
- sviluppare le risorse industriali e tecnologiche per la sicurezza informatica;
- istituire una coerente politica internazionale del ciberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE.

L'ottenimento di tutti questi obiettivi viene subordinato a un potenziamento della cooperazione tra le istituzioni europee e quelle nazionali e tra il settore pubblico e quello privato, il cui coordinamento è affidato principalmente alla

[117] Commissione Europea, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, Brussels, 07/02/2013.

responsabilità degli Stati, con il contributo ausiliario dell'UE[118]. A tal fine, gli Stati Membri sono invitati a sviluppare delle proprie strategie di cyber security.

Il terzo punto costituisce, forse, la parte più innovativa del documento, laddove rappresenta, rispetto ai documenti precedenti sulla sicurezza, sia interna sia esterna[119], il raggiungimento di una maggiore consapevolezza in ambito europeo nel giudicare il *cyberspazio* come possibile fonte di minacce diverse dal *cyber crime* ed alle molteplici origini[120], che possono attentare alla sicurezza e alla difesa comune, seppur nel documento non si faccia ancora nessun tipo di riferimento esplicito alla *cyber war*:

"If armed conflict extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights Law will apply to the case at hand"[121].

Ancora:

"…the response mechanisms will differ depending on the nature, magnitude and cross-border implications of the incidents…If the incidents seems to relate to cyber espionage or a state-sponsored attack, or has national security implications, national security and defence authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union)"[122].

Inoltre, appare chiara l'importanza di sostenere la ricerca e lo sviluppo in materia, di mantenere una stretta cooperazione tra i paesi membri e l'*European Defense Agency* (EDA)[123]e tra questi e il settore privato (l'Agenzia, nell'ambito

---

[118] *"National Governments are the best placed to organize the prevention and response to cyber incidents and attacks and to establish contacts and networks with the private sector and the general public across their established policy streams and legal frameworks"*, in *An open, Safe and Secure Cyberspace, cit.,* cap. 3.

[119] Per approfondimenti si veda Consiglio Europeo, *Relazione sull'attuazione della Strategia europea in materia di sicurezza – Garantire sicurezza in un mondo in piena evoluzione* (sintesi), Brussels, 11 dicembre, 2008, p. 5, dove si afferma che *"…gli attacchi contro sistemi informatici privati o governativi negli Stati membri dell'UE hanno dato a tale questione una nuova dimensione, quella di una nuova arma potenziale di tipo economico, politico e militare"*. V. anche COMMISSIONE EUROPEA, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, COM(2010) 673, Brussels, 22/11/2010, OBIETTIVO 3 – *Aumentare i livelli di sicurezza per i cittadini e le imprese nel ciberspazio*, dove la concezione della sicurezza delle reti informatiche appare limitata al buon funzionamento della società dell'informazione avverso i pericoli della criminalità informatica, al fine di instaurare un clima di fiducia e sicurezza per gli utenti della rete.

[120] *"Threats can have different origins including criminal, politically motivated,* ***terrorist*** *or* ***state-sponsored*** *attacks as well as natural disasters and unintentional mistakes"*, par. 1.1.

[121] *An open, Safe and Secure Cyberspace*, cit., cap. 2.5.

[122] *An open, Safe and Secure Cyberspace*, cit., cap. 3.2.

[123] Che fa parte della struttura CSDP, che a sua volta fa parte dell'EEAS (*European External Action Service*).

della politica di sicurezza e di difesa comune, sull'input datole dalla strategia, sta sviluppando le capacità e le tecnologie di difesa informatiche, implementando la formazione e le esercitazioni. Cerca di valorizzare le sinergie tra gli approcci civili e militari a protezione dei beni informatici critici, promuovendo il dialogo - in particolare con lo scambio di buone pratiche e informazioni - e la creazione di una cultura sulla cyber-sicurezza).

Soprattutto, però, viene ribadito il ruolo chiave della Nato quale partner privilegiato dell'UE nel garantire la sicurezza informatica.

Il documento suddetto rappresenta l'ultimo tassello di un percorso intrapreso ormai da tempo. La Commissione Europea, infatti, sostiene attivamente da molti anni la sicurezza informatica attraverso la promozione un maggiore dialogo tra gli Stati membri e le istituzioni comunitarie, così come tra tutti gli attori chiave del settore, sia pubblici sia privati. Un primo importante passo in tal senso è stato lo sviluppo del NIS (*Network and Information Security*[124]) quale punto di riferimento per la statuizione di criteri minimi comuni di sicurezza da adottare a livello nazionale.

Ad esso è succeduta la creazione di strutture ad hoc, come l'*Agenzia Europea per la Sicurezza delle Reti e dell'Informazione* (*European Network and Information Security Agency*, ENISA). Creata nel 2004 e con sede a Creta, l'ENISA è essenzialmente una piattaforma di scambio di informazioni e *best practice* tra le istituzioni UE, le autorità nazionali e le imprese. Può inoltre fornire pareri tecnici sia alle autorità degli Stati membri sia alle istituzioni comunitarie.

Essa non ha al momento un ruolo operativo, per cui non si occupa di questioni legate alla cyber criminalità.

Un ruolo di rilievo, in tal senso, è svolto, invece, dall'Europol, l'Ufficio Europeo di Polizia, che ospita la Piattaforma Europea per la cyber criminalità (*European Cybercrime Centre* -EC3) la cui funzione è favorire la raccolta, lo scambio e l'analisi di informazioni in materia di crimini informatici tra gli Stati membri. Contribuisce a promuovere la ricerca e l'innovazione, ad assicurare lo sviluppo di capacità da parte delle autorità incaricate dell'applicazione della legge, dei giudici e dei pubblici ministeri e a effettuare valutazioni e monitoraggi delle minacce (in specie botnets e intrusioni), compresi analisi delle tendenze, previsioni e allarmi rapidi.

Le aree principali su cui si concentrano le indagini dell'EC3 sono:

[124] Il NIS è un documento della Commissione Europea (COM(2001)298), periodicamente aggiornato.

- le attività illegali compiute dalla criminalità organizzata al fine di generare grandi profitti economici, come le frodi on-line o gli attacchi contro l'e-banking;
- i crimini che causano seri danni alle persone, come lo sfruttamento sessuale dei minori sulla rete[125];
- i reati che colpiscono direttamente le infrastrutture critiche e i sistemi di informazione dell'UE.

Esso coopera strettamente con Eurojust[126] e CEPOL[127], al fine di aumentare sensibilmente le loro capacità di contrastare il cybercrime, nel rispetto dei loro rispettivi mandati e competenze.

Con riferimento, invece, agli aspetti più operativi, le capacità di risposta ad attacchi o incidenti informatici variano sensibilmente tra gli Stati membri UE. Gli sforzi per colmare il divario tra i più e i meno attrezzati si concentrano sulla creazione di capacità (capacity building) e addestramento e formazione (training), ma soprattutto sulla creazione, in ogni Stato membro, dei *Computer Emergency Response Teams* (c.d. CERT)[128]. Si tratta di squadre per la risposta ad emergenze informatiche, finanziate da università, enti governativi, o, più recentemente, grandi imprese, e costituite da esperti del settore che svolgono una duplice funzione: da un lato, fornire assistenza immediata in caso di anomalie alle reti elettroniche; dall'altro, svolgere attività di prevenzione, monitoraggio e formazione. Il Piano d'Azione UE per la Protezione delle Infrastrutture Critiche Informatizzate[129] prevedeva che, entro il 2012, non solo tutti gli Stati membri, ma

[125] Per un approfondimento sulla normativa internazionale, europea e nazionale a tutela dei minori sui mass media cfr. EMANUELE GRECO, *Sicurezza dei minori e violenza massmediale. Il diritto ad avere diritti*, Biblioteca Archivio Disarmo, Roma, 2013;

[126] Eurojust è un organismo dell'Unione europea con sede all'Aia. Fu istituito nel 2002 per stimolare e migliorare il coordinamento e la cooperazione delle indagini e azioni penali tra le autorità giudiziarie competenti degli Stati membri dell'Unione europea nella lotta alle forme gravi di criminalità organizzata e transfrontaliera al fine di portare i criminali davanti alla giustizia nel modo più rapido ed effettivo possibile.

[127] La CEPOL (*European Police College*) è un'agenzia dell'Unione Europea con sede a Bramshill (Regno Unito). E' una rete che riunisce gli istituti nazionali di formazione degli alti funzionari delle forze di polizia con lo scopo di formare e rafforzare le capacità delle autorità che operano nell'ambito dell'applicazione della legge, di contrastare le minacce in evoluzione, concentrandosi su quelle che presentano una dimensione europea o transfrontaliera, come il traffico di droga, il terrorismo ed appunto la criminalità informatica.

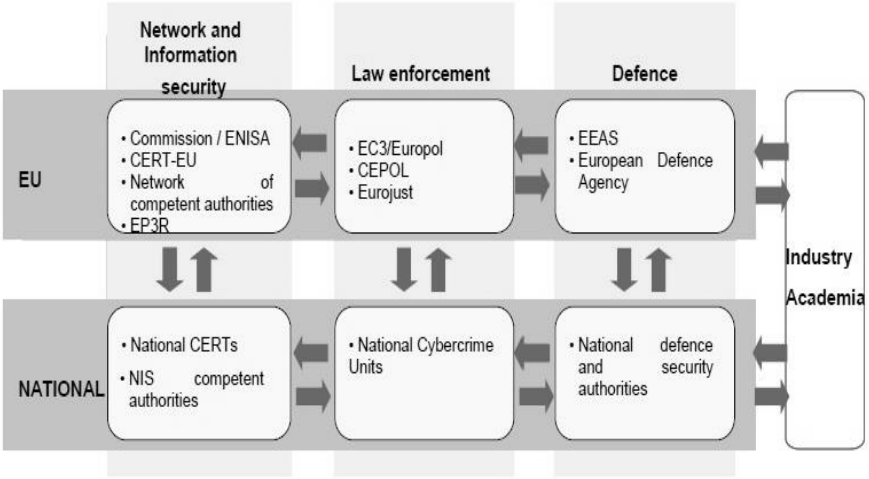
[128] Essi fanno capo al CERT-EU, creato nel 2012.

[129] Commissione Europea, *Protegger e le infrastrutture critiche informatizzate. Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai cyber attacchi e dalle cyber perturbazioni* (CIIP), COM(2009)149, Bruxelles, 2009. Il 31 marzo 2011 la Commissione ha adottato una comunicazione sulla protezione delle infrastrutture critiche – *"Achievements and next steps: towards global cyber-security"*- COM(2011)163 - COM (2011) 163. La comunicazione fa il punto sui risultati raggiunti dopo l'adozione del piano d'azione CIIP nel 2009. Esso descrive le prossime tappe previste per ogni azione a livello europeo e internazionale. Essa si concentra sulla

anche le istituzioni comunitarie si dotassero di almeno un CERT. **Le attività e le competenze specifiche dei CERT nazionali**, non essendo diversamente stabilito dalle direttive comunitarie, **sembra debbano essere disciplinate dal legislatore interno**.

Da quanto detto, emerge che il rafforzamento della security in Europa poggia su tre pilastri principali, ognuno dei quali opera all'interno di contesti legislativi differenti. Una tabella esemplificativa dell'insieme delle strutture europee predisposte alla sicurezza informatica e del loro coordinamento con le strutture nazionali può aiutare a fare chiarezza su un sistema alquanto articolato:

Figura n. 6 – Cyber Defence Governance in UE



Fonte: *An Open, Safe and Secure Cyberspace*, cit., cap. 3.

Infine, è necessario ribadire che la strategia europea, seppur finalizzata ad assicurare una protezione in senso lato, anche tramite attività di contrasto, non prevede esplicitamente la possibilità che operazioni informatiche possano essere considerate come un attacco armato ai sensi dello *jus ad bellum* e per cui si dovrebbe escludere che gli istituti di cui sopra, ad oggi, siano legittimati nonché capaci di condurre operazioni offensive e di prendere parte ad una *cyber war* così come intesa nel capitolo precedente. Molti, infatti, sono ancora gli aspetti da chiarire: dalla definizione di una dottrina europea all'elencazione degli obiettivi ritenuti sensibili, dalla creazione di infrastrutture *ad hoc* a una chiara suddivisione delle competenze, alla formazione del personale e così via.

dimensione globale delle sfide e l'importanza di rafforzare la cooperazione tra gli Stati membri e il settore privato a livello nazionale, europeo e internazionale.

Tuttavia il documento del 2013 e le attività dell'EDA, lasciano presagire un graduale e successivo adattamento della strategia europea in questa direzione, considerato il fatto che non tutti i paesi dell'UE fanno parte della Nato.

A conferma di questa previsione il Consiglio Europeo sulla Difesa del dicembre 2013, ha chiesto, coerentemente con gli sforzi della NATO, di sviluppare un quadro strategico UE più articolato in materia di cyber difesa durante il 2014[130].

IV. La strategia statunitense

Durante lo scorso decennio la consapevolezza americana della minaccia informatica è cresciuta considerevolmente ed è culminata nella formulazione di una precisa strategia in materia. Nel documento *The National Strategy to Secure Cyberspace*, rilasciato dalla Casa Bianca nel febbraio 2003, il presidente Bush per la prima volta fece capire a chiare lettere l'importanza di difendere il cyberspazio quale centro nevralgico all'interno del quale si svolgono tutte le più importanti attività dello Stato: *from business and economy to national defense*. La strategia veniva articolata secondo tre obiettivi:

- Prevent cyber attacks against America's critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur.

Il documento sottolineava la difficoltà e l'originalità della strategia che eccezionalmente richiedeva la cooperazione tra i governi federali e locali, il settore industriale privato e i singoli cittadini americani.

In generale, questi obiettivi strategici rimangono validi ancora oggi e l'attenzione politica nei confronti della sicurezza informatica non è certo diminuita, tutt'altro.

Nel 2009 il Presidente Obama ha descritto la minaccia cibernetica come *"one of the most serious economic security challenges we face as a nation"* e che *"America's economic prosperity in the 21st century will depend on cybersecurity"*[131], esprimendo la preoccupazione che l'America possa probabilmente essere l'oggetto privilegiato di attacchi informatici a causa della sua elevata dipendenza tra le infrastrutture critiche dello Stato e le IT[132].

[130] Consiglio Europeo, *Conclusioni*, EUCO 217/12, 20 Dicembre 2013, Brussels, p. 4.
[131] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity.
[132] Un esempio della dipendenza tra le infrastrutture militari e il cyber spazio è il sistema GIG (*Global Information Grid*) http://www.nsa.gov/ia/programs/global_information_grid/index.shtml.

La necessità di salvaguardare il cyberspazio da un variegato insieme di minacce è stata ribadita anche all'interno del documento *US National Security Strategy* del maggio 2010[133].

La predisposizione della strategia americana, infine, è culminata nel documento pubblicato dalla Casa Bianca nel maggio 2011 dal titolo: *International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World*[134]. Al suo interno viene attribuita una maggiore importanza alla sicurezza informatica in tutti i più importanti campi governativi: negli affari esteri, nella difesa, nella politica economica. Vengono, inoltre, ampliati gli obiettivi strategici statunitensi in considerazione dei propri interessi internazionali. Secondo il documento, infatti, gli Stati Uniti agiranno dentro e oltre i propri confini per sviluppare una informazione globale libera e sicura, consentire il commercio internazionale, proteggere la proprietà intellettuale, rafforzare la sicurezza globale propria e degli alleati attraverso una più stringente cooperazione (soprattutto con la NATO), promuovere la libertà di espressione, la privacy, il rispetto dei diritti umani e il progresso, incoraggiare la cultura della responsabilità delle proprie condotte e supportare lo Stato di diritto nel cyberspazio.

L'evoluzione più importante, che caratterizza la strategia americana, è dovuta al fatto che gli Stati Uniti nel corso degli anni hanno predisposto le premesse teoriche per prepararsi alla *cyber war*. Nel luglio 2011 infatti, il Dipartimento della Difesa ha introdotto cinque iniziative strategiche in linea con la strategia generale della Casa Bianca al fine di implementare le capacità militari nel cyberspazio[135]:

- **Strategic Initiative 1:** *Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential*.
- **Strategic Initiative 2:** *Employ new defense operating concepts to protect DoD networks and systems*. Devono essere considerate sia le difese passive sia quelle attive. A differenza delle prime che consistono in barriere impiegate per ostacolare e impedire a un attacco informatico di andare a buon fine (ad es. i firewall), le difese attive si basano su un approccio dinamico e operano al fine di scovare e contrastare ogni minaccia prima che causi qualsiasi tipo di danno.

[133]http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf, pag. 18 e pag. 27.
[134] Reperibile al sito http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[135] Per approfondimenti si veda il documento *Department of Defence Strategy for Operating in Cyberspace*, del luglio 2011, disponibile su: http://www.defense.gov/news/d20110714cyber.pdf.

- **Strategic Initiative 3:** *Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cyber security strategy*.
- **Strategic Initiative 4:** *Build robust relationships with U.S. allies and international partners to strengthen collective cyber security*. Partendo dalla considerazione che nessun singolo Stato è in grado di garantire una efficace difesa informatica da solo, viene riproposta con maggiore enfasi l'importanza della cooperazione internazionale tra gli alleati per difendere i comuni interessi del cyberspazio attraverso lo scambio di informazioni circa gli attori e le minacce emergenti, attività congiunte di formazione e addestramento, *best practice* condivise o accordi di ripartizione degli oneri per rafforzare le aree in cui gli alleati sono meno abili.
- **Strategic Initiative 5:** *Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation*.

Una ormai matura predisposizione ad affrontare una guerra nel cyberspazio, però, gli Stati Uniti l'hanno manifestata riservandosi il diritto di reagire militarmente di fronte a ogni significativo attacco cibernetico rivolto contro la propria economia, il proprio governo o le proprie forze armate, secondo le regole esposte nel capitolo precedente.

When warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means - diplomatic, informational, military and economic - to defend our nation, our allies, our partners and our interests....If directed by the president, DoD will conduct offensive cyber operations in a manner consistent with the policy principles and legal regimes that the department follows for kinetic capabilities, including the law of armed conflict[136]*.*

L'istituto preposto alla salvaguardia delle infrastrutture critiche della nazione dalle minacce fisiche e informatiche che possono influenzare la difesa nazionale, la sicurezza pubblica e la prosperità economica è il *Department of Homeland Security*, costituito nel 2001[137].

Al tal scopo al suo interno opera la *National Cyber Security Division* (NCSD), l'agenzia specificatamente preposta alla protezione delle reti e delle attività informatiche della nazione. Essa collabora sia con il pubblico sia con il

[136] Even Shmuel, Siman David-Tov, *Cyber Warfare*, cit., pp. 55-56.
[137] http://www.dhs.gov/topic/cybersecurity.

privato, nonché con svariati enti della comunità internazionale. Si occupa di prevedere i rischi e i pericoli dei programmi informatici, della prevenzione degli stessi nonché delle *best practice* e delle procedure da seguire in caso di eventi inusuali. Inoltre si occupa del coordinamento e della condivisione di informazioni tra il settore privato, gli istituti e le agenzie statali ed in ultimo monitora le attività ostili.

Quest'ultima attività, in particolare, è svolta in stretta cooperazione con il *Cyber Command* (CYBERCOM) del Dipartimento della Difesa (DoD), costituito nel maggio 2010, il quale che si occupa non solo delle attività informatiche difensive ma anche di quelle offensive. In sintesi, esso ha la missione di ridurre le minacce alla sicurezza nazionale e di assicurare la libertà nell'utilizzo del cyberspazio. Le attività da esso svolte si focalizzano su una serie di obiettivi quali: la protezione di tutte le reti militari; la creazione di una singola catena di comando che riguardi le decisioni relative alla *cyber war* (che va dal Presidente degli Stati Uniti alla singola unità militare); la creazione di partnership con elementi esterni al Dipartimento della Difesa (incluso il settore privato) e fuori dai confini nazionali per la condivisione di informazioni sulle minacce; assicurare una rappresentanza militare nel cyberspazio che possa fungere da punto di riferimento per gli altri rami della difesa nonché per le compagnie americane all'estero.

Un ruolo essenziale per la protezione del cyberspazio, ovviamente, è svolto anche dall'*intelligence* statunitense (IC), la cui comunità è composta da una serie di agenzie governative (in tutto 16), tra le quali la *Defense Intelligence Agency* (DIA) del Dipartimento della Difesa, la *National Security Agency* (NSA) e la *Central Intelligence Agency* (CIA)[138]. Il documento strategico del 2009 dimostra come attualmente il rafforzamento delle capacità informatiche rientra tra i cinque compiti più importanti di cui debbono occuparsi le agenzie di intelligence americana ognuna nelle rispettive aree di competenza[139].

[138] http://www.dni.gov/index.php/intelligence-community/members-of-the-ic#dia.

[139] Director of National Intelligence, *The National Intelligence Strategy of the USA*, Agosto 2009, MO 5 -Enhance Cyb ersecurity, p. 9, disponibile su http://www.dni.gov/index.php/newsroom/reports-and-publications/165-reports-publications-2009: *"The Intelligence Community plays an integral role in enhancing cybersecurity both by increasing our ability to detect and attribute adversary cyber activity and by expanding our knowledge of the capabilities, intentions, and cyber vulnerabilities of our adversaries. The IC has made progress in implementing the initiatives and developing the enabling capabilities needed to meet national cybersecurity guidance. We must quickly add to these efforts through the following: • Leverage partnerships. Integrate cyber expertise throughout the IC, as well as with allied intelligence services, industry, and the academic community. • Protect U.S. infrastructure. Identify, prioritize, and close the gaps in our collection capability and analytic knowledge base on threats to our cybersecurity.• Combat cyber threats to non-traditional targets. Focus more resources on identifying and neutralizing cyber threats to non-traditional intelligence customers. • Manage the cyber mission. Strengthen Community-wide processes for mission management, specifically*

Da tutto ciò, emerge il fatto che, rispetto agli altri paesi, gli USA considerano particolarmente importante il settore della protezione informatica e ne predispongono una protezione olistica che coinvolge ogni singola forza della nazione.

Inoltre, dai documenti analizzati traspare la natura essenzialmente difensiva della strategia americana. Tuttavia, una eventuale battaglia nel *cyberspazio*, così come ventilata dalle attività preparatorie del Dipartimento della Difesa, comporterebbe ovviamente anche attività offensive. Ad oggi, sembra che gli Stati Uniti abbiano un considerevole vantaggio sugli altri paesi in termini di capacità offensive e presenza nel cyberspazio. Perciò è ragionevole presumere che le attività offensive siano parte integrante della strategia americana, intese non soltanto come risposta ad attacchi ostili, ma anche come vere e proprie attività offensive isolate, nonostante queste ultime non siano state palesemente previste né nei documenti strategici né da nessun alto funzionario (anzi sono ufficialmente negate) e che si concretizzino ad es. in attacchi informatici preventivi non rivendicati (come nel caso Stuxnet).

V. La strategia NATO

Sebbene la Nato abbia da sempre protetto i propri sistemi di comunicazione e di informazione, la difesa informatica vera e propria è stata inserita nell'Agenda politica dell'Alleanza per la prima volta nel vertice di Praga del 2002, a seguito degli attacchi subiti dalle organizzazioni Nato e dai paesi alleati durante l'operazione "Allied Force"[140]. L'elemento più importante del *Cyber Defence Program* adottato nella capitale ceca è stato la creazione dell'NCIRC (*Nato Computer Incident Reponse Capability*), il primo strumento in assoluto che l'Alleanza ha messo in piedi per prevenire, individuare e rispondere ai cyber attacchi.

Successivamente i leader alleati hanno ribadito la necessità di fornire una protezione aggiuntiva ai sistemi informatici, come testimoniato dal vertice di Riga del 2006.

Ma solo a seguito degli eventi estoni del 2007 (analizzati nel capitolo precedente), che hanno svelato la reale portata tecnica e le implicazioni politiche di eventuali attacchi informatici, l'esperienza Nato nell'approccio alla *cyber security*

processes for enabling collaborative planning and execution and for providing a scalable, foundational capability to conduct cyber operations".

[140] Questi attacchi, inclusi *denial of service* e *defacement* della pagina web del Quartier generale supremo delle Potenze Alleate in Europa, sono stati svolti da attivisti serbi, russi e cinesi nel 1999 per costringere le unità militari serbe a uscire dal Kosovo.

trova piena maturazione. Nel Summit di Bucharest del 2008[141] gli ufficiali Nato hanno dimostrato la consapevolezza dell'importanza di rafforzare i sistemi informatici, di creare una politica adeguata in materia di sicurezza cibernetica e di sviluppare strutture ed autorità specificatamente competenti.

La Dichiarazione di Bucharest ha prodotto due importanti risultati: uno operativo e uno strategico.

Il primo consisteva nella creazione del CDMA (*Cyber Defence Management Authority*). Esso era un organo che aveva sede a Brussels e che rappresentava la volontà di centralizzare le capacità di difesa informatica e di monitoraggio all'interno dell'Alleanza. Al contempo aveva il compito di aiutare i paesi membri a perfezionare le proprie capacità difensive. Le sue funzioni sono state delegate successivamente a un altro organo.

Il secondo prodotto del Summit è il centro di ricerca di Tallinn, il *Cooperative Cyber Defence Centre of Exellence* (CCD CoE), che ha dato vita al c.d. *Tallinn Manual*, analizzato nel corso della III parte di questo volume.

Mentre il CDMA era incaricato soprattutto di coordinare le operazioni informatiche difensive, il CCD CoE non ha compiti operativi. Piuttosto si occupa di sviluppare la dottrina Nato (in particolare quella giuridica) in materia, di condividerne la conoscenza e di istruire e formare il personale. Quest'ultimo centro ha programmato e continua a programmare una serie considerevole di eventi, incontri e workshop al fine di raccogliere opinioni provenienti sia dal settore pubblico sia da quello privato presenti all'interno e all'esterno dei paesi alleati.

Inoltre, dal 2008 nell'agenda Nato ha guadagnato un posto preminente l'idea di una partnership globale per la protezione informatica formata dal contributo alle missioni e alle operazioni Nato proveniente anche da paesi terzi e dalle organizzazioni internazionali come l'Unione Europea. Secondo la strategia Nato, infatti, un partenariato siffatto può giocare un ruolo essenziale nella protezione nella difesa dei paesi alleati, data la natura transnazionale della guerra informatica. Per questo motivo, vengono continuamente promosse esercitazioni che simulano attacchi provenienti da paesi esterni all'Alleanza, che possono essere sventati o limitati unicamente con la stretta cooperazione tra paesi di estrazione globale. Periodicamente, infatti, verso la fine dell'anno viene effettuata un'attività denominata *Cyber Coalition Exercise* (la sua sigla è CC, cui viene affiancato il numero dell'anno corrente), la quale offre una buona opportunità di esercitare le procedure di gestione delle crisi e di condivisione delle informazioni.

La strategia Nato prevede anche lo sviluppo di intensi legami con attori non-statali, come le corporazioni (Microsoft; Google; IBM; ecc.) e i gruppi no-profit

[141] Si veda *Bucharest Summit Declaration* reperibile al sito http://www.nato.int/cps/en/natolive/official_texts_8443.htm.

(International Standards Organization – ISO; Internet Engineering Task Force – IETF), i quali posseggono molti dei mezzi necessari per contrastare le minacce informatiche. Per questo motivo la partnership con l'industria privata è considerata vitale. A tal proposito il *Nato Industrial Advisory Group* (NIAG)[142] fornisce periodicamente rapporti, caratterizzati da un punto di vista industriale, su come un partenariato Nato/industria può essere realizzato.

Successivamente, il concetto difensivo strategico adottato a Lisbona nel 2010 ha evidenziato la necessità di *"sviluppare ulteriormente la…capacità di prevenire, individuare, difendersi e riprendersi da attacchi informatici…"*.

Così, l'8 giugno 2011, mentre la Nato conduceva le operazioni aeree sulla Libia, è stata adottata una nuova strategia di difesa informatica con un Piano di Azione associato in corso di attuazione che ha implementato le attività esistenti e ha previsto nuove procedure. Quindi, oltre a reiterare l'importanza della protezione dei network Nato nei singoli punti analizzati sopra, si specifica che ogni azione di risposta collettiva è soggetta alla decisione da parte del Consiglio Nord Atlantico, l'organo decisionale più importante dell'organizzazione. Per tale motivo è previsto che il Consiglio Nord Atlantico debba essere tempestivamente informato di ogni attacco, esercitazione o decisione assunta a livello nazionale. La Nato, infatti, anche nel caso degli attacchi cibernetici, non ha previsto nessun tipo di risposta standard e perciò mantiene una sorta di **flessibilità decisionale** nelle azioni che, di volta in volta, possono o non possono essere prese. E' molto improbabile, tuttavia, che il Consiglio Nord Atlantico possa invocare la difesa collettiva ex art. 5 del Patto Atlantico se non ci sono stati danni significativi e/o decessi, pari a quelli causati dalla forza militare cinetica.

Questo quadro favorisce il principio secondo il quale la protezione primaria delle infrastrutture critiche nazionali da parte della Nato non è automatica, ma rimane responsabilità dei singoli stati. La priorità della Nato consiste nell'aiutare gli Alleati nei loro sforzi per costruire le difese informatiche attraverso lo scambio di informazioni di buone pratiche e conducendo esercitazioni al fine di sviluppare le competenze necessarie per gestire la relativa tecnologia. Inoltre provvede a sviluppare principi e criteri che garantiscano un livello minimo comune di sicurezza.

Il processo di implementazione della difesa informatica nord atlantica passa poi dall'integrazione, in conformità con il mandato di Lisbona del 2010, di tale obiettivo all'interno del *Nato Defence Planning Process* (NDPP)[143] e, ultimamente,

[142] Il NIAG, formato nel 1968, è un organo consultivo di alto livello composto da industriali dei paesi membri della Nato, che agisce sotto la *Conferenza dei direttori nazionali degli armamenti* (CNAD), e svolge un ruolo importante nel consigliare il CNAD su questioni chiave in materia di politica di cooperazione, sviluppo, produzione e fornitura degli armamenti ed equipaggiamenti militari.
[143] Si veda cos'è l'*NDPP*, al link http://www.nato.int/cps/en/natolive/topics_49202.htm.

anche all'interno dell'iniziativa *Smart Defence*[144], approvata al successivo vertice di Chicago 2012.

A livello operativo, l'attuale struttura organica è molto articolata.

Come detto, ogni risposta difensiva collettiva è soggetta alle decisioni del Consiglio Nord Atlantico, che pertanto si pone al vertice della **cyber defence governance**.

Il compito di coordinare la difesa informatica tra gli organi militari e civili che collaborano con la Nato spetta, invece, al *Cyber Defence Management Board* (CDMB), che ha sostituito il CDMA. Il CDMB costituisce il principale organo di governo della Nato per la difesa informatica. Comprende rappresentanti politici, militari e operativi nonché personale dello staff tecnico ed opera sotto l'egida dell'*Emerging Security Challenges Division in Nato HQ*.Il suo lavoro è monitorato dal DPPC(R) (*Defence Policy and Planning Committee in Reinforced format*), il quale gestisce il processo di pianificazione generale della difesa della Nato, comprese ovviamente le capacità informatiche. In qualità di garante, accerta che la strategia di difesa informatica e il Piano d'Azione stiano ricevendo le attenzioni e i finanziamenti adeguati da parte della Nato e dei suoi membri.

L'NC3 (*Nato Consultation, Control and Command*), invece, costituisce l'organo principale di consultazione sugli aspetti tecnici e di implementazione di difesa informatica.

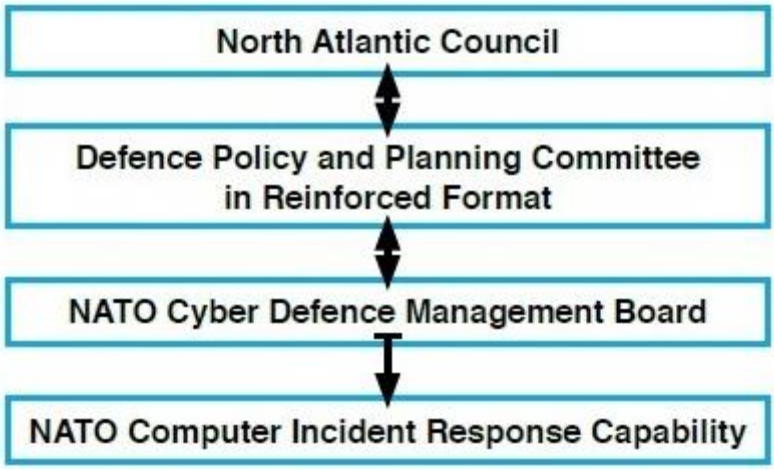
Le autorità militari della Nato (NMA) e l'*Agenzia Nato di comunicazione e informazione* (NCI o NCSA) hanno la responsabilità di identificare i requisiti operativi necessari nonché l'acquisizione, l'implementazione e la gestione delle capacità informatiche di difesa, nelle rispettive aree di competenza.

L'NCI, insieme con il Centro Tecnico *Nato Computer Incident Response Capability* (NCIRC), è anche responsabile della fornitura di servizi tecnici e operativi di sicurezza informatica in tutta la Nato. Con la sigla NCIRC si indica una capacità funzionale su due livelli: da una parte vi è il suddetto Centro Tecnico che costituisce la capacità tecnico-operativa principale della Nato e ha un ruolo chiave nel rispondere a qualsiasi incidente e/o aggressione informatica. Esso costituisce, altresì, un mezzo per la gestione e il resoconto degli incidenti/attacchi e la diffusione di informazioni correlate agli stessi. Dall'altra parte vi è il Centro di Coordinamento NCIRC, che ha sede a Brussels ed è responsabile del coordinamento delle attività di difesa informatica in seno alla Nato e con i paesi

[144] *"Smart defence"* è un nuovo modo di pensare per generare le moderne capacità di difesa di cui l'Alleanza ha bisogno per il prossimo decennio e oltre. Si tratta di una rinnovata cultura della cooperazione che incoraggia gli alleati a cooperare tra loro per sviluppare, acquisire e mantenere le capacità militari al fine di svolgere al meglio i compiti fondamentali che l'Alleanza ha concordato nel proprio concetto strategico. Ciò significa mettere in comune e condividere le capacità, le risorse, stabilire le priorità e coordinare meglio gli sforzi. V. su: http://www.nato.int/cps/en/natolive/topics_84268.htm?.

membri, sostiene il CDMB, pianifica le esercitazioni annuali e si occupa della gestione dei legami con le organizzazioni internazionali come l'UE, l'OSCE e l'ITU (United Nations/International Telecommunication Union).

Figura n. 7 – Cyber Defence Governance in NATO



Fonte: www.nato.int

Nonostante gli sforzi compiuti sinora, la discussione su come la Nato potrebbe facilitare ulteriormente questo sforzo collettivo e su che tipo di sostegno potrebbe ulteriormente fornire agli alleati non è diminuita.

Le alte cariche della Nato rimangono convinte della necessità di implementare notevolmente gli sforzi dell'Alleanza nello sviluppo di un sistema difensivo ancora più efficiente. Gli eventi di questo secolo hanno dimostrato la vulnerabilità delle strutture civili e militari di fronte agli attacchi cibernetici. Anche se finora, soltanto in pochi hanno dimostrato di possedere le abilità per distruggere o degradare i sistemi di controllo Nato, è ipotizzabile che le strategie offensive comprenderanno la sempre più manifesta possibilità di ricorrere a tattiche informatiche, cui seguirà pertanto un'innovazione tecnica delle strumentazioni. Di fronte a tale ipotesi, la Nato non può rischiare di restare indietro. Da questo punto di vista, quello che preoccupa maggiormente, è il crescente gap tecnico tra gli Stati Uniti e i suoi Alleati Europei, cui si richiede pertanto uno sforzo ulteriore per mantenere il passo.

VI. Considerazioni conclusive

La presente analisi fornisce una breve istantanea delle modalità con le quali le minacce cibernetiche vengono affrontate. Dalla lettura delle fonti, per quanto si sia cercato di presentare summa chiara e definita delle strutture dedite alla cyber security e dei relativi compiti, l'elemento predominante in tutti i documenti analizzati è un'elevata genericità ed astrattezza, che rasenta la confusione, laddove sembra sussistere anche una sovrapposizione di ruoli e di competenze.

Non è ben chiaro, in altre parole, di cosa debbano precisamente occuparsi gli enti citati né in che modo debbano collaborare tra loro.

Inoltre, si evince la probabile inesistenza di una "mappatura" completa e dettagliata, da parte degli enti preposti alla sicurezza informatica, degli obiettivi sensibili che potrebbero essere oggetto di attacchi.

Questa carenza rischia di rendere eccessivamente gravoso il compito di tali enti, al punto tale da rendere le loro attività di prevenzione e contrasto inutili e insufficienti.

Per quanto limitati, i dati immessi nelle reti informatiche sono spaventosamente grandi in termini informatici, richiedono spazi di archiviazione e risorse tecniche per la gestione ed il monitoraggio che non passano certo inosservati, né come grandezza fisica né come budget.

Pertanto, è necessario stabilire su quali obiettivi concentrare le risorse umane, tecniche e finanziarie a propria disposizione per garantire almeno negli ambiti più sensibili un grado di sicurezza più elevato.

GLOSSARIO

Antivirus: utility che cerca virus per eliminarli dalla memoria di massa (scansione dell'hard disk, floppy disk, etc.) e dalla memoria principale (RAM) di un computer.

Backup (sistema di): Il backup è l'operazione che permette di creare una copia dei dati su un supporto esterno per motivi di sicurezza. Scopo dell'operazione è il recupero dei dati che potrebbero essere stati persi a seguito di un errore, di un incidente o di un attacco dall'esterno (virus o altro malware).

Bit: è l'unità di misura dell'informazione (dall'inglese *"binary information unit"*), definita come la quantità minima di informazione che serve a discernere tra due possibili eventi equiprobabili.

Botnet: è una rete formata da computer collegati ad Internet e infettati da malware, controllata da un'unica entità, il *botmaster*.

Cloud computing: o *nuvola informatica*, indica un insieme di tecnologie che permettono, sotto forma di un servizio offerto da un provider al cliente, di memorizzare/archiviare e/o elaborare dati (tramite CPU o software) grazie all'utilizzo di risorse hardware/software distribuite e visualizzate in rete (es. Dropbox).

Computer network attack – CNA: operazioni finalizzate a disturbare, negare, degradare, distruggere le informazioni contenute all'interno di computer o reti di computer, o i computer e le reti stesse.

Counter-hacking: è una azione di contrasto alle operazioni di hacking (v. definizione).

Computer network defence – CND: azioni intraprese per proteggere, monitorare, analizzare, rilevare e rispondere alle attività non autorizzate all'interno di sistemi informativi e di reti informatiche.

C**omputer network exploitation** – CNE: operazioni di intelligence atte a permettere la raccolta di dati da un sistema informativo automatizzato o da una rete bersaglio o di un avversario.

Crimeware: è un software maligno installato di nascosto sui computer degli utenti. Il crimeware può presentarsi sotto forma di virus, Trojan o altro malware.

Cyberlaundering:è il riciclaggio elettronico di proventi illeciti.

Dominio: nel Domain Name System (DNS) è una parola singola oppure un'abbreviazione che corrisponde a un livello di responsabilità nell'attribuire nomi a host e gruppi subordinati. Esiste un dominio nazionale (Dominio geografico), di solito coordinato da enti senza fini di lucro che assegnano i nomi e registrano quelli assegnati. Esistono poi domini aziendali all'interno dei quali si trovano molteplici computer e sottodomini sotto la responsabilità di uno o più amministratori locali.

Domain Name System; è un sistema di denominazione del dominio, realizzato nel 1983 da Paul Mockapetris e Jonathan Bruce Postel (v. IANA[145]). E' un database distribuito che viene utilizzato in ambiente TCP/IP per creare una corrispondenza tra indirizzo numerico e nome mnemonico assegnato alla macchina. E' distribuito perché nessuno dei computer collegati ad Internet ha una visione completa dell'intera rete, ma deve usare il particolare protocollo previsto dal DNS per comunicare con gli altri sistemi e procurarsi le informazioni. La definizione dei nomi per i vari domini segue una struttura gerarchica ad albero rovesciato, partendo dal generale per scendere nel particolare. In questo modo è possibile delegare a livello locale parte del controllo della rete, seguendo un approccio Client/Server (il gestore di un particolare dominio può determinare in modo indipendente i nomi e gli indirizzi delle risorse che saranno disponibili all'interno di quel dominio). Ogni computer collegato ad Internet dispone di un proprio indirizzo che viene letto e utilizzato dal protocollo di comunicazione Internet Protocol (IP) per convogliare pacchetti di dati da una macchina all'altra. Ad ogni macchina e ad ogni utente, tuttavia, viene anche assegnato un nome distintivo e univoco, tale nome viene poi attribuito a un particolare dominio di appartenenza. Ad esempio l'indirizzo commerciale@info-2000.it indica che l'ufficio commerciale è identificato presso una macchina chiamata info-2000 che fa parte di un dominio geografico Italia. Le indicazioni di corrispondenza tra i nomi delle reti, dei gateway (router) e degli host con i relativi indirizzi IP vengono memorizzati all'interno di un file che si chiama hosts.

DDoS: è la sigla di *distributed denial of service*, letteralmente *negazione del servizio*. Si tratta di un attacco informatico in cui si cerca di portare il funzionamento di un sistema informatico che fornisce un servizio, ad es. un sito

[145] IANA è l'acronimo di *Internet Assigned Number Authority*. Organizzazione nata nel 1988 ed amministrata da Jon Postel e Joyce K. Reynolds, con sede presso l'*University of Southern California's Information Sciences Institute*. Il nome viene presentato formalmente nel 1990 nell'RFC 1060. IANA si occupa dell'assegnazione univoca dei numeri IP (Internet), dei numeri di porta e di protocollo, delle versioni del TCP e UDP, nonchè delle informazioni sui domini di primo livello (TLD). Dal 1998 è un dipartimento dell'ente governativo ICANN (*Internet Corporation for Assigned Names and Numbers*).

web, al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più capace di erogare il servizio.

e-Government: o Amministrazione digitale (a volte anche governo elettronico o e-gov) è il sistema di gestione digitalizzata della pubblica amministrazione, il quale, unitamente ad azioni di cambiamento organizzativo, consente di trattare la documentazione e di gestire i procedimenti con sistemi informatici, grazie all'uso delle tecnologie dell'informazione e della comunicazione (TIC), allo scopo di ottimizzare il lavoro degli enti e di offrire agli utenti (cittadini ed imprese) sia servizi più rapidi, che nuovi servizi, attraverso, ad esempio, i siti web delle amministrazioni interessate.

Exploit kit: metodo che, sfruttando un bug o una vulnerabilità, porta all'acquisizione di privilegi o al Diniego di Servizio (DoS) di un computer. L'exploit viene generalmente sfruttato per ottenere l'accesso ad un sistema protetto e, una volta acquisiti i privilegi amministrativi, l'obiettivo è quello di installare servizi, aprire porte o semplicemente creare utenti per entrare nel sistema in modo più agevole.

Firewall: è, come suggerisce il suo nome, un sistema progettato per impedire accessi non autorizzati a (e da) reti private. Esso può essere realizzato sia via software sia via hardware (o anche con una combinazione delle due). Il suo utilizzo tipico è quello di impedire agli utenti provenienti da Internet l'accesso non autorizzato ad una Intranet.

Hacker: è un individuo che possiede una approfondita conoscenza dei computer, dei sistemi elettronici e delle reti di computer. Il termine può avere un'accezione sia positiva sia negativa. Nel primo caso si identifica una persona completamente assorbita dalla programmazione e nella tecnologia informatica o interessata ad esaminare il codice dei sistemi operativi e di altri programmi per capirne il funzionamento. Nel secondo caso, il termine è utilizzato impropriamente da mass media per indicare una persona, comunemente definita come "pirata informatico", che tenta di forzare i sistemi di protezione dei sistemi computerizzati per estrarre illegalmente informazioni o causare danni informatici. In quest'ultimo caso sarebbe opportuno utilizzare il termine "cracker".

Hacking: è l'atto di penetrare in un sistema per guadagnare conoscenze su di esso e su come questo lavora.

Hardware: termine generico per indicare le componenti fisiche (devices) di un elaboratore, quali i circuiti elettronici, chip, schede, disk drive, stampante, mouse,

lettori CD-ROM, monitor, tastiera etc. Si contrappone al software che è la parte logica del computer.

Informazione: un'informazione è una coppia costituita: *da una rappresentazione materiale* (che ne costituisce il formante); *da un insieme di interpretazioni* (che ne costituisce il formato), la cui natura, evenemenziale, consiste in un cambiamento di stato che, tramite l'occorrenza di tale rappresentazione materiale, provoca l'attivazione del corrispondente campo interpretativo, secondo le regole fissate da un codice prestabilito. Georges Ifrahm, *Enciclopedia universale dei numeri*, p.1469.

Internet: (contrazione della locuzione inglese interconnected networks, ovvero "reti interconnesse") rete mondiale di reti di computer ad accesso pubblico, attualmente rappresentante il principale mezzo di comunicazione di massa, che offre all'utente una vasta serie di contenuti potenzialmente informativi e servizi.

Malware: insieme di programmi che espongono il PC a rischi sia in fatto di privacy sia di funzionamento del sistema operativo, si trasmettono via internet attraverso la posta elettronica o la semplice navigazione sfruttando le porte aperte del computer analogamente o congiuntamente ai worms. In questa categoria rientrano sicuramente virus, dialers, tracking cookies, ecc.

Peer to peer: Architettura di rete decentrata che si sviluppa tra i vari host (detti *Peer* – nodi) che si collegano tra loro. I network P2P vengono solitamente utilizzati per la comunicazione tra utenti (*Instant Messaging*) e la condivisione di risorse (*file sharing*).

Pharming*:* è una tecnica di cracking utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri dati sensibili, come numero di conto corrente, nome utente, password, numero di carta di credito, ecc.

Phishing: è un tipo di truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili. Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale, attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica di siti bancari o postali.

Ransom: è un tipo di malware (software dannoso) installato illegalmente su un computer, senza autorizzazione. Tramite il *ransomware* i criminali riescono a

bloccare il computer in remoto; a questo punto si apre una finestra popup che richiede il pagamento di una somma di denaro per sbloccarlo.

Server: con questo termine (dall'inglese, letteralmente *servitore*), si indica genericamente un componente o sottosistema informatico di elaborazione che fornisce, a livello logico o a livello fisico, un qualunque tipo di servizio ad altre componenti (tipicamente chiamate *client*, cioè "cliente") che ne fanno richiesta attraverso una rete di computer, o all'interno di un sistema informatico o direttamente in locale su un computer.

Social engineering: questa espressione definisce la tecnica di manipolare gli individui al fine di aggirare i dispositivi di sicurezza. Consiste, cioè, nell'ottenere informazioni sensibili da parte degli utenti attraverso comunicazioni telefoniche, posta elettronica e tradizionale o per contatto diretto. Si basa quindi basata sulla persuasione e sullo sfruttamento dell'ingenuità e le debolezze degli utenti.

Software: termine generico per indicare i programmi eseguibili dal calcolatore (computer). Un programma è costituito da un insieme di istruzioni e dati. Il software di sistema è quello utilizzato dal sistema operativo. Invece il programma utilizzato direttamente dall'utente, si indica col termine applicazione.

Spam: descrive l'uso abusivo della tecnologia legata alla posta elettronica, chat, tag board, forum, social network al fine di intasare gli account degli utenti attraverso messaggi indesiderati.

Spear fishing: è nuova categoria di minaccia phishing, che si distingue per essere più mirata perché sfrutta le informazioni disponibili su un utente-obiettivo per rendere gli attacchi maggiormente specifici e "personali". I messaggi email di questo tipo, per esempio, possono rivolgersi alla vittima adoperandone nome, carica o posizione, anziché usare titoli generici come accade nelle campagne di phishing generalizzate. Obiettivo dell'azione è catturare l'attenzione di un determinato individuo, spingendolo ad aprire un allegato pericoloso o a cliccare su un link dannoso.

Spoofing: è un tipo di attacco informatico dove viene impiegata la falsificazione dell'identità (*spoof*).

Spyware: contrazione di spy (ingl., spia) e software. Software che installato su una macchina, invia a terzi, tramite Internet informazioni relative all'utente, a sua insaputa.

Virus informatico: programma dotato di una certa autonomia operativa, capace di replicarsi e di alterare il funzionamento del computer. I virus possono modificare e danneggiare il sistema operativo, o singole applicazioni, ad esempio cancellando file. Possono restare inerti anche per un periodo predefinito.

Virus "benigni": sono virus informatici che si limitano a generare suoni, colori, messaggi o spostamenti di file.

WiMAX (Worldwide Interoperability for Microwave Access): è una tecnologia ed uno standard tecnico di trasmissione che consente l'accesso di tipo wireless a reti di telecomunicazione a banda larga.

Worm: ingl. lett., Verme, è un file in grado di autoreplicarsi all'interno di un sistema per un numero indefinito di volte – rallentandolo o portandolo anche fino al crash – e quindi di ritrasmettersi ad altri computer attraverso posta elettronica. Taluni di questi non fanno altro che creare un'infinita "catena di Sant'Antonio" senza ulteriori disturbi, altri possono arrecare danni ingenti ai sistemi informatici non protetti, e violarne comunque la privacy.

BIBLIOGRAFIA

Articoli ♦ Monografie ♦ Periodici ♦ Tesi di laurea:

- BLANK LAURIE R., *International Law and Cyber Threats from Non-State Actors*, Emory Public Law Research Paper No. 12-234, Emory University School of Law, Atlanta, 2012;
- BROWN DAVIS, *A Proposal for an International Convention to Regulate the Use of Information System in Armed Conflict*, 47 Harv. Int'l L.J., 179, 2006;
- BUONOMO VINCENZO, *Il Diritto della Comunità Internazionale*, Lateran University Press, Città del Vaticano, 2010;
- ANTONIO CASSESE, *The International Community's 'Legal' Response to Terrorism*¸ in 38 INT'L & COMP. L. Q., 1989, pagg. 589 – 597;
- CENCETTI CLAUDIA, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, Quaderni IAI, Edizioni Nuova Cultura, Roma, 2014;
- CLARKE RICHARD, *Cyber war*, Harper-Collins, New York, 2010;
- CONFORTI BENEDETTO, *Diritto Internazionale*, Editoriale Scientifica, Napoli, 2006;
- CONFORTI BENEDETTO, FOCARELLI CARLO, *Le Nazioni Unite*, Cedam, VIII ed., Verona, 2011;
- DAVID, *Portée et limite du principe de non-intervention,* in "Revue Belge de Droit International"*,* 1990;
- DI CAMILLO FEDERICA, MIRANDA VALÈRIE VICKY, FELICIAN STEFANO, *Cyber-security: Europa e Italia*, in "Osservatorio di politica internazionale" n. 32 – maggio 2011;
- DROEGE CORDULA, *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*, in "International Review of the Red Cross, June 2012 – Vol. 94, No 886 – New technologies and warfare", pp. 533 – 578, Published online by Cambridge University Press, 05/06/2013;
- ENEKEN TIKK, KADRI KASKA, LIIS VIHUL, *International Cyber Incidents*, Cooperative Cyber Defence Centre of Exellence (CCD COE), Tallinn, 2010;
- ENISA, *National Cyber Security Strategies. Setting the course for national efforts to strenghthen security in cyberspace*, Heraklion, 2012;
- EVEN SHMUEL, SIMAN DAVID-TOV, *Cyber Warfare: Concepts and Strategic Trends*, INSS - Memorandum 117, Tel Aviv, 2012;
- GRAY JHON, *Al Qaeda e il significato della modernità*, Fazi Editore, Roma, 2004;
- GRECO EMANUELE, *Sicurezza dei minori e violenza massmediale. Il diritto ad avere diritti*, Biblioteca Archivio Disarmo, Roma, 2013;

- GRECO EMANUELE, MALATESTA EMANUELA, *Violazione dei diritti umani nei conflitti armati internazionali. Il caso dei bambini soldato e della violenza di genere*, Gruppo CEDUR, Roma, 2013;
- HEALEY JASON, VAN BOCHOVEN LEENDERT, *NATO's Cyber Capabilities: Testerday, Today, and Tomorrow*, in Atlantic Council, ISSUEBRIEF, Washington, 2012;
- HEATHER HARRISON DINNIS, *Cyber Warefare and the Laws of War*, in "Cambridge studies in international and comparative law", Cambridge University Press, Cambridge and New York, 2012;
- HOLLIS, DUNCAN B., *Why States Need an International Law for Information Operations*, in 11(4) "Lewis & Clark L. Rev." 1023, 2007;
- HUGHES REX B., *NATO and Cyber Defence. Mission Accomplished?*, in "Atlantisch Perspectief" n° 1/2009, pag, 4;
- IFRAH GEORGES, *Enciclopedia universale dei numeri*, Milano, Arnoldo Mondadori Editore S.p.A., 2008;
- LAUTERPACHT HERSCH, *Oppenheim's Intnational Law*, Longmans, Green & Co, VII ed., Londra, 1952;
- LIN HERBERT, *Cyber conflict and international humanitarian law*, in "International Review of the Red Cross, June 2012 – Vol. 94, No 886 – New technologies and warfare", pp. 515 – 531, Published online by Cambridge University Press, 01/05/2013;
- MARCHETTI ESTHER, *Private Military and Security Companies: il caso italiano nel contesto internazionale*, Quaderni IAI, n. 7 Edizioni Nuova Cultura, Roma, 2013;
- MELZER NILS, *Cyberwarfare and International Law*, UNIDIR Resources, Ideas For Peace And Security, Ginevra, 2011;
- NIGRO RAFFAELLA, *La nozione di terrorismo nel diritto internazionale*, Università degli suti di Napoli Federico II, Facoltà di Giurisprudenza, Tesi di dottorato in diritto internazionale, XVII ciclo, 2006;
- OLIMPIO GUIDO, *La testa del serpente. Tutti i segreti di Osama Bin Laden,* Istant book Corriere della Sera n.32 del 25/01/2010;
- SCHMITT MICHAEL N., *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 Col. J. Trans. L., 1999, p. 885;
- SCHMITT MICHAEL N., *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, "Harvard International Law Journal", Volume 54, Harvard, 2012;
- SCHMITT MICHAEL N. (a cura di), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Tallinn, 2013;

- ROSCINI MARCO, *World Wide Warefare – Jus ad bellum and the Use of Cyber Force*, in Armin Bogdany and Rudiger Wolfrum (eds), *"Max Planck Yearbook of United Nations Law"*, vol. 14, 2010;
- SCAGNETTI GIANLUCA, *La geostrategia nel cyberspazio*, in in "RID – Rivista Italiana Difesa" n. 7, p. 45, 2013;
- SHARP WALTER G., *Cyberspace and the Use of Force*, Aegis Research Corp., Falls Church, Virginia, 1999;
- SIMONCELLI MAURIZIO, *Dove i diritti umani non esistono più. La violazione dei diritti umani nelle guerre contemporanee*, Ediesse, Roma,2010;
- SIMONCELLI MAURIZIO (a cura di), *La pace possibile. Successi e fallimenti degli accordi internazionali sul disarmo e sul controllo degli armamenti*, Ediesse, Roma, 2012;
- SIPRI YEARBOOK, *Armaments, Disarmament and International Security,* Oxford University Press, Oxford, 2011 e 2012;
- TALLARICO RENATA, *La definizione di conflitto armato nel diritto internazionale umanitario*, CORSO DI DOTTORATO DI RICERCA IN DIRITTO INTERNAZIONALE E DELL'UNIONE EUROPEA CICLO XXIII, Università degli Studi di Macerata, 2011;
- VIGNARCA FRANCESCO, *Mercenari S.P.A.*, BUR Futuropassato, Milano, 2004;
- VISMARA LUCA FRANCESCO, *Il cyber-terrorismo esiste o non esiste?*, in "Eurasia Rivista di Studi Geopolitici", 2012;

Casi giurisprudenziali:

- *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda),* Judgment, I.C.J. Reports 2005;
- *Case Concerning Militarv and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America).* Merits, Judgment. I.C.J. Reports 1986;
- *Legality of the threat or use of nuclear weapons*, Advisory opinion, I.C.J. Report 1996;
- *Oil Platforms (Islamic Republic of Iran v. United States of America)*, Judgment,I. C. J. Reports 2003, p. 161;

Dichiarazioni ♦ Risoluzioni ♦ Trattati:

- *Carta delle Nazioni Unite*, 1945;

- *Convenzione del Consiglio d'Europa sulla criminalità informatica*¸ n. 185, Budapest, 2001;
- *Convenzioni di Ginevra*, Ginevra, 1949;
- *Creation of a global culture of a cyber security and the protection of critical information infrastructure*, Risoluzione dell'Assemblea Generale ONU 58/199 del 30 gennaio 2004;
- *Dichiarazione relativa ai principi di diritto internazionale riguardanti le relazioni amichevoli e la cooperazione tra gli Stati conformemente alla Carta delle Nazioni Unite*, Ris. 2625 (XXV) 24 ottobre 1970;
- *Dichiarazione di San Pietroburgo*, 1868;
- Risoluzione del Consiglio di Sicurezza ONU n. 1368, 12 settembre 2001;
- *Trattato Nord Atlantico*, Washington, 4 aprile 1949;
- *Trattato sull'Unione Europea* (TUE) *e sul funzionamento dell'Unione Europea* (TFUE) [Versione Consolidata];
- *I e II Protocollo Aggiuntivo alle Convenzioni di Ginevra*, Ginevra, 1977;

Documenti ufficiali:

- COMMISSIONE EUROPEA, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final, Brussels, 07/02/2013;
- COMMISSIONE EUROPEA, *Achievements and next steps: towards global cyber-security*, COM(2011)163, Brussels, 31/05/2011;
- COMMISSIONE EUROPEA, *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, COM(2010) 673, Brussels, 22/11/2010;
- COMMISSIONE EUROPEA, *Proteggere le infrastrutture critiche informatizzate. Rafforzare la preparazione, la sicurezza e la resilienza per proteggere l'Europa dai ciber attacchi e dalle ciber perturbazioni* (CIIP), COM(2009)149, Brussels, 2009;
- COMMISSIONE EUROPEA, *Network and Information Security: Proposal for A European Policy Approach* (NIS), COM(2001)298, Brussels, 2001;
- CONSIGLIO EUROPEO, *Conclusioni*, EUCO 217/12, 20 Dicembre 2013, Brussels;
- CONSIGLIO EUROPEO, *Strategia di sicurezza interna per l'Unione Europea: "Verso un modello di sicurezza europeo"*, Brussels, Marzo 2010;
- CONSIGLIO EUROPEO, *Relazione sull'attuazione della Strategia europea in materia di sicurezza – Garantire sicurezza in un mondo in piena evoluzione* (sintesi), Brussels, 11 dicembre, 2008;
- CONSIGLIO EUROPEO, *Un'Europa sicura in un mondo migliore – Strategia europea in materia di sicurezza*, S407/08, Bruxelles, 12 dicembre 2003;

- DIRECTOR OF NATIONAL INTELLIGENCE, *The National Intelligence Strategy of the USA*, Washington, Agosto 2009;
- EUROPOL, *Valutazione delle Minacce: I Vantaggi offerti da Internet al crimine organizzato*, L'Aia, 2013;
- NATO, *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon*, Lisbona, 19 Novembre 2010;
- NATO, *Bucharest Summit Declaration*, 3 Aprile 2008;
- THE INTERNATIONAL COMMON CRITERIA CONFERENCE (ICCC), *Common Criteria for Information Technology Security Evaluation,* International Standard ISO/IEC *15408,* ver. 3.1, Revision 3 Final, Luglio 2009;
- THE WHITE HOUSE, *The National Strategy to Secure Cyberspace*, Washington, Febbraio 2003;
- THE WHITE HOUSE, *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World* o c.d. *White House Cyber Strategy,* Washington, Maggio 2011;
- THE WHITE HOUSE, *The National Security Strategy of the United States of America*, Washington, 2002, 2006, 2010;
- US DEPARTMENT OF DEFENSE, *Department of Defense Strategy for Operating in Cyberspace*, Luglio 2011;
- US DEPARTMENT OF DEFENSE, *The National Military Strategy for Cyberspace operations*, 2006;

Sitografia:

- www.archiviodisarmo.it
- www.cambridge.org
- www.ccdcoe.org
- www.cepol.europa.eu
- www.cert.europa.eu
- www.chathamhouse.org
- www.comitatoatlantico.it
- www.commoncriteriaportal.org
- www.defense.gov
- www.dhs.gov
- www.difesa.it
- www.dizionarioinformatico.com
- www.dni.gov
- www.eda.europa.eu

- www.eeas.europa.eu
- www.enisa.europa.eu
- www.eurojust.europa.eu
- www.europa.eu
- www.european-council.europa.eu
- www.europol.europa.eu
- www.fedoa.unina
- www.guardian.co.uk
- www.harvardilj.org
- www.iana.org
- www.icana.org
- www.ilsole24ore.com
- www.inss.org.il
- www.icj-cij.org
- www.icrc.org
- www.intelligence.gov
- www.nato.int
- www.nsa.gov
- www.pbs.org
- www.sicurezzanazionale.gov.it
- www.state.gov
- www.un.org
- www.unidir.org
- www.whitehouse.gov

IS e il nuovo volto del Jihad

Il 2 maggio 2011, all'annuncio della cattura e morte di Osama Bin Laden, il mondo ha tirato un sospiro di sollievo. Sembrava, infatti, essere giunti all'epilogo di un incubo che ha tenuto con il fiato sospeso centri di potere politico, persone comuni ed interi paesi. Ma l'entusiasmo che aveva fatto credere che la guerra al terrore fosse finita definitivamente con il suo capo carismatico è durato giusto il tempo di realizzare che il terrorismo non solo non era stato sconfitto, ma, al contrario, dimostrava di essere ancora forte e più multiforme che mai.

Il termine terrorismo è tristemente conosciuto ai quattro angoli del globo, ma riuscire a districarsi tra le sue definizioni, tra le differenti e numerose sigle dei gruppi fondamentalisti esistenti ed operanti e, soprattutto, capirne intenti ed obiettivi è tutt'altro che semplice. Lo stesso termine "Jihad", che in lingua araba vuole dire "lottare", è stato spesso usato in occidente come sinonimo della parola terrorismo o di fondamentalismo rischiando di creare un pericoloso travisamento. La parola Jihad in realtà ha più di un significato, rappresentando sia un obbligo e una lotta contro se stessi ed i propri desideri, sia contro gli oppressori. Ma ormai è di uso comune parlare di Jihad legandolo indissolubilmente al fondamentalismo islamico.

Ma chi sono i terroristi e, principalmente, come distinguerli? La questione potrebbe apparire puramente di forma, ma in realtà, a seconda di come vengono classificati, mutano profondamente sia le politiche di intervento militare, sia le strategie dei paesi occidentali e dei paesi coinvolti nelle aree di crisi. Certo è che la figura del terrorista è in continuo mutamento ed ha saputo adeguarsi perfettamente ai tempi ed ai contesti storici e sociali in cui opera.

Restringendo il campo al solo terrorismo di matrice islamica, Al-Qaeda è stato il brand più famoso che è riuscito a sponsorizzare, per anni, una "Guerra Santa" contro l'odiato occidente in nome di un Islam deviato e violento.

Facendo un passo indietro alla fine degli anni ‘70, nomi come il Fronte Popolare di Liberazione della Palestina e Settembre Nero riportano alla mente efferati attentati terroristici che li hanno resi tristemente famosi in tutto il mondo occidentale. Ma solo con la guerra sovietica in Afghanistan il fenomeno “terrorismo” acquista la notorietà e la massima attenzione dei media e dei governi occidentali. L’invasione russa dell’Afghanistan nel 1979 ha portato alla nascita di un fronte comune di guerriglieri islamici per difendere il proprio Paese contro gli invasori sovietici. Nel 1989 nasce Al-Qaeda (la base) con l’obiettivo di trasformare la resistenza antisovietica in un movimento fondamentalista islamico pronto ad attaccare tutti i nemici interni ed esterni dell’Islam. Il suo ideatore e capo indiscusso è stato il giovane e ricco saudita Osama Bin Laden. I disordini e la feroce guerra civile che seguirono negli anni successivi al ritiro sovietico, indussero nel 1995 gli Stati Uniti ed il Pakistan a stringere un azzardato sodalizio con il mullah Mohammed Omar, capo spirituale ed operativo del movimento dei Taliban.

Grazie al sostegno economico dell’Arabia Saudita, all’addestramento militare dei servizi segreti pakistani ed alle armi statunitensi, i taliban si trasformarono da sparuta milizia di studenti coranici in un agguerrito esercito pronto a difendere la propria libertà ed autonomia con tutti i mezzi possibili. Quando poi, alla fine degli anni ’90, il mullah Omar fornì ospitalità ad Osama Bin Laden negli aspri territori pashtun, al confine tra Afghanistan e Pakistan, gli eventi precipitarono ed i giochi furono oramai fatti.

Negli anni seguenti Al Qaeda ha iniziato ad espandersi al di fuori dei confini afghani operando in Paesi come lo Yemen, la Cecenia, il Caucaso. Dopo l’11 settembre 2001 la regionalizzazione di tutti i movimenti fondamentalisti ha portato alla nascita di gruppi particolarmente violenti quali AQI (Al-Qaeda in Iraq) nei territori dell’Iraq, AQIM (Al-Qaeda in the Islamic Maghreb) in Nord Africa ed Al Nousra in Siria, fino a giungere, ai giorni nostri, alla proclamazione della nascita Califfato da parte dell’IS (giugno 2014).

Oggi il mondo si ritrova nuovamente a combattere un fantomatico e fanatico terrorista che ha messo in allarme tutti i governi mondiali. Si riparte con la macchina della paura e dell’insicurezza, creando nuovi spauracchi e nuove ondate di intolleranze e pericolosi rigurgiti nazionalistici.

Il fenomeno terrorismo, che sembra ormai figlio dei nostri tempi e di difficile sradicamento, con i gruppi fondamentalisti sembra ben prosperare e crescere in tutti quei Paesi islamici che hanno vissuto un drammatico collasso dei poteri centrali. E’ accaduto in Afghanistan ed accade oggi in Iraq e Siria, Paesi che hanno vissuto un drammatico vuoto del potere statale, dando così la possibilità alle violente milizie dell’IS di insediarsi pericolosamente in quei territori.

Al di là delle responsabilità, degli errori e delle errate valutazioni strategiche e politiche è anche vero che sia Al-Qaeda, sia l’IS (che è un offshot di Al Qaeda) non avrebbero mai visto la luce senza i finanziamenti e l’aiuto logistico di Paesi che nell’ombra hanno mosso le fila geopolitiche e strategiche di questi gruppi.

Poco c'entra il problema religioso, che in realtà sembrerebbe più un paravento mediatico per giustificare efferate esecuzioni pubbliche, quando il vero interesse risiede nello sfruttamento delle risorse energetiche di quelle terre. Infatti, nonostante la Guerra Fredda sia parte del nostro passato, il modus operandi per giustificare alcuni obiettivi politici rimane lo stesso. Paesi egemoni e forti dell'area mediorientale, come l'Iran, l'Arabia Saudita e non solo, continuano a dare vita a conflitti per procura, nei quali a farne le spese sono per lo più le popolazioni dei teatri di crisi. Ma, come non di rado accade nella vita e nella storia, la probabile conseguenza di un'azione viene troppo spesso trascurata: i supporti logistici, insieme ad ingenti quantità di denaro e di armi, hanno creato un "mostro" difficile ora da controllare. E allora ecco che gruppi terroristici come l'IS, grazie anche all'uso di strategie mediatiche e ad una potente macchina propagandistica, si trasformano in una priorità assoluta nelle Agende politiche internazionali. Ma il dato forse più allarmante di questa nuova ondata terroristica è la nascita di una nuova generazione di jihadisti globali pronti a raggiungere l'IS da tutta Europa, Italia compresa, e Stati Uniti (ad oggi sono circa 30.000), segno evidente che il disagio, la povertà e un senso di frustrazione violenta è un problema che non riguarda più solo paesi lontani, ma il mondo intero.

L'educazione per tutti e la battaglia di Malala Yousafzai

"Rabad mangia wakht de teer sho
Da kali ta Talibaan raaghali dena"
("Addio musica! Anche le tue melodie più dolci sono zittite. I talebani ai margini del villaggio hanno messo a tacere tutte le labbra." Da "*Io sono Malala*")

Malala Yousafzai, quella giovane ragazza pakistana dai grandi occhi neri, che nel 2012 ha commosso il mondo intero, ha ricevuto il Premio Nobel per la Pace 2014. Proprio quegli occhi così profondi e quell'espressione a volte troppo adulta per la sua giovanissima età, raccontano, più di tante parole, cosa voglia dire essere donna in un Paese dove spesso i diritti di genere vengono violentemente calpestati.

Nata in un piccolo villaggio pasthun, di nome Mingora, Malala ha vissuto la sua infanzia nella Valle dello Swat, tristemente nota per essere rifugio dei Taliban pakistani.

Una vita, quella di Malala, come di tante altre bambine e bambini di quelle regioni del Pakistan, scandita dalla paura e dalla violenza dei militanti fondamentalisti, che bombardano ed incendiano le scuole responsabili, dal loro punto di vista, della diffusione dell'odioso modello di cultura occidentale. Ma questa ragazza a soli 17 anni è diventata il

simbolo universale del diritto all'istruzione. Nonostante, infatti, le minacce ricevute ed i rischi per la sua incolumità fisica, Malala all'età di11 anni inizia a scrivere un blog in urdu della BBC denunciando con coraggio e forza le violenze dei talebani e battendosi contro gli stereotipi ed i pregiudizi nei confronti delle giovani donne che vogliono frequentare liberamente corsi scolastici. Queste le sue parole: "Era la scuola ad aiutarmi ad andare avanti nei momenti difficili. Quando ero per strada avevo la sensazione che tutti quegli uomini che mi passavano accanto potessero essere talebani. Nascondevamo gli zainetti ed i libri sotto lo scialle. Papà diceva sempre che la cosa più bella che si può vedere in un villaggio di mattina è un bambino con l'uniforme scolastica, ma ormai avevamo paura ad indossarla." (cit. dal libro: "Io sono Malala"). Nel 2011, Malala riceve, per il suo impegno in favore dei diritti delle donne, il Pakistan's National Youth Peace Prize.

Il 9 ottobre del 2012, Malala sale, come ogni giorno, sul pulmino scolastico che l'avrebbe dovuta riportare a casa, ignara di andare invece incontro ad un tragico destino. Ad attenderla infatti c'è un talebano pronto ad ucciderla, che le spara tre proiettili al volto e al collo con l'obiettivo di fermare la penna e la voce di quella ragazza così giovane, ma così determinata a voler raccontare al mondo ciò che stava vivendo. Ridotta in fin di vita, Malala è costretta, insieme alla sua famiglia, ad abbandonare il Pakistan trasferendosi in Inghilterra, dove riceve le cure necessarie per vincere la sua battaglia contro la morte.

La storia di questa giovane ragazza ha fatto il giro del mondo e nel 2012 è uscito un libro di successo mondiale intitolato: "Io sono Malala".

Oggi Malala vive a Birmingham, Inghilterra, frequenta regolarmente la scuola e vive la sua vita da adolescente in un paese straniero poiché le è impossibile, almeno per il momento, tornare a Mingora (Pakistan) a causa delle molteplici minacce ricevute. Ciò non le ha impedito però di continuare a lottare trasformandosi in un'attivista per il diritto all'istruzione sia delle bambine sia dei bambini, ma soprattutto divenendo, nel tempo, la voce di tutte quelle giovani donne che, per motivi culturali o a causa di guerre o gruppi estremisti, sono costrette ad una vita senza speranza.

Anche se lontana dal suo amato Pakistan, Malala, grazie ad una incredibile maturità ed al suo costante impegno umanitario, che la porta in giro per il mondo, ha il dono di saper usare un linguaggio universale di pace in grado di superare barriere culturali e religiose e di essere divenuta, nel tempo, il simbolo e la speranza per un'intera generazione di donne che sognano la possibilità di potere scegliere liberamente il proprio destino.

IL "SISTEMA INFORMATIVO A SCHEDE" NEL 2014

- A. Iaria, *Il Trattato sul Commercio di Armi e lotta al trasferimento illecito*, SIS 10/2014;
- G. Valentini, *La lotta non violenta in Tibet*, SIS 09/2014;
- E. Greco, *Il ricorso italiano alle Maritime Security Companies e ai Nuclei Militari di Protezione in funzione antipirateria*, SIS 08/2014;
- G. Valentini, *Resistenza non violenta palestinese*, SIS 07/2014;
- J. Raddusa, V. Gallo, *Speciale Africa - 1) Ecowas: impatto delle armi piccole e leggere sui diritti umani e sullo sviluppo socio-economico della regione. 2) Armi in Africa. Ciad: la spesa militare prima dello sviluppo*, SIS 06/2014;
- S. Bacchi, *I droni: arma del futuro?*, SIS 05/2014;
- G. Palestini, *La guerra in Siria nella prospettiva mediorientale: ricerca sui media di Libano, Arabia Saudita, Iran e Israele*, SIS O4/2014;
- D. Ferretti, *Gli F-35 nella campagna elettorale del febbraio 2013*, SIS 03/2014;
- V. Gallo, *La crisi in Sud Sudan*, SIS 02/2014;
- R. Daveri, *Armi chimiche siriane: il problema dello smaltimento,* SIS 01/2014.

Sistema informativo a schede (SIS)
Mensile dell'Istituto di Ricerche Internazionali Archivio Disarmo (IRIAD)
Piazza Cavour 17, 00193 – Roma (RM)
Tel. 0636000343; Fax. 0636000345
www.archiviodisarmo.it

Direttore Responsabile: Sandro Medici
Direttore Scientifico: Maurizio Simoncelli
Registrazione Tribunale di Roma n. 545/96

Copyright © Istituto di Ricerche Internazionali Archivio Disarmo (IRIAD)