Manuela Farinosi,
Gian Luca Foresti,
Francesco Zucconi
(a cura di)

INTELLIGENCE E TECNOLOGIE EMERGENTI

Per la pace, per la sicurezza informatica, per la lotta alla criminalità

FrancoAngeli

FrancoAngeli
Edizioni La passione per le conoscenze

Informazioni per il lettore

Questo file PDF è una versione gratuita di sole 20 pagine ed è leggibile con **Adobe Acrobat Reader**

La versione completa dell'e-book (a pagamento) è leggibile **con Adobe Digital Editions**.

Per tutte le informazioni sulle condizioni dei nostri e-book (con quali dispositivi leggerli e quali funzioni sono consentite) consulta **cliccando qui** le nostre F.A.Q.

Manuela Farinosi,
Gian Luca Foresti,
Francesco Zucconi
(a cura di)

INTELLIGENCE E TECNOLOGIE EMERGENTI

Per la pace, per la sicurezza informatica, per la lotta alla criminalità

FrancoAngeli

Immagine di copertina: istock.com/Viorica

Isbn: 9788835167426

Indice

III – Rischi e lotta alla criminalità

IV – Diritto e nuove sfide

Introduzione

di *Francesco Zucconi, Gian Luca Foresti, Gianluigi Sechi, Manuela Farinosi*

Il presente volume raccoglie una collezione di ricerche e studi realizzati all'interno del Master in Intelligence and Emerging Technologies del Dipartimento di Scienze Matematiche, Informatiche e Fisiche dell'Università degli Studi di Udine. Vi è un'importante distinzione tra i concetti di "*disruptive technology*" e "*emerging technology*". L'aggettivo "*disruptive*" indica quelle tecnologie o scoperte scientifiche che, nei prossimi vent'anni, imporranno un cambiamento rivoluzionario nell'operatività di organismi complessi, come le entità statuali o strutture quali l'ONU, la Commissione Europea, la NATO, l'*European Defence Agency* (EDA). Con l'aggettivo "*emerging*" si indicano, invece, quelle tecnologie o scoperte scientifiche ancora in fase fortemente sperimentale, i cui effetti non sono ancora pienamente stimabili e che si prevede raggiungeranno la maturità entro il 2040. Un tipico esempio di tecnologia *disruptive* è l'intelligenza artificiale (AI), mentre il *quantum computing*, con tutte le sue diramazioni nel settore delle comunicazioni e della crittografia, rappresenta un esempio di tecnologia emergente.

I lavori del Master in Intelligence and Emerging Technologies sono orientati in modo da adattarsi ai molteplici ambiti disciplinari che pervadono il mondo dell'intelligence. Naturalmente, l'attenzione rivolta a ciò che è qualificabile come "emergente" è guidata da uno studio attento di ciò che è qualificato come "*disruptive*"; l'incertezza che avvolge il futuro deve essere uno stimolo per lavorare sul presente.

I contributi presenti nel volume sono frutto di un intenso lavoro di squadra, che vede docenti e discenti protagonisti di un esperimento didattico-formativo dalle caratteristiche peculiari e innovative. Prima di introdurre i singoli risultati qui raccolti, è opportuno descrivere brevemente le architetture che sostengono tale processo formativo; utilizziamo il plurale poiché,

al disegno complessivo, concorrono molte forme del sapere contemporaneo, mantenendo le rispettive specificità disciplinari. Il disegno complessivo è stato negli anni continuamente raffinato. Infatti, è apparso sempre più evidente, nel succedersi delle edizioni del Master, quanto i discenti, provenienti dai più svariati ambiti formativi e lavorativi, necessitino di integrare i loro strumenti cognitivi in una visione più olistica della realtà, orientata in senso predittivo.

Abbiamo osservato che sia i modelli intellettuali proposti nei diversi percorsi formativi di livello universitario, sia le pratiche mentali acquisite nei rispettivi ambiti lavorativi – anche in gradi di carriera piuttosto elevati – tendono a consolidare forme settoriali di rigidità mentale e operativa, incompatibili con la poliedricità necessaria per affrontare le sfide derivanti dai rapidi cambiamenti della società odierna, prodotti dall'uso sempre più diffuso e pervasivo delle moderne tecnologie matematico-informatiche.

Uno dei problemi che il Consiglio Scientifico del Master si è trovato ad affrontare è il seguente: come integrare una preparazione mirata alla gestione consapevole delle tecnologie emergenti (intelligenza artificiale, *machine* e *deep learning*, *big data analysis*, *cyber security*, biometria e *gait analysis*, *web intelligence*, *text mining*, *open source intelligence*, *crowdsourcing intelligence*, *augmented* e *virtual reality*, ecc.) con la capacità, che un analista di intelligence deve possedere, di interpretare, a fini predittivi, la realtà? Questa capacità interpretativa, a nostro avviso, non può prescindere da una formazione umanistica. Gli argomenti presentati all'interno dei moduli di storia dell'intelligence, di diritto per l'intelligence, di fondamenti di geopolitica e di fondamenti di intelligence economica mirano, appunto, a rafforzare le basi culturali di tipo umanistico. È evidente che una capacità tecnica, ben allenata nell'attingere a un'inesauribile mole di dati, può essere valorizzata solo se si è capaci di organizzare e interpretare tali dati, sino a produrre informazioni che, nei casi più fortunati, possono fornire una conoscenza sul "come" delle cose e, in ultimo, meta spesso irraggiungibile, sul "perché" delle cose.

Per favorire un'integrazione tra l'ambito culturale di tipo scientifico e tecnologico e quello umanistico, sia nella sua versione più classica che nella versione espressa dalla SOCMINT (*Social Media Intelligence*), abbiamo costruito dei ponti didattici basati, a partire dai fondamenti del Ciclo dell'Intelligence, sia sul laboratorio di OSINT (*Open Source Intelligence*) sia su specifiche attività seminariali condotte da esperti di chiara fama, che hanno sperimentato sul campo l'utilità e la necessità di realizzare tale integrazione. Un altro obiettivo di grande interesse per il Consiglio Scientifico del Master, che ha condizionato il disegno complessivo, è quello di trasmettere una conoscenza sufficientemente ampia per orientarsi nelle problematiche alla base

della sicurezza nel mondo contemporaneo, quali: (a) le minacce all'integrità dei sistemi informatici, difficili da rilevare e mitigare, basate su tecniche sempre più sofisticate di phishing, malware, ingegneria sociale e hacking; (b) le vulnerabilità dei sistemi informatici, spesso dovute a errori di programmazione, configurazioni errate, mancata applicazione di patch di sicurezza o uso di software non aggiornato; e soprattutto (c) la mancanza di consapevolezza degli utenti riguardo alle minacce informatiche e la scarsa adozione di buone pratiche di sicurezza.

Per conseguire tali obiettivi non è possibile né assecondare la tentazione di indebolire quella rigidità disciplinare necessaria per acquisire davvero le capacità di utilizzare in modo efficace e consapevole gli strumenti informatici più recenti, né rinunciare a presentare con la dovuta ampiezza e profondità le basi di storia dell'intelligence, di diritto per l'intelligence, di fondamenti di geopolitica, di fondamenti di intelligence economica, di fondamenti della social media intelligence e di teorie della comunicazione e della ricerca sociale.

L'approfondimento di tutte le pratiche – e dei loro presupposti teorici – relative al ciclo dell'intelligence e lo studio del rapporto tra intelligence e nuovi media, nella prospettiva della SOCMINT, ci hanno permesso di plasmare un percorso disciplinare unico nel suo genere, che, senza questi due pilastri, avrebbe rischiato di favorire una mentalità semplicemente specialistica.

Riteniamo di essere riusciti a gettare le fondamenta per far emergere nei nostri corsisti un *habitus* mentale proattivo, capace di sopportare autoanalisi fortemente autocorrettive e di leggere quelle differenze, difficoltà, incongruenze, inganni e autoinganni che l'uso di ogni modello teorico o di qualsivoglia pratica rigidamente codificata incontra nella sua interazione pratica con la realtà.

I contributi raccolti in questo volume, che originano dai lavori di tesi di corsiste e corsisti del Master, o da docenti del Master vanno quindi letti tenendo presente questa volontà di forgiare un personale capace di cogliere anche quei segnali, inizialmente deboli, di ciò che, una volta dispiegato, avrà effetti niente affatto deboli.

Apre il volume il contributo "Misurare la pace: provocazione, utopia o inderogabile necessità" di Giuseppe Santomartino. Questo lavoro verte sugli indicatori oggettivi sui quali si basano i moderni studi sulla pace. Riprendendo il pensiero di Johan Galtung, sono ivi esposti, in modo sintetico, i concetti di *Negative Peace* (NP) e di *Positive Peace* (PP) elaborati dall'*Institute for Economic and Peace* diretto da Steve Killelea. Ricordiamo che NP significa, essenzialmente, l'assenza di violenza o l'assenza dalla paura di forme di violenza rispetto alla violenza in atto o alla paura della violenza che si dispiega-

no durante uno stato di guerra. Invece con PP si intende la determinazione e la capacità che istituzioni o strutture, statuali o non statuali, attivano per creare, sostenere e mantenere la pace nella totalità di una situazione sociale. La chiarezza apportata dall'uso di indicatori oggettivi (descritti nel lavoro, quali il *Global Peace Index* (GPI), il *Positive Peace Index* (PPI), il *Corruption Perception Index* (CPI), il *Fragility State Index* (FSI)), per distinguere NP rispetto a PP, fornisce un solido apparato concettuale per distinguere, per esempio, il concetto di "tregua" da quello di "pace" e anche dei modelli predittivi che possono supportare futuri percorsi di pace. In questo senso, data la complessità di molti degli indicatori, l'autore individua un interessante utilizzo dell'AI per scopi pacifici. Santomartino mette in guardia, tuttavia, contro "un eccessivo appiattimento epistemologico su paradigmi di positivismo quantitativo". Il resto del volume è suddiviso in quattro sottosezioni: Intelligenza artificiale e sicurezza nazionale, sicurezza informatica e *cyber security*, rischi e lotta alla criminalità, diritto e nuove sfide.

Il contributo "Servizi segreti o agenzie d'intelligence: questioni e criticità solo semantiche?" di Francesco Serra consente di seguire l'evoluzione legislativa sull'intelligence che si è avuta in Italia, a partire dalla L. 801/1977 sino alla L. 124/2007, sotto la particolare angolatura delle forme linguistiche utilizzate per indicare le strutture dell'intelligence. La necessità inderogabile di tornare a valorizzare la HUMINT, proprio a causa del travolgente impiego delle nuove tecnologie in ambito intelligence, conduce l'autore a delle riflessioni sul tipo di disposizione interiore necessaria per assolvere i compiti che un moderno servizio di intelligence deve svolgere nel deteriorato contesto geopolitico attuale.

Il contributo "La comunicazione in un contesto strategico" di Lorenzo Lena, che chiude la prima sezione, studia le teorie (e le pratiche) russe che mirano ad amplificare preesistenti tensioni sociali interne a un'entità statuale che si vuole sottomettere. La teoria della *Gibridnaya Voyna*, al di là di finezze semantiche relative a una corretta traduzione linguistica di tale espressione russa, è inquadrata nel contesto costituito dalle nuove forme di comunicazione disintermediata. In particolare, viene accennata la potenzialità negativa, veramente dirompente, che lo sviluppo della *Generative AI* potrà sviluppare per spezzare il legame fiduciario tra il singolo individuo e lo Stato. Una solida formazione democratica costituisce senza dubbio un ottimo antidoto contro tali minacce, ma, conclude l'autore, essa non può che venire rafforzata da una piena consapevolezza delle medesime.

La seconda sezione "Sicurezza informatica e *cyber security*" consiste di tre contributi. Il primo: "Proposta di una nuova strategia per la *cyber secu-*

rity a difesa del patrimonio informativo aziendale", di Alessandro Franchi, propone di considerare l'intera struttura dell'IT aziendale come un artefatto cognitivo, nozione epistemologica introdotta da Donald Arthur Norman. In particolare, Franchi costruisce un modello progressivo teso a migliorare l'attuale gestione, talvolta non ben coordinata, della sicurezza ICT di un'azienda di medie dimensioni. Tale modello è incentrato su: 1) un'analisi del rischio, 2) una stima accurata del reale valore delle informazioni, 3) l'utilizzo della metodologia *Zero Trust Network Access* (ZTNA), il tutto da supportare con 4) moderne tecniche di OSINT e con 5) sistemi integrati di AI.

Il secondo contributo "I cavi sottomarini di Internet" di Virginia Maria Buzzoni esplora, anche attraverso una vasta bibliografia, le caratteristiche, le principali rotte, le problematiche di tipo giuridico, le vulnerabilità di tipo accidentale così come quelle di tipo intenzionale e le relative questioni geopolitiche, concernenti la rete dei cavi in fibra ottica posti sui fondali marini, anche a migliaia di metri di profondità, che assicurano il funzionamento di tutte le trasmissioni via Internet. Crediamo che questo contributo costituisca una buona base per acquisire una piena consapevolezza di quanto poco immateriale sia, in realtà, il mondo della rete.

Chiude la seconda sezione il lavoro: "Il *continuos learning* per il rilevamento delle intrusioni nelle reti: analisi dell'algoritmo SF-SOINN sul dataset CIC IDS 2018" di Giulia Giacosa. Il problema del rilevamento delle intrusioni nelle reti informatiche è un problema di classificazione del traffico di rete. A tal fine sono stati sviluppati metodi di machine learning che vengono ricordati nel lavoro. Un problema tipico nel caso delle intrusioni è che i dati sono generati da processi che evolvono nel tempo. Pertanto, l'accumulo dei nuovi dati da utilizzare per il riaddestramento costante del modello pone sfide non banali per l'alto consumo di memoria e per conseguenti possibili abbassamenti nell'efficienza computazionale. Inoltre, i nuovi dati possono interferire con le conoscenze pregresse e questo può provocare conseguenze assai negative sul livello delle prestazioni. Il districarsi tra la necessità di acquisire nuove conoscenze e, contemporaneamente, evitare che i nuovi dati interferiscano con quanto già appreso ha portato alla costruzione di reti SOIN, acronimo che sta per "*self organized incremental neural networks*" da parte di Shen Furao e Osamu Hasegawa. Tale algoritmo di *continuos learning* non supervisionato è evoluto in varie varianti, qui ricordiamo solo l'algoritmo SF-SOINN costruito da M.R. Martina e G. Foresti che è appunto oggetto di trattazione e di analisi da parte di Giacosa.

La terza sezione del volume, "Rischi e lotta alla criminalità" ospita due contributi. Il primo, "Il PNRR e i rischi connessi: corruzione, frodi, sprechi e

infiltrazioni della criminalità organizzata", scritto da Gianluigi Miglioli e da Paolo Marzano è di estrema attualità, perché descrive, in modo sintetico, sia il quadro generale del PNRR, che la strategia di controllo operativo sul corretto funzionamento del medesimo. Miglioli e Marzano, forti anche di una notevole esperienza operativa, conducono per mano il lettore a vedere i punti del quadro che, se non attentamente presidiati, potrebbero favorire comportamenti illeciti a vantaggio dell'economia controllata dalla criminalità organizzata. In particolare, si trova in questo contributo una pacata, quanto articolata disamina circa la difficoltà di coniugare procedure di semplificazione amministrative, con capacità di controllo che, in qualità di soggetti attuatori, deve essere superata da amministrazioni, talvolta piuttosto decentrate e che fino a poco tempo fa erano strutturate più per contenere la spesa che non per organizzare o gestire ingenti investimenti per di più in aree di interesse che richiederebbero un personale altamente formato e versato nell'uso delle nuove tecnologie. Non possiamo, quindi, non riscrivere la citazione che chiude questo lavoro, scritta da Giovanni Falcone, il quale, riferendosi alla mafia, scriveva "non è affatto invincibile; è un fatto umano e come i fatti umani ha un inizio e avrà una fine. Piuttosto, bisogna rendersi conto che è un fenomeno terribilmente serio e molto grave; e che si può vincere (...) impegnando in questa battaglia tutte le forze migliori delle istituzioni, per affermare che anch'esso può essere sconfitto".

Il secondo contributo della terza sezione "L'analisi delle segnalazioni per operazioni finanziarie sospette alla luce dell'intelligenza artificiale, quale strumento di lotta alle mafie e al riciclaggio del denaro" di Antonio De Santis propone un vero e proprio disegno strutturale, che potrebbe essere in parte fortemente automatizzato per connettere, secondo modalità operative fortemente efficientate dalle nuove tecnologie informatiche, le segnalazioni sospette di potenziale illecito finanziario alla Direzione Nazionale Antimafia e Antiterrorismo (DNAA). Il percorso, in sintesi, sarebbe il seguente: a partire dalla segnalazione da parte dei soggetti obbligati, l'Unità di Informazione Finanziaria (UIF) presso la Banca d'Italia, ricevuta la segnalazione ed effettuata una prima verifica nei suoi archivi, redige una relazione tecnica. In seguito, l'UIF invia la segnalazione al Nucleo di Polizia Valutaria della Guardia di Finanza e alla DIA per un riscontro di elementi investigativi di interesse. La DIA, sfruttando l'informatica di base verifica eventuali riscontri nel proprio patrimonio informativo. Contestualmente, viene effettuata una prima classificazione delle persone fisiche/giuridiche implicate in condotte delittuose e classificate come delitti di categoria 1 e delitti di categoria 2 a seconda anche del grado di sintomaticità di condotte potenzialmente di tipo mafioso. In

caso di esito positivo, la DIA provvede ad avvertire la DNAA. In seguito, l'Ufficio Informatica della DIA struttura i dati ricevuti all'interno della piattaforma web messa a disposizione dei Centri Operativi e delle Sezioni operative, che li consulteranno per evidenti e correlate esigenze investigative da svolgere nei rispettivi territori di riferimento. Naturalmente la Direzione Centrale svolge un ruolo di coordinamento con i diversi Centri Operativi. In ogni caso, sia che i Centri Operativi lavorino su segnalazione della Direzione Centrale, che a partire da una prima consultazione della comune piattaforma web, essi provvedono ad attivare un'investigazione con valutazione, attività quest'ultima descritta nel contributo. Tale investigazione con valutazione, in ogni caso, andrà ad arricchire il patrimonio informativo di quel determinato Centro/Sezione che avrà lanciato l'investigazione con valutazione. Quest'ultima, anche a causa delle molteplici tipologie di approfondimenti informativi che l'operatore di polizia deve effettuare si presta a essere integrata con algoritmi di *machine learning* e di *text mining*. In particolare, la clusterizzazione offerta dal *text mining*, oltre alla distribuzione dei dati per gruppi di appartenenza si presta anche per approfondimenti su dati anomali. Purtroppo, la sperimentazione di questo schema investigativo che integra naturalmente elementi di AI con aspetti di vera e propria conoscenza diretta dei territori non è ancora stata sperimentata per un espresso divieto imposto dalla normativa vigente.

La sezione finale del volume, "Diritto e nuove sfide" consta di due contributi. Il primo "L'intelligence territoriale, un patrimonio informativo della Regione Friuli Venezia Giulia. Aspetti dell'AI dalla programmazione energetica agli abusi edilizi" di Elena Viero, affronta le potenzialità che la messa a sistema della grande quantità di dati in possesso delle pubbliche amministrazioni potrebbe fornire alle medesime per una più attenta gestione del territorio. In particolare, il contributo analizza, anche nei suoi attuali limiti, come il rilievo ortofotogrammometrico possa essere utilizzato, per mezzo di diverse tipologie di reti, per un rilevamento dei pannelli solari distribuiti su porzioni del territorio della Regione Friuli Venezia Giulia. Un'altra analisi, eseguita in questo contributo, concerne l'uso del software "Erdas Imagine" e del filtraggio fornito dalla Carta Tecnica Regionale Numerica per il rilievo di coperture in cemento amianto di edifici. Il contributo contiene la descrizione di un possibile passo successivo, che consisterebbe nell'utilizzare un sistema di *machine learning* addestrato sui tetti che sappiamo essere di amianto, per poi fare, una volta completato l'addestramento, un censimento in modalità non supervisionata su larga scala.

Infine, chiude la quarta sezione e il volume il lavoro intitolato "Robot e diritto: i sistemi di arma letale autonomi" di Federico Sertori. In quest'ultimo contributo viene affrontata la definizione di sistema d'arma autonomo e i risvolti che ne derivano, dall'assumere l'una o l'altra definizione, in termini di diritto internazionale umanitario. L'autore sottolinea come la radice del problema risieda in quel tipo di armi aventi l'elemento umano fuori dal circuito decisionale. Insomma, il caso di robot in grado di selezionare gli obiettivi e di fornire forza letale senza alcun intervento da parte di un essere umano. Dal punto di vista giuridico, l'autore pone in evidenza i seguenti problemi: 1) se un'arma autonoma assicuri il rispetto del diritto internazionale umanitario, 2) chi debba rispondere in caso di decisioni errate da parte del sistema di arma autonoma, 3) se sia eticamente e quindi giuridicamente accettabile che decisioni potenzialmente letali possano essere delegate a un agente non umano. In linea teorica la produzione di sistemi d'arma autonomi, per poter rispettare i vincoli del diritto internazionale umanitario, dovrebbe essere sottoposta a controlli preventivi. Nel dicembre 2023, molti Paesi hanno preso atto della gravità della sfida ed hanno approvato a maggioranza, con la *General Assembly Resolution* 78/241, che un algoritmo non dovrebbe avere il pieno controllo nella decisione di procurare la morte di un essere umano. È del tutto evidente, tuttavia, che la produzione di armi sempre più sofisticate non sia stata ridotta e che, quindi, non resta, per il momento, che cercare il modo in cui possano essere applicabili i principi umanitari cardine del diritto internazionale umanitario in questi nuovi scenari di guerra.

Premessa

di *Giacinto Ottaviani**

Con vivo piacere mi accingo a stilare alcune righe di prefazione del presente volume che è – lo premetto subito – particolarmente significativo, perché tocca, nei suoi vari aspetti, uno dei nodi fondamentali della geopolitica, ovvero l'intelligence. Si è sostenuto, a ragione, che l'intelligence costituisca l'essenza della più alta politica, ovvero l'epicentro della geopolitica stessa. Non a caso le origini di tale attività umana non sarebbero imputabili all'uomo, bensì, secondo il Vecchio Testamento, addirittura a Dio (ovvero allorquando Yawhe ordinò a Mosè di inviare degli osservatori nella terra di Canaan, dando allo stesso Mosè istruzioni dettagliate sull'operazione stessa e come eseguirla)[1]. Si potrebbe parlare dunque di fondamento biblico delle attività di intelligence!

Orbene, nel cuore dell'evoluzione tecnologica contemporanea, il presente volume – che è un'opera collettanea di saggi frutto del prestigioso master in Intelligence and Emerging Technologies dell'Università di Udine – declina alcuni punti emergenti del comparto dell'intelligence contemporanea, evidenziando, in particolare, con i vari contributi scientifici, la "declinazione" di due nuovi concetti: "disruptive" ed "emerging"; questi infatti stanno plasmando non solo l'intelligence, ma il mondo intero, in cui pace, sicurezza (informatica) e lotta alla criminalità sono aspetti sempre più cruciali.

In tale contesto, gli Autori tutti si sono impegnati offrendo con i loro saggi un quadro applicativo, direi pratico, di ciò che più largamente possiamo chiamare "cultura" dell'intelligence stessa, contribuendo così a un approccio olistico verso tale complesso settore della conoscenza ma anche dell'attività

* Presidente del CASD.

1. *Num*. 13:1-2; *Num*. 13:17; *Num*. 13:17-20.

umana. Pur essendo l'intelligence un'attività prettamente umana – in cui la *Humint* non va mai trascurata – le nuove tecnologie stanno provvedendo a modificarne la modalità; la conseguenza è che oggi lo spettro delle attività di intelligence vede un vistoso ampliamento, in quanto il mondo iperconnesso e globalizzato, in cui sta entrando l'Intelligenza Artificiale, se non opportunatamente difeso, può diventare ancor più insidioso di quello del passato. L'incremento di tali nuove tecnologie e con esse nuovi saperi, non tange gli "arcana imperii" (per ricordare Tacito), che restano, ma cambia la modalità con cui si deve proteggere, difendere nonché perseguire gli interessi strategici.

Dunque il presente volume rappresenta un prezioso strumento ed evidenzia anche una fattiva collaborazione scientifica tra docenti e discenti all'interno del Master, da cui ne è scaturita un'opera che non solo arricchisce il dibattito accademico, ma fornisce anche strumenti concreti per affrontare le sfide del futuro. Pertanto, sono certo che queste pagine possano stimolare nuove riflessioni e pertanto formulo i miei più sinceri rallegramenti ai curatori così come anche a tutti gli Autori.

Misurare la pace: provocazione, utopia o inderogabile necessità?

di *Giuseppe Santomartino*

1. Introduzione

War to end all wars, 1914[1].
Salvare le future generazioni dal flagello della guerra, 1945[2].

Queste due citazioni, formulate all'inizio e fine rispettivamente della Prima e della Seconda Guerra Mondiale e che potrebbero oggi stimolare un facile sarcasmo, ci ricordano anche come l'aspirazione alla "pace", sempre presente nel genere umano, assuma valenza massima nelle fasi più critiche della storia. In tali fasi dobbiamo purtroppo includere anche questo inizio di XXI secolo che presenta un intreccio di vicende e fenomeni che vanno ormai consolidando un livello di complessità geopolitica che forse l'umanità non ha mai conosciuto prima nella storia. In particolare assume drammatica rilevanza l'aumento dei conflitti dal 1975 a oggi (Fig. 1) a opera anche degli *Armed-Non-State Actors* (ANSA)[3] e un costante peggioramento dei conflitti e crisi in atto (dati *ICG-Monthly Conflicts Tracker*)[4]. In tale quadro emerge con

1. Titolo di un brano dell'inglese G. Wells all'inizio della Prima Guerra Mondiale nell'illusione, diffusa all'epoca, che quella guerra avrebbe potuto eliminare ogni rischio di guerre future. La frase fu poi ripresa con maggiore enfasi dal Presidente americano Wilson nel 1919.

2. Preambolo della Carta delle Nazioni Unite, 1945, considerata ancora oggi quale principale riferimento del diritto internazionale e delle relazioni internazionali (RI).

3. Qui si citano, solo per memoria, alcune delle vicende e dei fenomeni che concorrono a tale complessità geopolitica, essi sono peraltro oggetto di comune conoscenza: l'11 settembre; la pandemia COVID che ha espresso forti valenze geopolitiche; i conflitti in Ucraina e in Palestina; jihadismo; la globalizzazione; lo spostamento del focus economico-finanziario verso l'Indo-pacifico; Brics; espansione dei *Non-State Actors*; erosione del modello Stato-Nazione specie in Asia e Africa, ecc.

4. ICG-International Crisis Group è un organismo indipendente con sede in Bruxelles la cui missione è "*to prevent wars and shape policies that will build a more peaceful world*", dall'osser-

sempre maggiore vigore e drammaticità la consapevolezza della priorità ontologica[5] della pace anche in riferimento alla stessa sopravvivenza dell'umanità in particolare in questo secolo. Ciò postula una riflessione circa l'adeguatezza del nostro impianto culturale, epistemologico e analitico nei confronti di tale complessità geopolitica e, conseguentemente, circa la nostra capacità di "pensare", prima che di ricercare, la pace. Si avverte in altri termini l'esigenza, per troppo tempo sottovalutata, di una riflessione critica utile per un percorso di oggettivazione del concetto di pace.

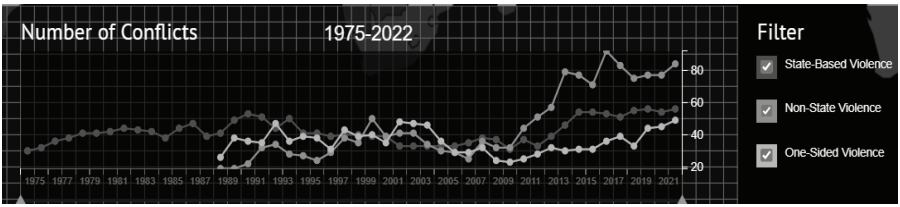

Fig. 1 - Andamento dei conflitti censiti dal 1975 al 2022 (Fonte: Uppsala University, 2024)[6]

Lo scopo, certamente ambizioso, di questo breve saggio è proporre alcune indicazioni e riflessioni analitiche, seppure non esaustive, utili almeno ad avviare tale percorso.

2. Contesto teorico e revisione dello state dell'arte

La panoramica dei modelli teorici e della letteratura sulla pace è certamente vasta, qui si è scelto di limitare l'analisi, necessariamente sintetica, a tre filoni principali:

- l'evoluzione dell'approccio epistemologico;
- il confronto col livello di complessità analitica riferibile alla pace;
- la collocazione dei relativi studi in ambito accademico/ricerca.

vazione di circa 70 conflitti e crisi in atto nell'ultimo anno è emerso che ogni mese si registrano in media 10 *deteriorated situations* a fronte di 1 *improved situation*. www.crisisgroup.org, Ultima data di consultazione: 04/05/2024.

5. Per priorità ontologica si intende qui un concetto e/o valore valutato quale "ente" prioritario rispetto ad altri, specie in termini di dipendenza. Non vi è dubbio che la pace, al di là di ogni sottigliezza speculativa, rientri pienamente in tale categoria ed è forse l'unico "ente" cui attribuire una vera priorità ontologica.

6. https://ucdp.uu.se Ultima data di consultazione: 30/04/2024.

Un'analisi esaustiva dell'evoluzione dell'approccio epistemologico sulla pace sarebbe qui impossibile, ma appare tuttavia utile ricordare almeno sommariamente le tappe fondamentali di tale evoluzione partendo, per l'Occidente, dalla Bibbia e, in Oriente, dalla religione e filosofia del taoismo, per continuare col pensiero di Sant'Agostino[7], San Tommaso, Ugo Grozio[8], Baruch Spinoza[9], Immanuel Kant[10]. Nel XX secolo autorevoli contributi in materia si sono poi avuti anche con alcune importanti encicliche e documenti pastorali della Chiesa Cattolica[11].

L'evoluzione più rilevante si è avuta con Johan Galtung[12], che ha raccolto anche il pensiero di Gandhi e M.L. King, in particolare nel testo *Theories of Peace. A Synthetic Approach to Peace Thinking* (Galtung, 1985) in cui introduce una teoria della pace fondata su "relazioni positive" (teoria da cui poi si svilupperà il concetto di *Positive Peace*, si veda *infra*) quali: cooperazione, libertà dalla paura e dal bisogno, crescita e sviluppo economico, eguaglianza, giustizia, pluralismo. Teoria da associare ai concetti da lui elaborati di "violenza strutturale" (derivante dai sistemi socio-politici) e "violenza culturale" (derivante da posture culturali, pregiudizi, razzismo, ecc.).

Dal pensiero di Galtung l'*Institute for Economic & Peace* (IEP), sotto la guida di S. Killelea[13], ha derivato negli ultimi anni le due principali definizioni in materia (2020, p. 48):

7. S. Agostino, *De civitate Dei*, IV secolo, testo fondamentale per la storia del pensiero politico occidentale, in particolare per l'enfasi sul concetto di pace quale bene supremo per l'umanità ("*Pax omnium rerum, tranquillitas ordinis*") e per i principi, validi ancora oggi, dei limiti nella violenza politica e bellica.

8. U. Grozio, ritenuto il padre del diritto internazionale, opera principale: *De iure belli ac pacis*, 1625.

9. B. Spinoza, filosofo olandese del XVII secolo, nel suo *Trattato teologico-politico* del 1670 (libro messo al bando dalla Chiesa): "la pace non è assenza di guerra: è una virtù, uno stato d'animo, una disposizione alla benevolenza, alla fiducia, alla giustizia".

10. Il contributo di I. Kant al pensiero occidentale sulla pace è di assoluta rilevanza in *Per una pace perpetua* del 1795, un vero progetto filosofico per la pace con elementi di notevole attualità e che ha in buona misura anche ispirato la Carta delle N.U.

11. Da ricordare in particolare le encicliche: *Pacem in Terris* di Giovanni XXIII del 1963 e la definizione della guerra quale "*alienum est a ratione*"; *Gaudium et Spes* di Paolo VI, quale esito del Concilio e definita quale "vera teologia della pace"; la recentissima enciclica *Fratelli tutti*, di Papa Francesco del 2020. Da ricordare poi, insieme a tanti altri documenti e iniziative, il capitolo sulla "Difesa della pace" del catechismo emanato da Giovanni Paolo II nel 1997.

12. J. Galtung, 1930-2024, filosofo e matematico norvegese, considerato il padre dei *Peace Studies*, ha fondato il *Peace Research Institute* in Oslo.

13. L'*Institute for Economics & Peace* (IEP) di Sydney, fondato nel 2007 da Steve Killelea, "*is an independent, non-partisan, non-profit think tank dedicated to shifting the world's focus to peace as a positive, achievable, and tangible measure of human well-being and progress*". Per ogni altra informazione sull'IEP e sulle pubblicazioni si visiti il sito web www.economicsandpeace.org.