



## Intelligenza Artificiale ed Etica: la necessità di un Codice di Guerra

Pubblicato il 23/08/2025

L'invasione russa dell'Ucraina e il recente conflitto a Gaza hanno riportato la guerra al centro delle dinamiche globali, mostrando come le regole consolidate della convivenza internazionale possano essere violate senza esitazione. In questo scenario, la riflessione sull'etica dell'**intelligenza artificiale applicata alla difesa** non è un esercizio teorico, ma una necessità strategica.

Lo sottolinea **Mariarosaria Taddeo**, docente all'Università di Oxford e membro del Ministero della Difesa britannico per l'IA Ethics Advisory Panel, nel suo nuovo libro *Codice di guerra*, in uscita il **26 agosto per Raffaello Cortina Editore**. Secondo l'autrice, proprio nei momenti in cui la guerra si fa più brutale occorre riaffermare principi e limiti, ancorando l'uso delle nuove tecnologie a un codice etico condiviso.

### Cyberwarfare e intelligenza artificiale: dal "Pearl Harbor digitale" alla guerra ibrida

Le aspettative di un “**cyber-Pearl Harbor**” all’inizio della guerra in Ucraina – un attacco digitale massiccio, capace di paralizzare il Paese – non si sono realizzate. Non perché la dimensione cibernetica sia marginale, ma perché, come osserva Taddeo, i **cyber-attacchi sono più disruptivi che distruttivi**: non producono devastazioni immediate paragonabili a quelle delle armi convenzionali, ma minano infrastrutture, economie e società digitali.

Esempi non mancano: dall’attacco del 2007 ai servizi digitali estoni, al malware Stuxnet contro l’Iran, fino agli attacchi ransomware **WannaCry** e **NotPetya**. Più recentemente, le offensive informatiche attribuite all’unità bielorusa **UNC1151** hanno colpito l’Ucraina alla vigilia dell’invasione russa del 2022.

Il problema, sottolinea Taddeo, è che la regolamentazione internazionale ha finora adottato un approccio per analogia, limitandosi a trattare i cyber-attacchi come guerra convenzionale solo se producono danni fisici equiparabili. Ma questo “**analogy-approach**” trascura la vera novità: la capacità del cyberwarfare di compromettere asset immateriali – dai dati all’economia digitale – con effetti sistemici sulle democrazie avanzate.



Intelligenza Artificiale ed Etica: la necessità di un Codice di Guerra

## Armi autonome e governance internazionale

Accanto al cyberspazio, il fronte più delicato riguarda i **sistemi d’arma autonomi (AWS e LAWS)**. Definirne i confini è già di per sé complesso: **dove finisce il controllo umano e dove inizia la decisione autonoma della macchina?**

Secondo Taddeo, senza una definizione condivisa di **“controllo umano significativo”** diventa impossibile affrontare le implicazioni giuridiche ed etiche. Per questo diversi Stati hanno avviato tavoli di confronto, mentre l’ONU nel 2021 ha riconosciuto che anche i cyber-attacchi devono essere regolati secondo i principi del diritto umanitario internazionale (IHL).

Nel frattempo, alcuni Paesi occidentali hanno fatto passi avanti: il **Ministero della Difesa britannico** ha pubblicato nel 2022 il documento *Ambitious, safe, responsible*, contenente principi etici per l’IA in difesa; il **Pentagono** aveva già definito le proprie linee guida attraverso il Defence Innovation Board. La convergenza di approcci tra alleati potrebbe rappresentare l’inizio di una **governance etica transatlantica delle tecnologie militari emergenti**.

## Implicazioni strategiche per l’ordine globale

L’analisi di Taddeo va oltre la dimensione accademica: tocca i nodi geopolitici di un’epoca in cui l’IA, i big data e la robotica militare sono sempre più centrali negli equilibri di potere.

Il rischio non è solo quello di un’**escalation tecnologica incontrollata**, ma anche la progressiva erosione dei valori democratici se le nuove armi saranno impiegate senza un codice etico comune. Come scrive l’autrice, «la guerra è il male assoluto, ma il difendersi è un diritto innegabile». Proprio per questo, aggiunge, bisogna evitare che le atrocità prodotte dalla violenza convenzionale vengano moltiplicate da sistemi automatizzati privi di responsabilità umana.

## Conclusione

La riflessione proposta da *Codice di guerra* è un contributo cruciale al dibattito internazionale: **come integrare l’IA e il cyberwarfare nella difesa senza sacrificare i principi del diritto e della morale?**

Per Taddeo, la risposta sta in una governance etica globale, fondata sulla proporzionalità, sulla necessità e sulla distinzione tra civili e combattenti, adattate alle nuove tecnologie. In gioco non c’è solo l’efficacia militare, ma la tenuta stessa dell’ordine internazionale e la capacità delle democrazie di difendersi senza snaturarsi.

---

**Link notizia:** [https://www.ansa.it/sito/notizie/cultura/libri/2025/08/20/letica-dellia-nella-difesa-nel-saggio-di-mariarosaria-taddeo\\_6ac8316f-7e66-448e-9205-ae581cec38a0.html](https://www.ansa.it/sito/notizie/cultura/libri/2025/08/20/letica-dellia-nella-difesa-nel-saggio-di-mariarosaria-taddeo_6ac8316f-7e66-448e-9205-ae581cec38a0.html)