

## Vantaggio Ucraina: Come l'IA sta cambiando i rapporti di forza nella guerra

Anselm Küsters e Jörg Köpke



© shutterstock

Una questione di vita o di morte: le tecnologie digitali, come l'intelligenza artificiale (AI), stanno sempre più condizionando gli eventi sul campo di battaglia. L'invasione dell'Ucraina da parte della Russia ha rivoluzionato la guerra. Tragicamente, il fronte tra Crimea e Donbass sta diventando un campo di esercitazione. Ma nonostante i successi dell'Ucraina e la superiorità dell'Occidente, le esperienze precedenti e gli esperimenti di IA dimostrano che nel lungo periodo i sistemi militari autonomi non sono armi miracolose.

## Contenuti

<b>1</b>	<b>Introduzione .....</b>	<b>3</b>
<b>2</b>	<b>Il potere militare nell'era dell'IA .....</b>	<b>3</b>
<b>3</b>	<b>Verso un'IA responsabile? .....</b>	<b>5</b>
<b>4</b>	<b>Imparare dal passato .....</b>	<b>6</b>
<b>5</b>	<b>Rischio: sconosciuto e non monitorabile .....</b>	<b>6</b>
<b>6</b>	<b>Un metodo basato sul rischio con test strutturati.....</b>	<b>7</b>

## 1 Introduzione

Mentre i parlamenti ed i governi occidentali discutono ancora di possibili esportazioni di armi, le tecnologie digitali hanno assunto da tempo **un ruolo militare e geopolitico decisivo**. L'invasione dell'Ucraina da parte della Russia è la prima guerra in cui entrambe le parti hanno fatto ampio uso di attrezzature da combattimento digitali come i droni.<sup>1</sup> Inoltre, ci sono circa 200 attacchi informatici al giorno, che Mosca utilizza in particolare come parte della sua **guerra ibrida**.<sup>2</sup> L'Ucraina ha avuto un sorprendente successo nel tenere testa alla potenza militare mondiale Russa utilizzando in modo creativo tecnologie originariamente non militari.<sup>3</sup> Esempi eloquenti sono i satelliti Starlink di Elon Musk o i droni volanti DJI. Il ministro ucraino della Trasformazione digitale, Mykhailo Fedorov, ha recentemente annunciato ulteriori piani per sistemi autonomi avanzati e start-up militari.<sup>4</sup>

La guerra in Ucraina mette in evidenza **il futuro ruolo dell'IA nelle forze armate** in vista dell'incombente conflitto su Taiwan, alimentato dalla Cina. Pechino e Washington stanno attualmente promuovendo lo sviluppo di sciami autonomi di droni che comunicano tra loro. La Cina punta a diventare la prima potenza mondiale nel campo dell'IA entro quest'anno ed ha adottato una strategia militare aggressiva ed orientata all'innovazione.<sup>5</sup> Anche il Regno Unito sta studiando robot dotati di IA per consentire alle truppe di terra di distruggere ponti strategicamente importanti, motivati anche dall'esperienza in Ucraina.<sup>6</sup>

Come dovrebbe posizionarsi l'Europa occidentale in questa **competizione digitale**? Le voci critiche chiedono che l'IA militare sia generalmente bandita a livello internazionale. Altri ritengono tali sistemi indispensabili per non mettere a rischio unilateralmente la sicurezza dell'Occidente. Le analisi del conflitto in Ucraina, le esperienze con i sistemi di armamento autonomi e gli esperimenti con le applicazioni di IA dimostrano quanto sia necessario valutare sistematicamente l'interazione tra uomini e macchine per evitare effetti negativi, ad esempio il "fuoco amico". I futuri negoziati sulla regolamentazione della cosiddetta IA responsabile in campo militare dovrebbero stabilire standard vincolanti a questo proposito.

## 2 Il potere militare nell'era dell'IA

L'automazione delle innovazioni tecnologiche militari è progredita sempre più negli ultimi anni. Nell'era dell'IA, secondo l'esperto di difesa Paul Scharre, **quattro elementi chiave sono cruciali per la potenza militare**: dati da raccogliere e analizzare, controllo continuo delle catene di fornitura dei chip, capitale umano ed innovazione industriale, nonché l'integrazione dell'IA con le imprese, la società e le forze armate. Scharre cita esempi in cui i cosiddetti agenti di IA simulano determinate situazioni di guerra.<sup>7</sup>

L'era dell'intelligenza artificiale **ridefinirà il potere militare**. La Russia sembra avere le carte peggiori al momento. Dall'inizio della guerra, più di **100.000 specialisti IT** - il 10% di tutti quelli

---

<sup>1</sup> [The Ukraine-Russia Drone War Is Crowdsourced and Made in China \(foreignpolicy.com\).](https://foreignpolicy.com/article/the-ukraine-russia-drone-war-is-crowdsourced-and-made-in-china/)

<sup>2</sup> [Digitale Schizophrenie - Tagesspiegel Background.](https://www.tagesspiegel.de/digital/digitale-schizophrenie-tagespiegel-background/)

<sup>3</sup> Altrettanto rilevante nei primi giorni è stato il drone tattico-militare TB2 Bayraktar di un fornitore turco. [TB2 Bayraktar : Grande stratégie d'un petit drone | IFRI - Institut français des relations internationales.](https://www.ifsri.fr/en/analyses/grande-strategie-d-un-petit-drone-ifsri-institut-francais-des-relations-internationales/)

<sup>4</sup> [Ukraine wants a robot army \(wired.com\).](https://www.wired.com/story/ukraine-wants-a-robot-army/)

<sup>5</sup> [The PLA's Strategic Support Force and AI Innovation \(brookings.edu\).](https://www.brookings.edu/research/the-plas-strategic-support-force-and-ai-innovation/)

<sup>6</sup> [British army seeks AI-powered robots to allow troops to demolish bridges in combat \(inews.co.uk\).](https://www.inews.co.uk/news/uk/british-army-seeks-ai-powered-robots-to-allow-troops-to-demolish-bridges-in-combat/)

<sup>7</sup> [Four Battlegrounds | Paul Scharre | W. W. Norton & Company \(wwnorton.com\).](https://www.wwnorton.com/press/press-releases/4-robot-battlefields)

precedentemente impiegati nel settore tecnologico - hanno voltato le spalle alla Russia.<sup>8</sup> Nello stesso periodo, il numero di start-up militari ucraine è decuplicato.<sup>9</sup> Inoltre, la scena tecnologica ucraina è meglio collegata a livello internazionale. Utilizza iniziative come "Army of Drones" per ottenere più rapidamente hardware di droni stranieri. Il collettivo internazionale di hacker *Anonymous* riesce regolarmente a piazzare critiche alla guerra nei media russi e a pubblicare terabyte di **file hackerati**.<sup>10</sup> Più recentemente, gli hacker ucraini della "Cyber Resistance" sono riusciti a recuperare le e-mail di una spia russa che voleva manipolare le elezioni presidenziali statunitensi del 2016.<sup>11</sup>

Le conseguenze di questo squilibrio tecnologico sono già chiaramente visibili sul campo di battaglia. Kiev utilizza l'IA in modo più efficace di Mosca. In particolare per quanto riguarda la **ricognizione geografica e il riconoscimento dei bersagli**. Ad esempio, i dati open source come le foto sensibili dal punto di vista geopolitico sui social media vengono analizzati con l'IA.<sup>12</sup> Gli sviluppatori ucraini hanno addestrato i sistemi di IA per identificare i carri armati nemici mimetizzati con le riprese in diretta dei droni ed a distruggerli in tempo quasi reale.<sup>13</sup> I sistemi sono programmati per imparare costantemente da soli. Poiché questi droni non utilizzano il GPS durante il volo, le contromisure russe sono state spesso inizialmente inutili. In risposta agli attacchi missilistici russi dalle navi da guerra nel Mar Nero, l'Ucraina ha sviluppato imbarcazioni drone che trasportano esplosivi e utilizzano l'intelligenza artificiale per individuare i bersagli.<sup>14</sup> L'azienda tecnologica ucraina *Primer* ha adattato il suo **servizio di trascrizione** e traduzione vocale AI per elaborare rapidamente le comunicazioni russe intercettate ed estrarre automaticamente informazioni sulle forze armate.<sup>15</sup> L'Ucraina sta approfittando del fatto che i soldati russi comunicano spesso tra loro in modo non criptato. Alla fine di febbraio, Fedorov ha scritto che l'uso di tecnologie militari innovative è uno dei settori in cui l'Ucraina è sempre un passo avanti rispetto alla Russia.<sup>16</sup>

Anche la Russia sta cercando di utilizzare le moderne tecniche digitali. Questi, tuttavia, **sono stati finora limitati principalmente agli attacchi ibridi nel cyberspazio**.<sup>17</sup> I "Vulkan Files", pubblicati di recente, mostrano come l'intelligence russa orchestri i cyber-attacchi, diffonda la disinformazione e censuri Internet con l'aiuto dell'appaltatore della difesa con sede a Mosca NTC Vulkan.<sup>18</sup> Sul campo di battaglia, tuttavia, il Cremlino sta facendo fatica, ricorrendo ai cosiddetti droni kamikaze, tecnicamente relativamente semplici, provenienti dall'Iran. Molte prove suggeriscono che l'esercito russo si è concentrato principalmente sulla guerra tradizionale con carri armati, artiglieria e potenza aerea nella sua invasione dell'Ucraina. Secondo Alex Karp, capo dell'azienda di Big Data *Palantir*, la Russia si trova in una situazione di "enorme svantaggio" a causa della mancanza di tecnologie di intelligenza artificiale (IA).<sup>19</sup> Anche le operazioni informatiche di Mosca, tecnicamente riuscite, non hanno portato ad alcun vantaggio operativo. L'attacco al provider *Viasat* all'inizio della guerra ha

---

<sup>8</sup> [How Russia killed its tech industry | MIT Technology Review.](#)

<sup>9</sup> [Ukraine wants a robot army \(wired.com\).](#)

<sup>10</sup> [Hacker im Cyberkrieg: Die kuriosesten Angriffe von Anonymous auf den Kreml \(watson.de\).](#)

<sup>11</sup> [Demokraten-Hack 2016: Ukrainische Hacker wollen russischen Spion gehackt haben - Golem.de.](#)

<sup>12</sup> [Ukraine A Living Lab for AI Warfare \(nationaldefensemagazine.org\).](#)

<sup>13</sup> [Artificial intelligence helps drones destroy camouflaged Russian vehicles \(gagadget.com\).](#)

<sup>14</sup> [Ukraine wants a robot army \(wired.com\).](#)

<sup>15</sup> [One year on: 10 technologies used in the war in Ukraine - TechInformed.](#)

<sup>16</sup> [Tech innovation helps Ukraine even the odds against Russia's military might - Atlantic Council](#)

<sup>17</sup> Fin dall'ottobre 2021, hacker vicini all'FSB hanno preso di mira gli account di organizzazioni ucraine e nel gennaio 2022 gli esperti di Microsoft hanno identificato un'operazione di malware su larga scala. [ACTINIUM targets Ukrainian organizations - Microsoft Security Blog](#); [Destructive malware targeting Ukrainian organizations - Microsoft Security Blog.](#)

<sup>18</sup> [Russlands Strategie der Cyberkriegsführung offengelegt – EURACTIV.de.](#)

<sup>19</sup> [Palantir CEO Alex Karp on Responsible AI in Warfare | REAIM 2023 - YouTube.](#)



paralizzato le comunicazioni satellitari sull'Ucraina, ma **ha chiaramente fallito l'obiettivo** di ostacolare le operazioni di comando e ricognizione ucraine.<sup>20</sup> E piuttosto, ha provocato una serie di effetti non preventivati, ad esempio disabilitando i modem satellitari delle turbine eoliche tedesche.

Lo svantaggio della Russia in termini di IA si spiega principalmente con un'importante **differenza sistemica**. I settori tecnologici dei due Paesi dipendono dai **rispettivi sistemi normativi**. In Russia, le aziende statali sviluppano attrezzature per la difesa per conto del governo, mentre in Ucraina c'è un ampio spettro privato di aziende, *start-up* e inventori freelands.<sup>21</sup> L'arsenale dell'Ucraina è più vario e quindi più difficile da combattere. Secondo Fedorov, l'Ucraina ha il talento informatico e la flessibilità necessari per trasferire nuovi concetti tecnici "dal tavolo da disegno al campo di battaglia" in un breve periodo di tempo.<sup>22</sup> In netto contrasto, anche le recenti attività di spionaggio dei servizi segreti russi che si basano su molti vecchi elementi già noti da campagne precedenti.<sup>23</sup> Con l'arretramento del settore tecnologico russo, regolamentato e spaventato da Putin, si riduce anche la capacità del Cremlino di impiegare la moderna IA militare.

### 3 Verso un'IA responsabile?

Anche se le tecnologie digitali offrono vantaggi di politica militare in Occidente, sollevano pure la questione della loro controllabilità. In particolare, l'aumento dell'uso di funzioni autonome e di sistemi di intelligenza artificiale nella guerra in Ucraina potrebbe accelerare lo **sviluppo di armi completamente autonome**, il cui uso non potrà mai essere completamente controllato. Nell'ultimo decennio si sono quindi diffuse iniziative come la "campagna per fermare i robot assassini", iniziata nel 2012. Secondo gli attivisti, le tecnologie potenzialmente incontrollabili dovrebbero essere vietate in una fase iniziale perché, secondo gli attivisti, violano i diritti umani e portano a un aumento dei conflitti.

Tuttavia, la guerra di aggressione della Russia ha dato a questo dibattito una nuova valenza. Al primo vertice globale sull'**IA militare responsabile**, tenutosi nei Paesi Bassi a metà febbraio 2023, il Dipartimento di Stato americano ha presentato una cosiddetta dichiarazione politica sulle condizioni in cui tali armi dovrebbero essere sviluppate.<sup>24</sup> Questa dichiarazione non vieta l'IA militare, ma elenca le "migliori pratiche" in astratto. Ad esempio, afferma che le armi AI dovrebbero essere sviluppate solo in conformità alle leggi internazionali e che i principi tecnici dovrebbero essere trasparenti. Alcuni ricercatori hanno anche considerato come i sistemi militari autonomi potrebbero essere progettati per comportarsi eticamente almeno meglio dei soldati convenzionali.<sup>25</sup>

Tuttavia, la richiesta di un divieto basato su principi etici non può più essere avanzata nell'attuale situazione geopolitica; da una prospettiva occidentale, sarebbe addirittura **ingenua**. La guerra in Ucraina dimostra, come un **laboratorio di prova quasi tragico**, che l'IA sarà utilizzata nei conflitti

---

<sup>20</sup> [Cyber Operations in Russia's War against Ukraine - Stiftung Wissenschaft und Politik \(swp-berlin.org\)](https://www.swp-berlin.org/en/analysis/cyber-operations-in-russia-s-war-against-ukraine).

<sup>21</sup> [Ukrainian developers use artificial intelligence for more accurate drones bombardment • Mezha.Media](https://www.mezha.media/en/ukrainian-developers-use-artificial-intelligence-for-more-accurate-drones-bombardment). Tuttavia, non c'è dubbio che l'ordine economico ucraino necessiti di ulteriori riforme. Anche se la legge marziale attualmente subordina l'intera economia e la sua amministrazione alle esigenze militari e di sicurezza, c'erano già dei deficit prima della guerra, soprattutto sotto forma di corruzione, ad esempio nel sistema giudiziario e nelle imprese statali. Per un'analisi si veda: [Reforming the Ukrainian Economy and State: The Unfinished Business | Publications | CESifo](https://www.cesifo.org/en/publications/2023/04/reforming-the-ukrainian-economy-and-state-the-unfinished-business).

<sup>22</sup> [Ukraine's millennial minister leads digital fight against Russia | The Hill](https://www.thehill.com/policy/ukraine/2023/02/22/ukraine-millennial-minister-leads-digital-fight-against-russia/).

<sup>23</sup> [Espionage campaign linked to Russian intelligence services - Baza wiedzy - Portal Gov.pl \(www.gov.pl\)](https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services).

<sup>24</sup> [Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy, Department of State](https://www.state.gov/statement/2023/02/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/). Per una simile analisi, si veda: [The US Pushing for Responsible AI in Military Use \(holisticai.com\)](https://www.holisticai.com/en/the-us-pushing-for-responsible-ai-in-military-use).

<sup>25</sup> Arkin, R. (2009). *Governing Lethal Behavior in Autonomous Robots* (1st ed.). Chapman and Hall/CRC.

futuri, a dispetto di tutti i principi etici. I vantaggi sul campo di battaglia di poter analizzare grandi quantità di dati, prevedere i movimenti del nemico e reagire rapidamente a qualsiasi minaccia sono troppo allettanti. Ma le armi autonome dell'IA possono anche portare a problemi incontrollabili come il "fuoco amico" nel proprio campo. Pertanto, è importante non solo da un punto di vista etico, ma anche strategico-militare, sviluppare **strategie per il loro monitoraggio** in una fase iniziale che tenga conto degli errori precedenti dei sistemi autonomi.<sup>26</sup>

## 4 Imparare dal passato

Le precedenti esperienze con i sistemi militari automatizzati rivelano gravi problemi che aumenteranno esponenzialmente nell'era dell'IA. Durante la guerra in Iraq, ad esempio, un Tornado britannico è stato abbattuto dalla Marina statunitense. Un programma informatico americano aveva **classificato erroneamente il caccia come un missile iracheno**. I criteri programmati nel sistema di difesa aerea *Patriot* avrebbero dovuto essere molto più restrittivi, viste le capacità dell'Iraq all'epoca, come ha scoperto in seguito un'inchiesta parlamentare.<sup>27</sup>

Questo incidente è elencato nell'**AI Incident Database**, un'enciclopedia online degli incidenti di intelligenza artificiale conosciuti, sotto la voce "errori epocali".<sup>28</sup> Il database contiene numerosi altri casi in cui i sistemi di armi automatiche hanno provocato vittime involontarie a causa di una classificazione errata.<sup>29</sup> Gli esperti dubitano che un'arma autonoma sarà mai in grado di distinguere adeguatamente tra obiettivi civili e militari.<sup>30</sup> Tali sistemi violano quindi il cosiddetto **principio di discriminazione**, secondo il quale nell'uso della forza occorre distinguere tra militari e civili.<sup>31</sup>

I problemi di classificazione descritti potrebbero essere amplificati nella prossima generazione di IA militare, come gli sciami automatizzati di droni. Ad esempio, i sistemi d'arma basati sull'IA richiedono dati completi, pertinenti e granulari per essere addestrati. Tuttavia, la **natura dinamica, complessa e ostile degli ambienti di conflitto** rende la loro applicazione, al di fuori dei laboratori, estremamente soggetta ad errori, poiché fattori nuovi o imprevedibili non sono inclusi nei dati di addestramento.<sup>32</sup> La situazione sta cambiando: ogni giorno che passa del conflitto ucraino, i sistemi di IA vengono addestrati con dati reali provenienti da un vero campo di battaglia.<sup>33</sup> Questo rende **più interessante** per Paesi come la Cina, che ha le sue ambizioni per i sistemi di IA militari, **fornire armi** per trarre profitto dai dati raccolti.

## 5 Rischio: sconosciuto e non monitorabile

Alla luce di questi problemi, c'è attualmente un consenso schiacciante sul fatto che i sistemi di IA militari dovrebbero offrire una combinazione di processi automatizzati e capacità di intervento

---

<sup>26</sup> [Understanding the errors introduced by military AI applications \(brookings.edu\)](https://www.brookings.edu/research/understanding-the-errors-introduced-by-military-ai-applications/).

<sup>27</sup> [maaszg710.doc \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/100000/maaszg710.doc).

<sup>28</sup> Atherton, Daniel. (2003-03-22) Incident Number 444. in Lam, K. (ed.) Artificial Intelligence Incident Database. Responsible AI Collaborative. Retrieved on March 1, 2023 from [incidentdatabase.ai/cite/444](https://incidentdatabase.ai/cite/444).

<sup>29</sup> Atherton, Daniel. (2003-04-02) Incident Number 445. in Lam, K. (ed.) Artificial Intelligence Incident Database. Responsible AI Collaborative. Retrieved on March 1, 2023 from [incidentdatabase.ai/cite/445](https://incidentdatabase.ai/cite/445).

<sup>30</sup> Kallenborn, Z. (2021). Meet the Future Weapon of Mass Destruction, the Drone Swarm. Bulletin of the Atomic Scientists, <https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm/>.

<sup>31</sup> Dresch-Langley Birgitta (2023), The weaponization of artificial intelligence: What the public needs to be aware of, Frontiers in Artificial Intelligence 6, <https://www.frontiersin.org/articles/10.3389/frai.2023.1154184>.

<sup>32</sup> Holland Michel, Arthur. 2021. Known Unknowns: Data Issues and Military Autonomous Systems. Geneva: United Nations Institute for Disarmament Research. <https://doi.org/10.37559/SecTec/21/AI1>.

<sup>33</sup> [Ukraine A Living Lab for AI Warfare \(nationaldefensemagazine.org\)](https://www.nationaldefensemagazine.org/articles/story/ukraine-a-living-lab-for-ai-warfare).

umano. Anche se l'intuizione di un tale modello "**human in the loop**" è da accogliere con favore in linea di principio, in vista delle decisioni epocali dei sistemi d'arma che riguardano la vita e la morte, occorre mettere in guardia dall'errata convinzione che tale combinazione di uomo e macchina sia sufficiente per un uso sicuro e affidabile. Questo perché gli esseri umani spesso accettano la decisione raccomandata da un sistema di IA, anche se è sbagliata - un problema noto come **AI overreliance**, o "fiducia cieca" nell'IA.

Pertanto, l'interazione tra esseri umani e macchine è difficile da valutare perché gli esseri umani non sempre reagiscono razionalmente alle raccomandazioni di un computer.<sup>34</sup> In un esperimento, i partecipanti hanno seguito i consigli deliberatamente mal programmati dell' algoritmo anche quando avrebbero dovuto saperlo da tempo.<sup>35</sup> Alcuni ricercatori sperano di ridurre la fiducia cieca nei sistemi di intelligenza artificiale costringendoli a **spiegare le loro decisioni**. Ma i test dimostrano che tali spiegazioni aumentano solo la probabilità che le persone accettino le raccomandazioni dell'IA, indipendentemente dalla loro correttezza.<sup>36</sup>

Una soluzione che funziona, almeno a livello sperimentale, non è solo quella di fornire una spiegazione, ma anche di incoraggiare le persone a impegnarsi a livello cognitivo.<sup>37</sup> Tuttavia, è discutibile che ci sia abbastanza tempo per un processo così sofisticato se sul campo di battaglia sono in gioco millisecondi. L'IA militare si occupa di compiti complessi, il che implica che le spiegazioni dell'IA saranno spesso complesse da capire quanto il compito stesso. Un esperto che ha studiato gli incidenti di "fuoco amico" in Iraq a cui si è fatto riferimento avverte che i dettagli del dispiegamento dei missili balistici sono "**troppo complessi e limitati nel tempo per un coinvolgimento umano diretto**".<sup>38</sup>

## 6 Un metodo basato sul rischio con test strutturati

Mentre l'IA in ambito militare sta diventando sempre più rilevante e allo stesso tempo soggetta a errori, il dibattito sulla sua regolamentazione è in ritardo.<sup>39</sup> **Non esistono accordi multilaterali, processi di certificazione o standard globali** per garantire sistemi d'arma IA solidi e affidabili. È significativo che la già citata dichiarazione degli Stati Uniti sull'IA militare responsabile non sia giuridicamente vincolante. Gli attuali negoziati delle Nazioni Unite sui sistemi di armi autonome letali, in corso a Ginevra, stanno arrancando.<sup>40</sup> Eppure tali regole sono urgentemente necessarie, poiché la progettazione etica di armi IA è "teoricamente interessante" ma "impraticabile", secondo un importante scienziato informatico.<sup>41</sup>

L'ispirazione potrebbe venire dalla **legge sull'IA** che i legislatori dell'UE stanno attualmente negoziando. La proposta segue un **approccio basato sul rischio**, in quanto vieta pratiche di IA particolarmente dannose. Anche se l'attuale proposta legislativa dell'UE esclude esplicitamente i sistemi di IA militari, il suo quadro e i suoi requisiti orizzontali possono contribuire allo sviluppo di

<sup>34</sup> [Algorithmic Risk Assessment in the Hands of Humans \(iza.org\)](https://iza.org/).

<sup>35</sup> Biermann, Jan and Horton, John J. and Walter, Johannes, Algorithmic Advice as a Credence Good ( 2022). ZEW - Centre for European Economic Research Discussion Paper No. 22-071, <http://dx.doi.org/10.2139/ssrn.4326911>.

<sup>36</sup> [\[2006.14779\] Does the Whole Exceed its Parts? The Effect of AI Explanations on Complementary Team Performance \(arxiv.org\)](https://arxiv.org/abs/2006.14779).

<sup>37</sup> [\[2212.06823\] Explanations Can Reduce Overreliance on AI Systems During Decision-Making \(arxiv.org\)](https://arxiv.org/abs/2212.06823).

<sup>38</sup> [Patriot Wars | Center for a New American Security \(en-US\) \(cnas.org\)](https://www.cnas.org/publications/policy-reports/patriot-wars).

<sup>39</sup> [Amazon.com: Death machines: The ethics of violent technologies: 9781526114846: Schwarz, Elke: Bücher](https://www.amazon.com/Death-machines-The-ethics-violent-technologies-9781526114846-Schwarz-Elke-Bücher/dp/B098888888).

<sup>40</sup> [Verhandlungen von der CCW in die UNO? - Tagesspiegel Background](https://www.tagesspiegel.de/verhandlungen-von-der-ccw-in-die-uno-2020-07-14).

<sup>41</sup> Michael Wooldridge, A Brief History of Artificial Intelligence, New York 2020, S. 195.

norme pertinenti per le applicazioni di IA in ambito militare.<sup>42</sup> Sarebbero ipotizzabili categorizzazioni analoghe, in base alle quali le armi autonome letali sarebbero vietate, mentre tutti gli altri sistemi militari di IA dovrebbero soddisfare requisiti di gestione del rischio, documentazione, trasparenza, verificabilità, robustezza e sicurezza informatica.

Poiché gli esseri umani spesso non riescono a monitorare le raccomandazioni dell'IA, l'efficacia dei modelli militari *human-in-the-loop* deve essere **valutata in modo strutturato**.<sup>43</sup> Una documentazione così trasparente promuoverebbe un discorso politico più razionale su questo argomento, perché le precedenti ricerche sui sistemi d'arma autonomi sono state applicate quasi esclusivamente in ambito militare.<sup>44</sup> Se questi test dimostrano che gli esseri umani non sono in grado di controllare efficacemente i cosiddetti droni killer o altri sistemi di IA, questi dovrebbero essere inseriti nella categoria delle IA militari vietate.

L'attacco della Russia all'Ucraina e le crescenti tensioni geopolitiche con la Cina stanno costringendo i politici occidentali a prendere seriamente in considerazione l'uso dell'IA militare. Ma le potenziali conseguenze dell'uso di armi guidate dall'IA possono essere valutate solo in maniera approssimativa. Pertanto, l'opinione pubblica deve essere **sensibilizzata sui pericoli**. È compito della politica stabilire **condizioni quadro vincolanti** con classificazioni giuridiche, obblighi di trasparenza e test strutturati sulla controllabilità umana di questi sistemi.

---

<sup>42</sup> [Challenges of Governing AI for Military Purposes and Spill-Over Effects of the AI Act | Futurium \(europa.eu\)](#).

<sup>43</sup> Analog für andere KI-Bereiche: [The AI Act should use humans to monitor AI only when effective – EURACTIV](#).

<sup>44</sup> Dresch-Langley Birgitta (2023), The weaponization of artificial intelligence: What the public needs to be aware of, *Frontiers in Artificial Intelligence* 6, <https://www.frontiersin.org/articles/10.3389/frai.2023.1154184>.





**Autori:**

Dr. Anselm Küsters, Capo dipartimento Digitalizzazione e nuove tecnologie  
[kuesters@cep.eu](mailto:kuesters@cep.eu)

Dr. Jörg Köpke, Responsabile Comunicazione Centrum für Europäische Politik  
[koepke@cep.eu](mailto:koepke@cep.eu)

**Centrum für Europäische Politik** FREIBURG | BERLIN  
Kaiser-Joseph-Straße 266 | D-79098 Freiburg  
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin  
Tel. + 49 761 38693-0



**Traduzione** (dalla versione originale in lingua tedesca):

**Prof. Dr. Andrea De Petris**, Direttore scientifico  
[depetris@cep.eu](mailto:depetris@cep.eu)

**Centro Politiche Europee** ROMA  
Via G. Vico, 1 | I-00196 Roma  
Tel. +390684388433  
[cepitalia@cep.eu](mailto:cepitalia@cep.eu)

Il **Centrum für Europäische Politik** FREIBURG | BERLIN, il **Centre de Politique Européenne** PARIS, ed il **Centro Politiche Europee** ROMA costituiscono il **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Gli istituti della rete CEP sono specializzati nell'analisi e nella valutazione degli atti promossi dalle istituzioni dell'Unione europea nell'ambito delle politiche di loro competenza e nel quadro d'insieme del processo di integrazione. Il lavoro scientifico, riflesso in particolare nelle proprie pubblicazioni, viene portato avanti indipendentemente da qualsiasi interesse di parte e in favore di una Unione europea che rispetti lo stato di diritto ed i principi dell'economia sociale di mercato.